BeyondTrust Software, Inc.

IT Risk Management Framework

v6.0

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.0

Prepared for:

BeyondTrust™
VISIBILITY. KNOWLEDGE. ACTION.

BeyondTrust Software, Inc.
5090 North 40th Street
Suite 400
Phoenix, AZ 85018
United States of America

Phone: +1 480 405 9131
www.beyondtrust.com

Prepared by:

Corsec

Corsec Security, Inc.
13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

List of Figures

List of Tables

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the BeyondTrust Software, Inc. (BeyondTrust) IT[1] Risk Management Framework v6.0 and will hereafter be referred to as the TOE. The TOE is a unified hardware and software suite of privileged account management and vulnerability management components. The TOE provides organizations with advanced threat analytics, system malware analysis, user management, and auditing of multiple systems.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	BeyondTrust Software, Inc. IT Risk Management Framework v6.0 Security Target
ST Version	Version 1.0
ST Author	Corsec Security, Inc.
ST Publication Date	May 8, 2017

[1] IT – Information Technology

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

TOE Reference	BeyondTrust IT Risk Management Framework v6.0 which includes the following:
	• PowerBroker for Windows v7.1.0.32
	• BeyondTrust UVM50[2] hardware appliance running:
	  ○ UVM50 software v2.0.3
	  ○ Retina v6.0.0.6071
	  ○ BeyondInsight v6.2.0.1092
	• PowerBroker Management Suite v5.0.138.0 using the below modules:
	  ○ PowerBroker Auditor for Active Directory (AD) v5.0.138.0
	  ○ PowerBroker Recovery for AD v5.0.138.0
	  ○ PowerBroker Auditor for File System v5.0.138.0
	  ○ PowerBroker Auditor for Exchange v5.0.138.0
	  ○ PowerBroker Auditor for SQL[3] Server v5.0.138.0

1.3 Product Overview

The Product Overview provides a high-level description of the product that is the subject of the evaluation. The following section, TOE Overview, will introduce the parts of the overall product offering that are specifically being evaluated.

BeyondTrust's IT Risk Management Framework v6.0 is a unified platform for privileged account management, vulnerability management, and auditing. The IT Risk Management Framework delivers a comprehensive view of the vulnerabilities that provide doors into an environment, as well as the privileges that present corridors to sensitive assets. Multiple systems are audited by The IT Risk Management Framework for any user actions or changes. This fusion of asset and user intelligence enables IT and Security teams to collectively:

- Reduce user-based risk and mitigate threats to information assets.
- Address security exposures across large, diverse IT environments.
- Comply with internal, industry and government mandates.
- Provide an audit history on critical events.

By unifying BeyondTrust's privileged account management, vulnerability management solutions, and auditing solutions, BeyondTrust's IT Risk Management Framework provides a single-pane of visibility and control over user and asset risk.

1.3.1 IT Risk Management Framework Components

The IT Risk Management Framework contains these main components: BeyondInsight (BI), PowerBroker for Windows (PBW), Retina, and the PowerBroker Management Suite (PBMS) loaded with the PowerBroker Auditor (PBA) modules. The BI and Retina components are housed within BeyondTrust's UVM50 hardware appliance. The PBW Policy Editor and PBA components will be installed on Windows 2012 R2[4] servers in the environment. The below sections further describe each component.

1.3.1.1 BeyondInsight

BI is a data warehousing solution with business intelligence and analytics. BI extracts data from the BI Console UI[5] in the form of Online Analytical Processing (OLAP) cubes and processes the data in Microsoft SQL Reporting

[2] UVM50 – Unified Vulnerability Manager 50
[3] SQL – Structured Query Language
[4] R2 – Release Two
[5] UI – User Interface

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Services (SRS). Read-only data can also be extracted from the cubes for use in various third-party applications. Using BI, administrators can:

- Run reports on Retina's vulnerability and attack data from the BI Console UI.
- Run reports on data from PBW.
- Subscribe to reports that are scheduled for automatic delivery to a network file share or through email.
- Save report views to easily reuse a report with predefined parameters.
- Create report snapshots to save static views of report data.
- Interactively explore live data with a Pivot Grid.
- Evaluate risk on assets using the Threat Analyzer.

BI provides a set of tools to help administrators organize assets for scanning. Depending on the number of assets that an administrator wants to scan, or the critical nature of some of the assets, they might consider organizing the assets using address groups or AD queries, which can be part of a Smart Rule. Scans can return significant amounts of information. To help administrators review scan results, they can create filters and set preferences on the Assets page to easily review scan results.

1.3.1.2 PowerBroker for Windows (PBW)

PBW enables administrators to create privileged identity, risk and compliance, event monitoring, and file integrity rules in the Group Policy Management Editor, which is part of the Group Policy Management Console (GPMC). Each PBW rule elevates or reduces the permissions and privileges of a Windows application or process at runtime. A rule can also elevate or reduce the permissions and privileges of an MSI[6] package or an ActiveX control when they launch. Administrators can create rules by using the Create a Rule Wizard or by using the Properties dialog for a rule. Rule generation is a practical way to assemble a basic rule set for an organization based on existing application usage. Administrators can then refine this set of rules to meet their specific needs. For increased targeting granularity, administrators can use item-level targeting to apply certain rules to only the selected computers or specific users.

PBW incorporates BeyondTrust's proprietary Vulnerability Based Application Management (VBAM) software, which controls privileged access to applications. VBAM enables administrators to create rules for individual applications based on risks and compliance initiatives. When creating the rule, administrators can choose from a list of actions that enforce restrictions on applications. Administrators can also set parameters based on access risks, risk severity, PCI[7] score, or CVSS[8] score.

PBW enables administrators to create a rule that can quarantine a specific application. When the rule matches, the application is moved to PBW Quarantine. Administrators can also configure a Quarantined Application User Message to display when a user attempts to access a quarantined application. Quarantine rules can also be configured to restore applications that were previously moved into quarantine by using the Restore Application from Quarantine action. Quarantine rules are processed before all other rules. This ensures that any rules that may be made on a quarantined application are nullified.

[6] MSI – Microsoft Installer
[7] PCI – Payment Card Industry
[8] CVSS – Common Vulnerability Scoring System

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.3.1.3 Retina

Retina provides vulnerability testing for multiple platforms, automatic fixes of vulnerabilities (when using the patch management module via WSUS[9]/SCCM[10]), and the ability to create one's own audit scans. In addition, Retina allows administrators to proactively secure their networks against the most critical vulnerabilities by incorporating the most up-to-date vulnerabilities database. Since vulnerability audits are added continually, this database is updated at the beginning of each session. Using Retina, administrators can:

- Scan in parallel using the Retina queuing system to scan up to 128 targets simultaneously.
- Perform the majority of scans without administrative rights. This allows administrators to quickly and easily secure their globally distributed networks. However, it is strongly recommended that scans be performed with administrative credentials to avoid any issues.
- Run configuration benchmark scans using profiles for DISA[11] Gold Disk, SCAP[12], NIST[13], FDCC[14], USGCB[15], CIS[16], Microsoft, and in-house policies.

1.3.1.4 PowerBroker Management Suite

PBMS contains several PBA modules, namely PBA for File Systems, PBA for Exchange, PBA for SQL Server, and PBA for AD including PowerBroker (PB) Recovery for AD, that allow administrators to do the following:

- Deploy agents to selected Domain Controllers (PBA for AD)
- Create real-time policies for Active Directory (PBA for AD)
- Create pre-defined schedules that can be selected when creating collectors (PBA for AD and PB Recovery for AD)
- Recover deleted objects (PB Recovery for AD)
- Rollback objects to a previously saved state (PB Recovery for AD)
- Rollback unwanted audit changes (PBA for AD)
- Create audit views that can be opened to examine and analyze activity and audit trails for AD, SQL server, Windows file system, and/or Exchange server (PBA for AD, SQL server, Windows File System, and Exchange Server)

PBA for AD provides a centralized control to AD auditing and compliance. The PBA for AD module is installed on the server with PBMS, and the PBA for AD agent is deployed to each domain controller. The PBA for AD agent monitors the AD server and Group Policy in real-time, tracking every change. PowerBroker Recovery for AD, when used with PBA for AD, provides continuous object backup and recovery to minimize the risk of business disruptions. The solution stores every object change in a continuous change log. This enables administrators to instantly rollback unwanted changes to any previous state, right up to the point of the error. PB Recovery for AD eliminates tedious manual recovery efforts, saving critical time and ensuring business productivity.

The PBA for Microsoft Exchange module is installed on the server with PBMS, and the PBA for Microsoft Exchange agent is deployed to the Microsoft Exchange server. The PBA for Microsoft Exchange agent tracks and reports all changes made to all Exchange Server configurations, groups, mailbox policies, information store changes, and permissions in a centralized audit log. The integrated solution provides a centralized, real-time audit database for

[9] WSUS – Windows Server Update Services
[10] SCCM – System Center Configuration Manager
[11] DISA – Defense Information Systems Agency
[12] SCAP – Security Content Automation Protocol
[13] NIST – National Institute of Standards and Technology
[14] FDCC – Federal Desktop Core Configuration
[15] USGCB – United States Government Configuration Baseline
[16] CIS – Center for Internet Security

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

reporting and alerting against all Exchange activity including users and non-owner mailbox access for compliance and tighter security controls. This powerful solution monitors the Exchange environment in real-time, tracking every change.

The PBA for Windows File System module is installed on the server with PBMS, and the PBA for Windows File System agent is deployed to a Windows 2012 R2 server. The PBA for Windows File System enables tighter security and control over File System resources across the enterprise. The PBA for Windows File System agent provides real-time tracking, interactive analysis, and flexible reporting on all key share, file, and folder changes. Administrators can instantly know the details for every access and change event and schedule reports for data owners to show them who is accessing and modifying their data.

The PBA for SQL Server module is installed on the server with PBMS and monitors the Microsoft SQL 2014 SP1[17] server. PBA for SQL Server provides a centralized control to SQL Server auditing and compliance. PBA for SQL Server monitors all SQL Server activity in real-time, tracking every change.

1.3.1.5 UVM50

The BeyondTrust UVM50 Security Management Appliance delivers pre-installed and pre-configured vulnerability and privileged account management capabilities, combining BeyondTrust's Retina and PBW under the BI centralized management, reporting and analytics console. This 2U[18] rack-mount appliance reduces the time to implement integrated vulnerability, privileged account, compliance, and incident management capabilities across the enterprise. The UVM50 also contains a hardened version of Windows Server 2012 R2 and a local Microsoft SQL Server 2014 database.

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the TOE, and defining the specific evaluated configuration.

The TOE is a unified hardware and software suite of privileged account management, vulnerability management, and audit management components. The software components of the TOE include:

- BeyondInsight
- PowerBroker for Windows
  - PowerBroker for Windows Policy Editor installed on a server
  - PowerBroker for Windows client setup for Group Policy rules
- Retina (only accessed through BI)
- PowerBroker Management Suite including the four PowerBroker Auditor modules and their agents as listed below:
  - PowerBroker Auditor for AD (module and agent)
    - PowerBroker Recovery for AD (add-on to PowerBroker Auditor for AD module)
  - PowerBroker Auditor for SQL Server (module)
  - PowerBroker Auditor File System (module and agent)
  - PowerBroker Auditor for Exchange (module and agent)

[17] SP1 – Service Pack 1
[18] 2U – Two Units

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The TOE contains one hardware component, the UVM50. The UVM50 is a 2U[19] rack-mount appliance that hosts the BI and Retina software components. The Operating System (OS) that hosts the software components is a hardened version of Windows Server 2012 R2 and the database that houses their data is a local Microsoft SQL Server 2014 SP1 database.

The following interfaces are used to interact with the TOE: BI Console UI, BI Reporting & Analytics UI (R&A UI), UVM Diagnostics UI, UVM Remote Desktop Connection UI (RDC UI), PBW Editor UI, PBW Polmon UI, PBMS Audit Viewer UI, PBMS Report Interface, and the PBMS UI. The BI Console UI allows BI Administrators to manage the BI and Retina components of the TOE. It also allows access to run scans and create reports based on the scanned data. The BI R&A UI is used for reporting and creating data views based on data collected by Retina. The UVM Diagnostics UI is used by BI Administrators to configure the UVM50's settings, manage BI services, and manage BI roles. The UVM RDC UI is used to access the hardened OS of the UVM50. The BI Administrator will be able to access the file system directly and should only use this interface when instructed by BeyondTrust Technical Support. The PBW Editor UI is used by PBW Administrators to create and manage the PBW rules that are read by the PBW clients. Once the rules are read, the PBW Administrators use the PBW Polmon UI to check the status of the clients and the applied rules. The PBMS UI allows PBMS Administrators access to the PBA modules. Using the PBA modules, the PBMS Administrator manages the collection of events from the various servers. Once events have been collected and stored on the Microsoft SQL server, the PBA modules are used by PBMS Administrators to generate reports based on the collected events. Reports generated by the PBMS Administrator can be viewed using the PBMS Report Interface, which requires SRS, and PBMS Audit Viewer UI.

There are multiple paths of communication in the TOE. When the PBW Editor UI is used to create or update policies in Group Policy, the updates are pushed to the AD server over SMB[20]. The AD server will push Group Policy updates to the PBW Group Policy Client's host OS over SMB where the PBW Group Policy Client will reads the embedded PBW policies and enforce them on the host. The PBW Group Policy Clients will send event log information to BI for analytics and reporting over a TLS[21] connection. BI interacts with Retina when a scan is initiated. Retina sends the scan results and event data to BI for analytics and reporting. Communications sent between BI and Retina are over TLS and does not leave the UVM50. The PBMS component uses SMB to communicate with the PBA Agents installed on the various servers. Communications to the PBA Agents contain collection parameters or changes to settings. The PBA Agents feed all the collected data into a central database over TLS. PBMS accesses the database over TLS when generating reports based on Audit Views. The PBW, PBA, and PBMS TOE components rely on their underlying OS, which are part of the operational environment, to provide TLS and SMB. The TLS and SMB connections are used to secure communication within the TOE and between the TOE and components of its operational environment.

Each component of the TOE and its functionality is described in Section 1.3 (Product Overview) above. Figure 1 depicts the TOE boundary and components in a typical deployment configuration. Note that the previously undefined acronyms, which are used in Figure 1 below, are listed as follows:

- MS – Microsoft
- NTP – Network Time Protocol
- RADIUS – Remote Authentication Dial-In User Service

[19] 2U – Two Rack Units
[20] SMB – Server Message Block
[21] TLS – Transport Layer Security

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

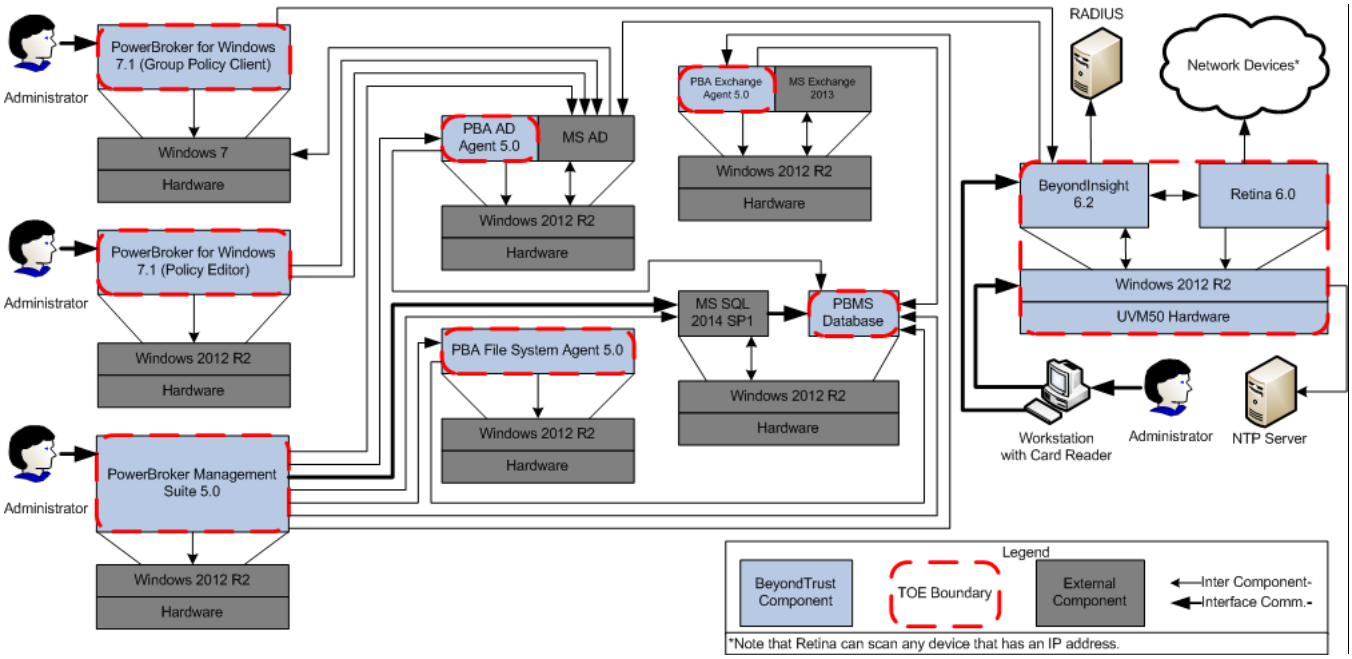

Figure 1 – TOE Boundary and Deployment Configuration

The TOE includes all of the components and functionality described above and in Section 1.3.1. The features and functionality listed below in Section 1.4.1 are not included in the TOE, but are vital for the complete functionality of the TOE. Section 1.4.1 identifies any major non-TOE hardware and software that is required by the TOE including the TOE minimum requirements.

1.4.1 TOE Environment

The TOE relies on hardware and software that is not part of the TOE for its essential operation. As stated in Section 1.4 above, the BI and Retina components run on the UVM50 hardware and Windows 2012 R2 OS that are both within the TOE boundary. The PBW and PBA components require hardware and operating systems that are not covered by the TOE boundary. Refer to Table 2 below for specifics on the required hardware and software versions.

The PBW Policy Editor is installed on a machine running Windows Server 2012 R2 on the required hardware. This machine is usually a domain controller, as PBW Policy Editor requires access to Group Policy Objects. Otherwise, this machine communicates with an AD server to store rules and client configuration settings.

The PBW client is installed on a machine running Windows 7 on the required hardware. This machine will receive Group Policy updates from the AD server that were created using the PBW Policy Editor.

The PBMS software is installed on a machine running Windows Server 2012 R2 on the required hardware. The PBA modules are added to the PBMS Management Console. The PBA modules communicate with the AD server to verify the PBMS Administrator's rights to use the modules. The PBA modules also pull data from the SQL server when displaying audit data from each of the modules' views or reports. The PBA SQL Server module will pull event information from the OS of the SQL server.

A machine running Windows Server 2012 R2 on the required hardware is used to host the PBA File System agent. The PBA File System agent will also communicate with the SQL server to upload any audit logs it captures.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

An Active Directory server running Windows Server 2012 R2 on the required hardware is used to host the PBA AD agent. The PBA AD agent will also communicate with the SQL server to upload any audit logs it captures. The AD server will also be used by BI for authenticating AD accounts.

A Microsoft SQL server running Windows Server 2012 R2 on the required hardware is used to host the PBA audit records. This machine will also be audited by the PBA SQL Server module.

A Microsoft Exchange server running Windows Server 2012 R2 on the required hardware is used to host the PBA Exchange agent. The PBA Exchange agent will also communicate with the SQL server to upload any audit logs it captures.

A RADIUS server will be required for two-factor authentication using RADIUS from BI.

An NTP server may be used to synchronize the UVM's system time to the host's network time.

Any available network devices with a valid IP[22] address can be used by Retina for scanning purposes.

A general-purpose computer or workstation, like the PBW client's host, is used to connect to the BI Console UI, BI R&A UI, UVM RDC UI, and UVM Diagnostics UI. Microsoft Silverlight is required for various BI R&A UI features. A Smart Card reader must be present on the workstation if Smart Card authentication is enabled on the BI Console UI and BI R&A UI.

The underlying operating systems of the operating environment will provide reliable time stamps to the PBW, PBA, and PBMS components.

Table 2 specifies the minimum system requirements for the proper operation of the TOE.

Table 2 – TOE Environment Minimum Requirements

Category	Requirement
PowerBroker for Windows (Policy Editor) host	• Windows Server 2012 R2 • Latest version of .NET Framework • 1.4 GHz[23] processor • 512 MB[24] of RAM[25] • 32 GB[26] of disk space
PowerBroker for Windows (Group Policy client) host	• Windows 7 • Latest version of .NET Framework • 1 GHz processor • 1 GB of RAM • 16 GB of disk space • DirectX 9 graphics device with Windows Display Driver Model 1.0 or higher driver

[22] IP – Internet Protocol
[23] GHz – Gigahertz
[24] MB - Megabyte
[25] RAM – Random Access Memory
[26] GB - Gigabyte

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Category	Requirement
PowerBroker Management Suite host	• Windows Server 2012 R2 • Latest version of .NET Framework • Group Policy Management Console • 1.4 GHz processor • 2 GB of RAM • 32 GB of disk space
PowerBroker Auditor for File System host	• Windows Server 2012 R2 • 1.4 GHz processor • 512 MB of RAM • 32 GB of disk space
Active Directory server	• Windows Server 2012 R2 • 1.4 GHz processor • 512 MB of RAM • 32 GB of disk space
Microsoft SQL server	• Windows Server 2012 R2 • Microsoft SQL Server 2014 SP1 • Latest version of .NET Framework • 1.4 GHz processor • 512 MB of RAM • 38 GB of disk space
Microsoft Exchange server	• Windows Server 2012 R2 • Microsoft Exchange 2013 • Latest version of .NET Framework • 1.4 GHz processor • 8 GB of RAM • 62 GB of disk space
RADIUS server	• Compliant with RFC[27] 2865
NTP server	• Compliant with RFC 5905 (NTPv4) or RFC 1305 (NTPv3)
Network devices scanned by Retina	• An IP address
Workstations	• Windows 7 • Latest version of Internet Explorer • Latest version of Adobe Flash Player • Latest version of Microsoft Silverlight • Latest version of .NET Framework • A Smart Card reader when using Smart Card authentication into BI

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

[27] RFC – Request for Comments

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.5.1 Physical Scope

The TOE is a unified hardware and software suite that runs on the UVM50 hardware and the machines compliant with the minimum software and hardware requirements as listed in Table 2. Note that the machines listed in Table 2 are part of the TOE environment and not the TOE. Figure 1 in Section 1.4 above illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and TOE environment. The essential physical components of the TOE in the evaluated configuration are:

- UVM50 hardware appliance running UVM, BI, and Retina software

The following machines (specifications are listed in Table 2) running TOE software (software versions are listed in Table 1) are required in the TOE environment for proper operation of the TOE:

- At least one machine running one PBW client (in Group Policy mode)
- A server, usually a domain controller, to run the PBW Policy Editor
- A server, which cannot be a domain controller, to host PBMS with the PBA modules
- A domain controller with the PBA AD agent installed
- A server with Windows 2012 R2 to host the PBA File System agent[28]
- A MS SQL database server for storing the PBA events database
- A MS Exchange server with the PBA Exchange agent installed

The TOE boundary includes the UVM50 hardware appliance, UVM software, BI, Retina, PBW client (in Group Policy mode), PBW Policy Editor, PBMS with the PBA modules, PBA AD agent, PBA File System agent, PBA events database, and the PBA Exchange agent. The TOE Boundary does not include any of the third-party software or hardware that the TOE relies upon as described in Section 1.4.1.

1.5.1.1 TOE Software/Hardware

The TOE hardware is the UVM50 and is obtained from a carrier shipment after placing an order for the TOE with BeyondTrust. The TOE software is provided in two ways. BI 6.2 and Retina 6.0 are installed on the UVM50 hardware and is obtained when the shipment is delivered. For PBMS 5.0, the PBA 5.0 modules, and PBW 7.1, BeyondTrust will generate a customer license and send an email that includes a link to download the product installers after placing an order for the TOE.

1.5.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- For BI[29]:
  - *BeyondInsight User Guide*[30]; Revision/Update Information: November 2016; Software Version: BeyondInsight 6.2; Revision Number: 0
  - *BeyondInsight Analytics and Reporting User Guide*; Revision/Update Information: November 2016; Software Version: BeyondInsight 6.2; Revision Number: 0
  - *BeyondInsight Third Party Integration Guide*; Revision/Update Information: November 2016; Software Version: BeyondInsight 6.2; Revision Number: 0

[28] Note that multiple PBA agents can run on the same machine. The PBA File System agent can also run on the AD, SQL, or Exchange server.

[29] Note that an installation guide is not required for BI or Retina as they are preinstalled on the UVM50 appliance.

[30] Note that administrators will use BI to interact with Retina. Retina documentation will not be required as scanning instructions are available in the BI user guide.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- *BeyondInsight Release Notes*; Date of Release: 30 November 2016; Product Name: BeyondInsight; Updated Version: 6.2

- For PBW:
  - *PowerBroker for Windows Installation Guide*; Revision/Update Information: August 19 2016; Software Version: PowerBroker for Windows 7.1; Revision Number: 0
  - *PowerBroker for Windows User Guide*; Revision/Update Information: August 19 2016; Software Version: PowerBroker for Windows 7.1; Revision Number: 1
  - *PowerBroker for Windows Release Notes*; PowerBroker for Windows 7.1.0 – Released 2 September 2016
- For PBA:
  - *PowerBroker Management Suite Installation Guide*; Revision/Update Information: September 7 2016; Software Version: PowerBroker Management Suite 5.0; Revision Number: 1
  - *PowerBroker Management Suite 5.0.138 Release Notes*
  - *PowerBroker Auditing & Security Suite Version 5.0 New and Updated Features*
  - *PowerBroker Auditor for SQL Server User Guide*; Revision/Update Information: July 15 2016; Software Version: PowerBroker Auditor for SQL Server 5.0; Revision Number: 0
  - *PowerBroker Auditor for Exchange User Guide*; Revision/Update Information: July 15 2016; Software Version: PowerBroker Auditor for Exchange 5.0; Revision Number: 0
  - *PowerBroker Auditor for File System User Guide*; Revision/Update Information: July 18 2016; Software Version: PowerBroker Auditor for File System 5.0; Revision Number: 1
  - *PowerBroker Auditor for Active Directory User Guide*; Revision/Update Information: August 12 2016; Software Version: PowerBroker Auditor for Active Directory 5.0; Revision Number: 2
  - *PowerBroker Recovery for Active Directory User Guide*; Revision/Update Information: July 15 2016; Software Version: PB Recovery for AD 5.0; Revision Number: 0
- For the UVM50:
  - *UVM Appliance Getting Started Guide*; Revision/Update Information: July 2016; Software Version: UVM Appliance 2.0; Revision Number: 0

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes, which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- TOE Access
- Scanning and Reporting

1.5.2.1 Security Audit

The TOE generates audit records for the startup and shutdown of the audit function. Audit records are also generated for the following components: PBW, BI, PBMS, PBA for AD, PBA for File Systems, and PBA for Exchange. If applicable, administrators are associated to each of the audit records that are generated by their actions within BI. The TOE also limits which administrators have access to the audit logs. BI Administrators with the Audit Viewer

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

permission are able to review all audit records in the User Audit page. While viewing the audit logs, the BI Administrator is able to apply ascending or descending ordering to the displayed columns or a text filter.

1.5.2.2 Identification and Authentication

The TOE allows a BI Administrator to define the number of failed logon attempts a BI Administrator can make on the BI Console UI and R&A UI. Once exceeded, the TOE will lock the account based on the BI Administrator's configuration. The TOE will maintain the following list of security attributes belonging to local BI user accounts: Email Address, User Name, Password, Associated Groups, User Active checkbox, Account Locked checkbox, and Two Factor Authentication settings. The TOE will maintain the following list of security attributes belonging to UVM's Windows user account: User Name and Password. The BI component allows a BI Administrator to define the password requirements for local accounts. The requirements include complexity rules, password history usage, minimum and maximum password length, and timing of password expiration. The UVM component will enforce password complexity requirements on the account passwords that can be reset through its Diagnostics UI. The TOE provides access to the following areas without identification or authentication of a valid administrator account: use of the PBW Policy Monitor and the ability to download the guidance documentation stored in BI. Administrators must successfully identify and authenticate before they are allowed to take any other administrative actions. The TOE utilizes local authentication mechanisms, AD/LDAP[31] authentication mechanisms, RADIUS authentication mechanisms, and Smart Card authentication mechanisms. The TOE obscures the BI Administrator's password using asterisks ("*") in place of each character during authentication to the BI Console UI and bullets ("•") during authentication to the BI R&A UI.

1.5.2.3 Security Management

The Security Management functionality provides the capability for authorized administrators to manage various security functionality provided by the TOE. The TOE will also maintain the BI Administrator, PBMS Administrator, and PBW Administrator roles.

1.5.2.4 Protection of the TSF

The UVM50's OS, which is inside the TOE boundary, will provide the reliable time stamps to the BI and Retina components.

1.5.2.5 TOE Access

Inactive BI Administrator sessions on the BI Console UI and BI R&A UI will be terminated after a 20-minute period of inactivity. The TOE will also allow a BI Administrator to terminate their own interactive session on the BI Console UI and BI R&A UI by providing a logout option. An access banner will be displayed by the TOE when a BI Administrator accesses the BI Console UI and BI R&A UI.

1.5.2.6 Scanning and Reporting

The Scanning and Reporting function performs the collection of data from network devices, analysis of the collected data, and generation of reports based on the analysis. The TOE provides many different collectors, scans, and reports that will perform various analysis on the collected data. During review of the collected data, administrators are able to exports information from the TOE. An administrator can export reports from PBA, policies and translation files from PBW, or reports and asset information from BI. Also during the review of PBA for AD data, the PBMS Administrator can rollback an AD change on modified or deleted AD objects.

[31] LDAP – Lightweight Directory Access Protocol

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.5.3 Product Functionality not Included in the TOE

Features and/or functionality that are not part of the evaluated configuration of the TOE are:

- PBMS web console
- PBMS Remote Server Administration Tools (RSAT) extensions
- PowerBroker Endpoint Protection
- Retina Protection Agent
- PowerBroker Password Safe
- Retina Mobile
- PBW Central Policy mode
- BI Clarity
- BeyondSaaS
- The Silverlight version of the login page to BI's R&A UI
- Use of the Web Console reports in BI's R&A UI

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2. Conformance Claims

This section and Table 3 provide the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 – CC and PP Conformance

CC Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the Common Evaluation Methodology (CEM) as of 09/27/2016 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.2)

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3. Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not administrators: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters, and no physical access to the TOE.
- Administrators: Have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters, and physical access to the TOE. (Administrators are not assumed willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 4 below lists the applicable threats.

Table 4 – Threats

Name	Description
T.CONFIG	An attacker could improperly gain access to TSF data if the product is in an unsecure location, misconfigured, or does not properly identified and authenticated users before enforcing permissions.
T.EXPLOIT	An attacker may attempt to exploit a known vulnerability on a network device to gain access to the TOE.
T.LOSS	An attacker or administrator may modify or cause the loss of AD objects.
T.UNAUTH	An unauthorized administrator may gain access to security data on the TOE, even though the administrator is not authorized in accordance with the TOE security policy.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. Table 5 below lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 5 – Organizational Security Policies

Name	Description
P.ACCESS	Administrators who access the TOE through Microsoft Management Console snap-ins must have Domain or Enterprise administrator access.
P.MANAGE	The TOE may only be managed by authorized administrators.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 6 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 – Assumptions

Name	Description
A.AUTHENTICATE	The TOE environment will provide authentication servers for the identification and authentication of administrators attempting to access the TOE. The TOE environment will also protect communications between the TOE and authentication servers. The authentication servers will support AD, RADIUS and Smart Card authentication.
A.COMMS	The TOE environment will provide secure communications for the PBW, PBA, and PBMS components.
A.INSTALL	The TOE is installed on the appropriate hardware, OS, and runtime environment.
A.LOCATE	The TOE and all components of the TOE environment (including the authentication servers, database server, Exchange server, and administrator workstations) are located within a controlled access facility and appropriately located within the network to perform their functions.
A.NOEVIL	There are one or more competent individuals assigned to manage the TOE, its operating environment, and the security of the information it contains. Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration, and management of the TOE in a secure and trusted manner.
A.OS_AUTH	The TOE environment will provide the identification and authentication of administrators attempting to manage and use the TOE from the Microsoft Management Console.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.TIMESTAMP	The TOE and TOE environment will provide the TOE with the necessary reliable timestamps.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4. Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 7 below.

Table 7 – Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that administrators with the appropriate privileges, and only those administrators, may exercise such control.
O.AUDIT	The TOE must record events of security relevance at the "not specified level" of audit, the resulting actions of the security functional policies, and associate the causing administrator to that event (if applicable). The TOE must also restrict read access of the audit trail to only the authorized administrators with the ability to review the audit trail and provide the ability to apply sorting the audit records.
O.AUTHENTICATE	The TOE must ensure administrators are identified and authenticated prior to allowing access to TOE administrative functions and data except when using parts of the TOE that do not require a login. The TOE must handle failed login attempts in a secure manner and display a logon banner to administrators prior to accessing the BI Console UI and BI R&A UI. The TOE must provide multiple authentication mechanisms, a configurable password policy, obfuscated passwords, and be able to store account attributes.
O.PERMISSION	The TOE must be able to associate administrators with the appropriate permissions after the administrator authenticates.
O.ROLLBACK	The TOE must be able to backup and restore AD objects that have been deleted or modified.
O.SCAN	The TOE must be able to collect information from devices, analyze the information, and generate reports based on the scanning results.
O.SESSION	The TOE must terminate an administrator's session after a defined period of inactivity or after an administrator-initiated session termination.
O.TIMESTAMP	The TOE must provide a reliable timestamps to the BI and Retina components.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 8 below lists the IT security objectives that are to be satisfied by the environment.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 8 – IT Security Objectives

Name	Description
OE.AUTHENTICATOR	The TOE environment will provide authentication servers for the identification and authentication of administrators attempting to access the TOE. Communications with the authentication servers will be protected by the TOE environment.
OE.COMMS	The TOE environment will provide secure communications when the PBW, PBA, and PBMS components communicate with other parts of the TOE or with parts of the TOE environment.
OE.PLATFORM	The TOE environment hardware and OS must support all required TOE functions.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.PERMISSION	The TOE environment will provide administrators accessing the TOE through the Microsoft Management Console snap-ins with the Domain/Enterprise Administrator permissions.
OE.TIMESTAMP	The TOE environment must provide reliable timestamps to the PBW and PBA components.

4.2.2 Non-IT Security Objectives

Table 9 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 9 – Non-IT Security Objectives

Name	Description
NOE.MANAGE	Sites deploying the TOE will provide competent, non-hostile administrators who are appropriately trained and follow all administrator guidance. Administrators will ensure the system is used securely.
NOE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

5. Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 10 identifies all extended SFRs implemented by the TOE.

Table 10 – Extended TOE Security Functional Requirements

Name	Description
EXT_SCR_ANL.1	Analysis
EXT_SCR_RDR.1	Restricted data review
EXT_SCR_SDC.1	System data collection

5.1.1 Class SCR: Scanning and Reporting

Scanning and reporting functions involves collecting information from network devices, analyzing the data for potential vulnerability and compliance to predefined standards, and providing reports on the findings. The EXT_SCR: Scanning and reporting function class was modeled after the CC FAU: Security audit class. The extended family and related components for EXT_SCR_SDC: System data collection were modeled after the CC family and related components for FAU_GEN: Security audit data generation. The extended family EXT_SCR_RDR: Restricted data review was modeled after the CC family FAU_SAR: Security audit review.

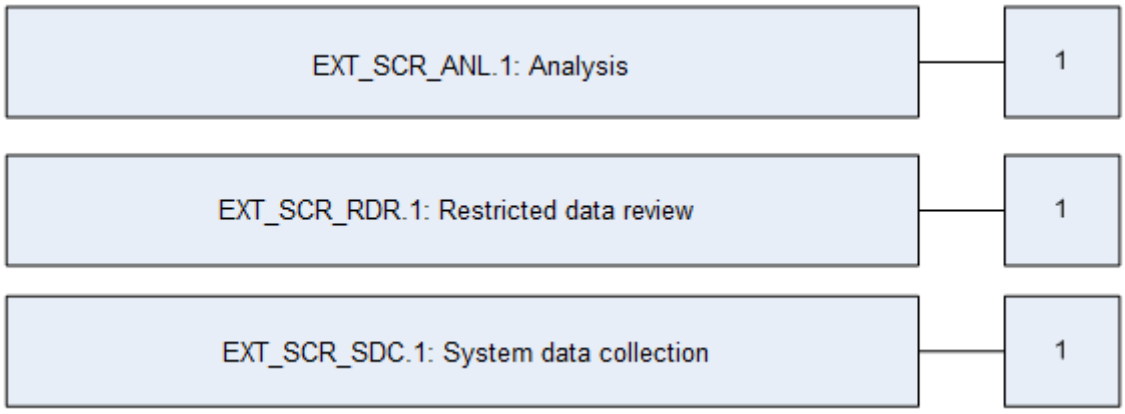

Figure 2 – EXT_SCR: Scanning and Reporting Class Decomposition

5.1.1.1 Analytics (EXT_SCR_ANL)

Family Behavior

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

This family defines the analysis the TOE performs on the collected application and change control data. This family also determines which changes are to be prevented, and which are to be monitored and reported.

Component Leveling

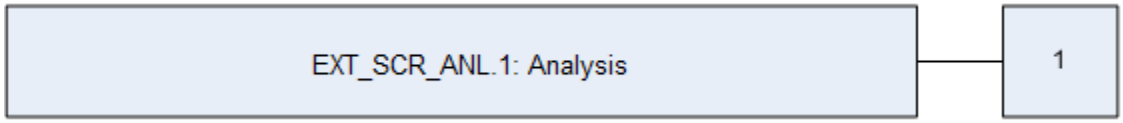

Figure 3 – EXT_SCR: Analytics Family Decomposition

EXT_SCR_ANL.1 Application and change control analysis, specifies the list of analyses the TOE will perform on the collected application data.

Management: EXT_SCR_ANL.1
The following actions could be considered for the management functions in FMT:

- Configuration of the analysis that shall be performed.

Audit: EXT_SCR_ANL.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- There are no audit activities foreseen.

EXT_SCR_ANL.1 Analytics
Hierarchical to: No other components
EXT_SCR_ANL.1.1
The TSF shall perform the following analysis function(s) on the collected data: [assignment: *analytical functions*].
Dependencies: EXT_SCR_SDC.1 System data collection

5.1.1.2 Restricted data review (EXT_SCR_RDR)

Family Behavior

This family defines the requirements for system data tools that should be available to authorized administrators to assist in the review of system data.

Component Leveling

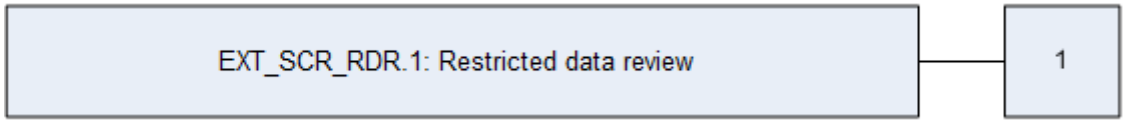

Figure 4 – EXT_SCR Restricted Data Review Family Decomposition

EXT_SCR_RDR.1 Restricted data review, the TSF shall provide the System data in an understandable form only to authorized administrators.

Management: EXT_SCR_RDR.1
The following actions could be considered for the management functions in FMT:

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- Management of the configuration used to generate reports.

Audit: EXT_SCR_RDR.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- There are no audit activities foreseen.

EXT_SCR_RDR.1 Restricted data review
Hierarchical to: No other components
EXT_SCR_RDR.1.1
The TSF shall provide [assignment: *authorized administrators*] with the capability to read [assignment: *list of data*].
EXT_SCR_RDR.1.2
The TSF shall provide the collected data in a manner suitable for the administrator to interpret the information.
EXT_SCR_RDR.1.3
The TSF shall prohibit all administrators read access to the collected data, except those administrators that have been granted explicit read-access.
Dependencies: EXT_SCR_SDC.1 System data collection
EXT_SCR_ANL.1 Analysis
FMT_SMR.1 Security roles

5.1.1.3 System data collection (EXT_SCR_SDC)

Family Behavior

This family defines the requirements for collecting data. This family identifies the level of system data collection, enumerates the types of information that shall be collected by the TSF, and identifies the minimum set of SCR-related information that should be provided within various SCR record types.

Component Leveling

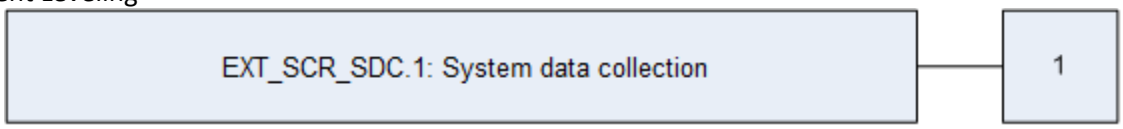

Figure 5 – EXT_SCR: System Data Collection Family Decomposition

EXT_SCR_SDC.1 System data collection, defines the level of information, and specifies the list of data that shall be recorded within the scanning results.

Management: EXT_SCR_SDC.1
The following actions could be considered for the management functions in FMT:

- Configuration of the scanning process

Audit: EXT_SCR_SDC.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- The initialization of the scanning process.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

EXT_SCR_SDC.1 System data collection

Hierarchical to: No other components

EXT_SCR_SDC.1.1

The TSF shall be able to collect the following information from the network device(s): [assignment: *specifically defined information*]

EXT_SCR_SDC.1.2

At a minimum, the TSF shall record the following information: [assignment: *information that shall be recorded*].

Dependencies: FPT_STM.1 Reliable time stamp

5.2 Extended TOE Security Assurance Components

There are no extended TOE security assurance components.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6. Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined text within brackets*].
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_GEN.2	User Identity Association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FAU_SAR.3	Selectable audit review		✓		
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_ATD.1	User attribute definition		✓		
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.1	Timing of authentication		✓		
FIA_UAU.5	Multiple authentication mechanisms		✓		
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.1	Timing of identification		✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_STM.1	Reliable time stamps				

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	S	A	R	I
FTA_SSL.3	TSF-initiated termination		✓		
FTA_SSL.4	User-initiated termination				
FTA_TAB.1	Default TOE access banners				
EXT_SCR_ANL.1	Analytics		✓		
EXT_SCR_RDR.1	Restricted data review		✓		
EXT_SCR_SDC.1	System data collection		✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions;
b. All auditable events, for the [*not specified*] level of audit; and
c. [*The below auditable event types:*
   - *In BI*
     - *Login/Logout*
     - *Add/Edit/Delete*
     - *Enable/Disable*
     - *Update*
     - *Start/Stop/Shutdown/Reset*
   - *In PBMS*
     - *SQL handler events*
     - *PBA management events*
     - *PBA deployment events*

   ].

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

FAU_GEN.2 User identity association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [*BI Administrators with the Audit Viewer permission*] with the capability to read [*All audit information inside BI*] from the audit records.

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1

The TSF shall provide the ability to apply [

- *In the BI Console UI's User Audit page:*
  - *Text filters*
  - *Sort in ascending or descending by column*

] of audit data based on [

- *The following columns in the BI Console UI's User Audits page:*
  - *Action*
  - *Date*
  - *Section*
  - *IP Address*
  - *User Name*

].

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.2 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1

The TSF shall detect when [*a BI Administrator configurable positive integer*] unsuccessful authentication attempts occur related to [*attempted logins to the BI Console UI and R&A UI*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [*Lock the account for a set number of minutes as defined by the BI Administrator*].

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.
Dependencies: No dependencies

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [*Email Address, User Name, Password, Associated Groups, User Active checkbox, Account Locked checkbox, and Two Factor Authentication settings*].

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.
Dependencies: No dependencies

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [

- *The following password requirements within BI for local accounts:*
  - *BI Administrator-defined complexity requirements when creating a password.*
  - *BI Administrator-defined integer for the number of passwords a BI Administrator must create before an old password can be reused.*
  - *BI Administrator-defined integer for the minimum number of characters for the password.*
  - *A maximum limit of 64 characters for the password.*
  - *BI Administrator-defined integer for the maximum number of days before a password must be changed.*
  - *BI Administrator-defined integer for the minimum number of days that a password must be used before it can be changed.*
- *The following password requirements when resetting a password through the UVM Diagnostics UI:*
  - *The password does not contain all or part of the user's account name*
  - *The password is at least fourteen characters in length*
  - *The password is not a previously used password*
  - *The password contains characters from three of the following four categories: Upper case characters, lower case characters, numbers 0-9, non-alphanumeric characters*

].

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

FIA_UAU.1.1

The TSF shall allow [*the following TSF mediated actions:*

- *Download the PDF[32] guides stored in BI*
- *Use of the Policy Monitor on the PBW client machines*

] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UAU.5.1

The TSF shall provide [*the following authentication mechanisms for BI:*

- *Local authentication mechanisms*
- *AD/LDAP authentication mechanisms*
- *Two-factor authentication mechanisms using RADIUS*
- *Smart Card, Common Access Card (CAC), and Personal Identification Verification (PIV) card authentication mechanisms*

] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*following rules:*

- *Local authentication: A BI Administrator sends their BI credentials to the BI Console UI or R&A UI. BI compares the BI Administrator's password to the value stored in the BI Administrator's account information. If they match, the BI Administrator is authenticated and allowed access to the TOE.*
- *AD/LDAP authentication: A BI Administrator sends their BI credentials to the BI Console UI or R&A UI. BI forwards the credentials to the AD/LDAP server. The AD/LDAP server evaluates the credentials and if the username corresponds to a valid domain user and the password matches the stored password, then the AD/LDAP server sends back to BI that the account is authenticated.*
- *Two-factor authentication using RADIUS: A BI Administrator sends their BI credentials (username/password) to the BI Console UI or R&A UI. These credentials are first checked following the local or AD/LDAP authentication method, depending on the account used. If the first check is successful, BI will then send the username, username/password, or username/token to the RADIUS server depending on which setting is used for the RADIUS server. When the options for username/token is chosen, BI will prompt the user to enter their token to be sent to the RADIUS server. The RADIUS server will respond to any request with Accept, Reject, or Challenge. BI acts upon services and services parameters bundled with Accept or Reject.*
- *Smart Card, CAC, and PIV card authentication: The BI Administrator inserts the card into a card reader attached to the workstation. The BI Administrator then navigates to the BI Console UI or R&A UI and chooses their certificate from the displayed list, which is read from the card. Once prompted, the BI Administrator types in their PIN[33]. The browser accesses the card using the provided PIN and validates the BI Administrator's stored certificates against the certificate realm on the network. Once successfully validated, the BI Administrator's username is read from the certificate. If the username is found in AD, the BI Administrator is allowed access to the TOE.*

[32] PDF – Portable Document Format

[33] PIN – Personal Identification Number

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

].

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1

The TSF shall provide only [*asterisks ("*") as feedback when accessing the BI Console UI and bullets ("•") as feedback when accessing the BI R&A UI*] to the user while the authentication is in progress.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UID.1.1

The TSF shall allow [*the following TSF mediated actions:*

- *Download the PDF guides stored in BI*
- *Viewing the Policy Monitor on the PBW client machines*

] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.3 Class FMT: Security Management

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [

- *Manage local BI accounts*
- *Manage organizations within BI*
- *Manage BI services*
- *Manage Retina scan options within BI*
- *Manage patch settings and deployment within BI*
- *Manage BI workgroups*
- *Manage asset information in BI*
- *Manage PBW translations*
- *Manage the PBA Audit Views*
- *Manage protection policies in BI*
- *Manage the PBA Audit Account settings*
- *Manage the PBA audit settings*
- *Manage the PBA agents*
- *Manage the PBA server settings*
- *Manage PBW policies and rules*
- *Manage BI password policy*
- *Manage BI account lockout policy*
- *Manage PBW user messages*

].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [

- *BI Administrator*
- *PBMS Administrator*
- *PBW Administrator*

].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.4 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

Application Note: The UVM50's OS, which is inside the TOE boundary, will provide the reliable time stamps to the BI and Retina components. The operating systems in the environment will provide reliable time stamps to the remaining components.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.5 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [*20-minute period of user inactivity when using the BI Console UI or BI R&A UI*].

FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.4.1

The TSF shall allow user-initiated termination of the user's own interactive session.

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

Application Note: FTA_TAB.1 is enforced by the BI Console UI and BI R&A UI. All other external interfaces are excluded from the scope.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.6 Class SCR: Scanning and Reporting

EXT_SCR_ANL.1 Analytics
Hierarchical to: No other components
Dependencies: EXT_SCR_SDC.1 System data collection

EXT_SCR_ANL.1.1

The TSF shall perform the following analysis function(s) on the collected data: [

- *For Retina:*
  - *Determine if there are any risks or vulnerabilities associated with the scanned device*
  - *List targets that are inaccessible and include a reason*
  - *Analyze all vulnerabilities found*
  - *Provide the vulnerability differences between scans*
  - *Analyze scanned data for trends*
  - *Analyze scanned data for regulatory compliance*
- *For PBMS:*
  - *Determine what data is needed to fulfil the custom Audit View*

].

EXT_SCR_RDR.1 Restricted data review
Hierarchical to: No other components
Dependencies: EXT_SCR_SDC.1 System data collection
EXT_SCR_ANL.1 Analysis
FMT_SMR.1 Security roles

EXT_SCR_RDR.1.1

The TSF shall provide [

- *BI Administrators with either the "Analytics and Reporting" or "Report Management" permissions*
- *PBMS Administrators with Domain/Enterprise Administrator and Audit Accounts permissions*
- *PBMS Administrators with Domain/Enterprise Administrator permissions*

] with the capability to read [

- *Reports generated from the data collected in the Retina scans and from systems monitored by PBW*
- *Audit Views generated from the data collected from the PBA for AD, PBA for SQL, and PBA for Exchange modules*
- *Audit Views generated from the data collected from the PBA for File Systems module*

].

EXT_SCR_RDR.1.2

The TSF shall provide the collected data in a manner suitable for the user to interpret the information.

EXT_SCR_RDR.1.3

The TSF shall prohibit all users read access to the collected data, except those users that have been granted explicit read-access.

EXT_SCR_SDC.1 System data collection
Hierarchical to: No other components
Dependencies: FPT_STM.1 Reliable time stamps

EXT_SCR_SDC.1.1

The TSF shall be able to collect the following information from the network device(s): [

- *In Retina:*

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- *Status of UDP[34] and TCP[35] ports for the target*
- *The operating system for the target*
- *The domain name for the target*
- *The Network Basic Input/Output System (NetBIOS) name for the target*
- *The Media Access Control (MAC) address or unique hardware number*
- *The packet routes across an IP network (traceroute) to the target*
- *List database instances, table, and user information*
- *The hardware for the target*
- *The services and processes running on the target*
- *The software installed on the target*
- *The hotfixes installed on the target*
- *The certificates installed on the target*
- *Lists open and filtered IP protocols*
- *Registry information for the target*
- *User and group information from the target*
- *Information for shares and files on the target*

- *In PBMS:*
  - *In PBA for AD*
    - *AD change events*
    - *Compliance events*
    - *Exchange configuration events*
  - *In PBA for SQL Server*
    - *Deleted/New SQL Server Objects*
    - *SQL Changes*
  - *In PBA for File System*
    - *Changes to files or folders*
    - *Delete/Restore files or folders to/from Recycle Bin*
    - *Open/Read files or folders*
    - *Drive mount/dismount*
  - *In PBA for Exchange*
    - *Exchange configuration activity events*
    - *Mailbox access activity events*
- *In PBW:*
  - *Windows Application events*
  - *Windows Security events*
  - *Windows System events*
  - *PBW Client events*

]

EXT_SCR_SDC.1.2

At a minimum, the TSF shall record the following information: [

- *In Retina:*
  - *Vulnerabilities*
  - *Hardware information*

[34] UDP – User Datagram Protocol
[35] TCP – Transmission Control Protocol

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- *Open port number, protocol, and description*
- *All the running processes, their PIDs[36], and their names*
- *Discovered services and the information about them*
- *Name and description of the shares on the asset*
- *A list of all the software discovered on the asset and the version*
- *Several attributes for a user account including: name, privileges, password age, last logon date, password expiry status, group membership, and status of the account*

- *In PBMS:*
  - *In PBA for AD*
    - *AD change events*
  - *In PBA for SQL Server*
    - *SQL Changes*
  - *In PBA for File System*
    - *Changes to files or folders*
  - *In PBA for Exchange*
    - *Exchange configuration activity events*
- *In PBW:*
  - *PBW Client events*

].

[36] PID – Process Identification

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2+ augmented with ALC_FLR.2. Table 12 summarizes these requirements.

Table 12 – Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC: Life Cycle Support	ALC_CMC.2 Use of a Configuration Management system
	ALC_CMS.2 Parts of the TOE Configuration Management coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7. TOE Security Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 13 lists the security functionality and their associated SFRs.

Table 13 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID[37]	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
Security Management	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functionality	FPT_STM.1	Reliable time stamps
TOE Access	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners
Scanning and Reporting	EXT_SCR_ANL.1	Analytics
	EXT_SCR_RDR.1	Restricted data review
	EXT_SCR_SDC.1	System data collection

[37] ID – Identification

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7.1.1 Security Audit

The TOE generates audit records for the startup and shutdown of all TOE services. Multiple types of audit records are generated for the BI and PBMS components of the TOE.

In BI, user audits are logged for Login, Logout, Add, Edit, Delete, Read, Enable, Disable, Priority Increase, Priority Decrease, Assign, Rename, Save As, Schedule, Pause Job, Resume Job, Delete Job, Reset, Import, Add Vulnerability Exclusion, Remove Vulnerability Exclusion, Copy, Update, Start, Stop, and Shutdown.

In PBMS, events for the SQL handler, managing the PBA Agents, and deploying PBA Agents are logged. The events from the SQL handler are recorded for the configuration and management of the PBA for SQL Server module. Events are also logged for when a PBMS Administrator is managing the PBA Agents from the PBMS UI. The events recorded for the PBA Agent deployment are related to activity when deploying the PBA for Exchange, PBA for AD, and PBA for File System Agents.

Audit events that are captured by BI are associated to the user that caused them if available.

BI Administrators are able to review the audit logs within the BI User Audit page. The TOE also limits which BI Administrators have access to the audit logs by their assigned permissions. Any other BI Administrators trying to access the logs will be denied. BI Administrators accessing BI with the Audit Viewer permission can view the User Audits and Services logs through the BI Console UI.

While viewing the BI User Audits page, the BI Administrator is able to apply ascending or descending ordering to the displayed columns or a text filter. The displayed columns in the BI Console UI's User Audits page include the following:

- Section – A grouping of events with a general name
- Action – The specific action taken for the event type in Section
- User Name – The user name of the administrator that caused the event
- Date – The data and time that the event took place
- IP Address – The IP address of the system that caused the event

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, and FAU_SAR.3.

7.1.2 Identification and Authentication

A BI Administrator may define the number of failed logon attempts for the BI Console UI and R&A UI. The value can be from 0 to 999. A value of five for the failed logon attempts will be recommended in the guidance documentation. Once the value is met, the TOE will take action based on the configuration setup by the BI Administrator. A BI Administrator can also configure the number of minutes the account will be locked. A lockout time of 15 minutes will be recommended in the guidance documentation.

The TOE maintains a list of security attributes belonging to each local BI account. Each record contains the security attributes for the account including email address, user name, user active checkbox, account locked checkbox, password, associated groups, and two-factor authentication settings. Under the two-factor authentication settings section, BI Administrators will find settings for the "Two Factor Authentication" and "Map Two Factor

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

User" options. Two Factor Authentication has two selectable values: RADIUS or none. If RADIUS is selected, the Map Two Factor User dropdown becomes available. If RADIUS is used on a local account, the selectable values are "As Logged In" or "Manually Specified". If RADIUS is used on an AD account, the selectable values are "Manually Specified", "Alternate Directory Attribute", "Distinguished Name", "User Principal Name", "SAM[38] Account Name", or "Domain\User Name". The TOE will also maintain the username and password security attributes that belong to the UVM's Windows account.

Local password requirements can be enforced by the TOE. The TOE allows BI Administrators to require accounts to adhere to complex password rules when creating a password. The BI Administrator can set the number of unique new passwords that must be associated with an account before an old password can be reused. After the defined number has been exceeded, the old password may be used again. Otherwise, the TOE will require the use of a new password. A BI Administrator can set the minimum password length that must be used for creating new passwords. A minimum password length of eight characters will be recommended in the guidance documentation. The maximum length for a local password is 64 characters. Any characters after the 64th will be truncated from the password. The BI Administrator also has options to set the minimum and maximum password age. When setting the minimum password age, the password must be used for that amount of time before it can be changed. When settings the maximum password age, the password will require the BI Administrator to set a new password once the age limit has been met. When resetting passwords through the UVM's Diagnostics UI, the TOE will require passwords to conform to the following complexity requirements:

- Does not contain all or part of the user's account name
- Is at least fourteen characters in length
- Is not a previously used password
- Contains characters from three of the following four categories:
    - English upper case characters (A-Z)
    - English lower case characters (a-z)
    - Base 10 digits (0-9)
    - Non-alphanumeric (For example, !,$#,%)

The TOE provides limited access to the TSF-mediating functionality without identification or authentication of a valid administrator account. The TOE allows users to download copies of the stored guidance documentation by directly linking to the saved files on the BI server. A user with access to the PBW client that is installed locally on their machine may access the Policy Monitor to view information about the system's processes and details about rule operations. The Policy Monitor can also be used to troubleshoot problems when a rule does not function as expected.

When an administrator accesses the components of the TOE using the Microsoft Management Console (PBMS UI and PBW Editor UI), the TOE relies on the underlying OS to authenticate the administrator. Once the administrator is authenticated by the OS, the TOE will check their account for the appropriate permissions to access the TOE components and features.

The TOE utilizes local authentication mechanisms, AD/LDAP authentication mechanisms, two-factor authentication with RADIUS mechanisms, and Smart Card/CAC/PIV card authentication mechanisms. Local authentication into BI is only available when a BI Administrator creates an account inside the BI Console UI.

[38] SAM – Security Account Manager

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Local authentication works by sending the authenticating account's credentials over the BI Console UI or R&A UI to the BI server. The BI server compares the entered credentials with the stored credentials. The entered username and password must match the stored information or an error is returned. If the two sets of credentials match, the BI Administrator is authenticated and allowed access to the TOE. Local authentication for the UVM also uses the same method for the Diagnostics UI.

The AD/LDAP authentication uses an AD/LDAP server to verify account information. The BI Console UI and R&A UI use an account-based AD/LDAP authentication method that works like the local authentication method. The BI Administrator's credentials are passed through the BI Console UI or R&A UI to the BI server that verifies them with the AD/LDAP server. The AD/LDAP server evaluates the BI Administrator's credentials. If the username corresponds to a valid domain user and the password matches the stored password, then the BI Administrator is authenticated and allowed access to the TOE. When accessing the PBW Editor UI, PBMS UI, and PBA modules, the administrator's access is based on their AD/LDAP permissions. The administrator launches one, either the PBW Editor UI or PBMS UI, from the Windows Server. Their permissions are verified with AD/LDAP based on the logged on account. If their account has the appropriate permissions, the application is opened without error. If their account is underprivileged, the TOE will prompt an error noting that access was denied.

Two-factor authentication with RADIUS can also be setup for the BI Console UI and R&A UI. The RADIUS authentication works when an account designated to use the RADIUS authentication method sends their credentials (username/password) to the BI server using the BI Console UI or R&A UI. These credentials are first checked following the local or AD/LDAP authentication method, depending on the account used. If the first check is successful, BI will then send either the username, username/password, or username/token to the RADIUS server for verification. When the options for username/token is chosen, BI will prompt the user to enter their token to be sent to the RADIUS server. The RADIUS server may be setup to interpret the token for multiple ways of verifying the user's identity including the use of text messaging, automated phone call, smart phone applications, or hard/soft tokens. The RADIUS server responds with Accept, Reject, or Challenge. BI acts upon services and services parameters bundled with Accept or Reject.

The final authentication method that the TOE offers is Smart Card, CAC, and PIV card authentication. All three cards work in the same manner; the cards are only physically different. The network must already be setup for this method of authentication. The cards, certificates, and PINs will be managed by the environment. Each account that requires Smart Card authentication access needs to be designated to use Smart Cards in the BI Console UI before the TOE will correctly work with them. Once set, the BI Administrator inserts the card into a card reader attached to the workstation. The BI Administrator then navigates to the BI Console UI or R&A UI and chooses their certificate from the displayed list. The BI Administrator is then prompted to type in their PIN. The browser accesses the card using the provided PIN and validates the BI Administrator's stored certificates against the certificate realm on the network. Once successfully validated, the BI Administrator's username is read from the certificate. If the username is found in AD, the BI Administrator is allowed access to the TOE.

The TOE obscures the BI Administrator's password using asterisks ("*") in place of each character during authentication to the BI Console UI and bullets ("•") when authenticating to the BI R&A UI.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.7, and FIA_UID.1.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7.1.3 Security Management

The TOE maintains a list of roles and permissions that are assigned to administrators after authentication. A BI Administrator, PBMS Administrator, or PBW Administrator is an administrator to which one or more permission is assigned. The permissions are described below:

- BI Administrator permissions:
  - Analytics and Reporting – Used to sign in to BI, generate reports, and subscribe to reports.
  - Asset Management – Used to create Smart Rules, edit or delete on the Asset Details window, create AD queries, and create address groups.
  - Attribute Management – Used to add, rename, or delete attributes when managing user groups.
  - Audit Management – Provides access to Audit Manager Tab under configuration
  - Audit Viewer – Used to access the Audit Viewer in the BI R&A UI.
  - Benchmark Compliance – Configure and run benchmark compliance scans.
  - BeyondInsight Login – Access the BeyondInsight management console.
  - Credential Management – Add and change credentials when running scans and deploying policies.
  - Dashboard – Provides access to the dashboard within the BI Console UI
  - Deployment – Activate the Deploy button.
  - File Integrity Monitoring – Work with File Integrity rules.
  - License Reporting – Provides access to the Licensing folder in the R&A UI
  - Manual Range Entry – Allows the user to manually enter ranges for scans and deployments rather than being restricted to Smart Groups.
  - Option Management – Change the application options settings (such as, account lockout and account password settings).
  - Patch Management – Use Patch Management module.
  - PowerBroker for Windows – Activates access to the PBW features, including PBW asset details and the exclusions page on the Configure tab.
  - Protection Policy Management – Activate the Protection Policy feature.
  - Reports Management – Run scans, create reports, create report category.
  - Scan - Audit Groups – Create, delete, update, and revert Audit Group settings.
  - Scan - Job Management – Activate Scan and Start Scan buttons.
  - Scan - Policy Manager – Activate the settings on the Edit Scan Settings view.
  - Scan - Port Groups – Create, delete, update, and revert Port Group settings.
  - Scan - Report Delivery – Create and edit email subscription to scan reports.
  - Scan Management – Delete, edit, duplicate, and rename reports on the Manage Report Templates. Activate New Report and New Report Category. Activate Update button on the Edit Scan Settings view.
  - Session Monitoring – Use the Session Monitoring features.
  - Ticket System – View and use the ticket system.
  - Ticket System Management – Mark a ticket as Inactive. The ticket no longer exists when Inactive is selected.
  - User Accounts Management – Add, delete, or change user groups and user accounts.
  - User Audits – View the User Audits window on the Configure tab to display audit details for BeyondInsight users.
  - Vulnerability Exclusions – Select to prevent users from setting exclusions.
- PBMS Administrator permissions:
  - Audit Accounts – Accessing the Audit Viewer UI. Viewing, exporting, and running audit views on stored audit records.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

  - Domain/Enterprise Administrator – Accessing and configuring the PBA modules excluding the areas that the Audit Accounts permissions cover.
- PBW Administrator permissions:
  - Domain/Enterprise Administrator – Accessing and configuring the PBW Editor UI.

The TOE provides access within BI to manage local accounts, organizations, services, Retina scan options, patch settings, workgroups, asset information, the password policy, the account lockout policy, and protection policies. Management functionality is also provided in the PBA modules for Audit Account settings, audit settings, Audit Views, agents, and server settings. Finally, using PBW Policy Editor, the TOE provides management access to the PBW policies and rules, PBW user messages, and PBW translations.

TOE Security Functional Requirements Satisfied: FMT_SMF.1, and FMT_SMR.1.

7.1.4 Protection of the TSF

The Windows 2012 R2 OS that is running on the UVM50, which are both inside the TOE boundary, will provide the reliable time stamps to the BI and Retina components for their auditing and scanning needs. The time on the UVM50 may be set manually or synchronized with an NTP server.

TOE Security Functional Requirements Satisfied: FPT_STM.1.

7.1.5 TOE Access

Inactive sessions will be terminated by the TOE after 20 minutes of inactivity on the BI Console UI and BI R&A UI.

A session can be terminated manually by the accessing BI Administrator. The TOE provides a logout option in the BI Console UI and BI R&A UI to manually end the current session. Once the session has been terminated, the BI Administrator is required to re-authenticate before they can access the functionality inside the BI Console UI or BI R&A UI.

When navigating to the BI Console UI or BI R&A UI, a BI Administrator will be prompted with an access banner. The access banner can be configured with a custom title and message to provide the authenticating BI Administrator with usage information for the TOE. Settings for the access banner are found in the Application Options of the BI Console UI. Any user that loads the BI Console UI will be presented with the access banner automatically.

TOE Security Functional Requirements Satisfied: FTA_SSL.3, FTA_SSL.4, and FTA_TAB.1.

7.1.6 Scanning and Reporting

The Scanning and Reporting function performs the collection of data from network devices, analysis of the collected data, and generation of reports based on the analysis. The TOE provides the following basic information, if available, from devices that are scanned or monitored for analysis:

- In Retina:
  - Vulnerabilities

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

    - Hardware information
    - Open port number, protocol, and description
    - All the running processes, their PIDs[39], and their names
    - Discovered services and the information about them
    - Name and description of the shares on the asset
    - A list of all the software discovered on the asset and the version
    - Several attributes for a user account including: name, privileges, password age, last logon date, password expiry status, group membership, and status of the account
- In PBMS:
    - In PBA for AD
        - AD change events
    - In PBA for SQL Server
        - SQL Changes
    - In PBA for File System
        - Changes to files or folders
    - In PBA for Exchange
        - Exchange configuration activity events
- In PBW:
    - PBW Client events

Retina scans can be configured by a BI Administrator to provide more information from the scanned devices. When the BI Administrator configures the Scan Policy options, they can choose what to display from the following:

- The operating system for the target
- The domain name for the target
- The NetBIOS name for the target
- The MAC address or unique hardware number
- The packet routes across an IP network (traceroute) to the target
- List database instances, table, and user information
- The hardware for the target
- The services running on the target
- The software installed on the target
- The certificates installed on the target
- Lists open and filtered IP protocols

Another area of Retina that provides more scan settings is the Audit Group settings. BI Administrators can create an audit that addresses particular risks or vulnerabilities that can be used to protect their assets. The Audit Group settings include information for the following:

- Registry
- Users
- Shares
- Files
- Hotfixes
- Named pipes
- Machine information
- Audit policy

[39] PID – Process Identifier

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- Per-user registry settings
- Groups
- Processes
- User and group privileges
- Software

BI Administrators can configure Retina's scanned port ranges or use a Port Group to show the status of UDP or TCP ports. Through the Advanced options, BI Administrators can configure settings to retrieve data on the port, operating system, and protocol scanned. The Advanced options can also show details about the vulnerabilities that are open, fixed, or not verified. Using the Retina Local Scan Service options, BI Administrators may choose to deploy a local Retina agent on a device to enumerated local ports, which includes active connections and the program or service using the port.

In PBMS, the different PBA modules log data for the servers that they monitor. In PBA for AD, AD events for Computer Changes, Container Changes, FRS[40] Changes, GPO[41] Changes, Group Changes, Infrastructure Changes, OU[42] Changes, Printer Changes, and User Changes are logged. For compliance events in AD, there are FISMA[43], HIPAA[44], PCI, and SOX[45] events that are logged. For Exchange events in AD, the event types of Administrative Group, Organization Configuration, and Server Configuration are logged.

In PBA for SQL Server, events for Deleted SQL Server Objects, Function Changes, Index Changes, Modified SQL Server Objects, Newly Created SQL Server Objects, Procedure Changes, Server Instance Changes, Server Role Changes, User Changes, and View Changes are logged.

In PBA for File System, events for Write data to files, Create/Delete files or folders, Set attributes on files or folders, Modify permissions on files or folders, Delete/Restore files or folders to/from Recycle Bin, Open files or folders, Read data from files, drive mount, drive dismount, and rename file or folder.

In PBA for Exchange, events for Exchange configuration activity are logged for Address list changes, Address lists added/removed, Configuration changes, Email address policies added/removed, Email address policy changes, Mailbox delegations, Mailbox quota changes, Protocol changes, and Storage group changes. Mailbox access events are also logged for Read/Rename/Create/Delete/Recycle/Copy/Move/Empty a folder, Recycle/Delete/Create/Update/Move/Copy/Read an item, send a message, mark a message as read/unread, and open a mailbox.

When Event Monitoring is configured in the PBW Editor UI, the PBW will collect Windows events from the host machine. Windows Application events, Security events, or System events can be collected and forwarded to BI for storage and later analysis. After event forwarding is configured for the PBW client, the PBW client will collect data about the actions that it takes and forwards them to BI.

[40] FRS – File Replication Service
[41] GPO – Group Policy Object
[42] OU – Organizational Unit
[43] FISMA – Federal Information Security Management Act
[44] HIPAA – Health Insurance Portability and Accountability Act
[45] SOX – Sarbanes-Oxley

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Once the data has been collected from the scanned devices or PBW, Retina will analyze it to determine if there are any risks or vulnerabilities associated with the device. The analysis will determine if a target is inaccessible, why it is inaccessible, and list all the vulnerabilities that are found. The vulnerability information includes the PCI DSS[46] score and any stored personally identifiable information. Once the data has been collected from the monitored devices, a PBMS Administrator can use an existing Audit View, or configure a custom one, to view the stored data. The Audit View will be used to analyze the data to determine what should be displayed to fulfil the current request.

When multiple sets of scanned data have accumulated from Retina scans, the TOE can analyze the data for trends, differences between scans, or for regulatory compliance. The TOE is able to analyze the scanned data for regulatory compliance in the following areas:

- Control Objectives for Information and Related Technology (COBIT) Compliance
- Federal Energy Regulatory Commission – North American Electric Reliability Corporation (FERC-NERC)
- Gramm-Leach-Bliley Act (GLBA) Compliance
- HIPAA Compliance
- Health Information Trust Alliance (HITRUST) Compliance
- International Organization for Standardization (ISO)-27002 Compliance
- Information Technology Infrastructure Library (ITIL) Compliance
- Mass 201 Code of Massachusetts Regulations (CMR) 17 Compliance
- NIST 800-53
- SOX Compliance

After the data has been collected and analyzed from the Retina scans, reports can be generated by a BI Administrator. The reports are limited to BI Administrators with either the “Analytics and Reporting” or “Report Management” permission. BI Administrators without the needed permissions will not be able to run or view the reports’ data. Using the generated reports to view the analytical data provides the BI Administrator with a suitable way to interpret the information.

After the data has been collected and analyzed from the PBA monitored servers, reports can be generated by a PBMS Administrator. The reports from the PBA for AD, PBA for SQL, and PBA for Exchange modules are limited to PBMS Administrators with Domain/Enterprise Administrator and Audit Accounts permissions. The reports from the PBA for File Systems module are limited to PBMS Administrators with Domain/Enterprise Administrator permissions. PBMS Administrators without the needed permissions will not be able to run or view the reports’ data. Using the generated reports to view the monitored data provides the PBMS Administrator with a suitable way to interpret the information.

While viewing any of the Audit Views, the PBMS Administrator is able to apply ascending or descending ordering to the displayed columns or a text filter. Within the Audit Viewer UI, the collected data can be grouped together based on the records’ Event Type.

In the PBA for SQL Audit Viewer UI, the displayed columns include the following:

- Date and Time – The data and time that the event took place
- Event – The recorded event type
- Server – The SQL server that caused the event
- Database – The database on the SQL server that was involved in the event

[46] DSS – Data Security Standard

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- Object Name – The object name inside the database that was involved in the event
- Login – The account of the user that caused the event on the SQL server

In the PBA for File System Audit Viewer UI, the displayed columns include the following:

- Date and Time – The data and time that the event took place
- Event – The recorded event type
- User – The account of the user that caused the event on the server
- Process – The name of the process used to cause the event, i.e., notepad.exe
- Attributes – The file system attributes of the file/folder when changed. Possible values are: Archive, Compressed, Directory, Encrypted, Hidden, Normal, Not Indexed, Offline, Read-only, Reparse point, Sparse file, System, Temporary.

In the PBA for Exchange Audit Viewer UI, the displayed columns include the following:

- Date and Time – The data and time that the event took place
- Event – The recorded event type
- Server – The Exchange server that caused the event
- Mailbox – The mailbox on the Exchange server that was involved in the event
- User – The account of the user that caused the event on the server
- Item Name – The folder/object within the mailbox that was involved in the event
- Setting – The setting for the mailbox/user that was involved in the event

In the PBA for AD Audit Viewer UI, the displayed columns include the following:

- Date and Time – The data and time that the event took place
- Action – The type of action taken on the object
- Object – The AD Object that was involved in the event
- Type – The recorded event type
- Modified By – The account of the user that caused the event on the server
- Attribute – The name of the attribute that was involved in the event
- New Value – The new value set to the attribute
- Old Value – The old value of the attribute before it was changed

While reviewing the collected data from the PBA for AD module, the PBMS Administrator is able to rollback AD data. The rollback can be performed on any modified or deleted AD objects that has previously been collected by the configured collector and are still within the purge limits. Objects that can be rolled back include AD objects in the current domain/forest, AD objects in another forest, Group Policy Objects, configuration naming context data, and schema naming context data.

While reviewing the PBW reports in BI, a BI Administrator is able to apply ascending or descending ordering to the displayed columns. The displayed columns in the Event Details report include the following:

- Application – The name of the application
- Asset Name – The name of the workstation
- Message – A description of why the event occurred
- User Name – The username of the causing user
- Occurrence Time Range – Date and time of the event (can be a range if the Occurrences column is higher than 1)
- Process Type – The level of access used to launch the application

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- Occurrences – Counts the number of times this event occurred. If clicked, more information is provided per event.

The displayed columns in the Event Rollup report include the following:

- Event Message – A description of why the event occurred
- Application Name – The name of the application
- Asset – The name of the workstation
- Rule Type – Shows the type of rule used in PBW associated to the event
- Date Range of Occurrences – Date of the event (can be a range if the Occurrences column is higher than 1)
- Exclusionary? – Counts the occurrences that are excluded from PBW rules
- Occurrences – Counts the number of times this event occurred. If clicked, more information is provided per event including the occurrence time.

While reviewing collected data, an administrator may export a copy of the records from the TOE. Using the BI Console UI, reports based on Retina scans and PBW data can be exported from the Reports tab, Reports section of the Job tab, or Report Viewer page. In addition, asset and vulnerability data may be exported using the BI Console UI. Using the R&A UI, reports based on Retina scans and PBW data can be exported after they have successfully ran. Using the Audit Viewer UI for PBA for AD/SQL/Exchange/File Systems, a PBMS Administrator may export the collected data to .XML or .PDF files.

TOE Security Functional Requirements Satisfied: EXT_SCR_ANL.1, EXT_SCR_RDR.1, and EXT_SCR_SDC.1.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 extended and Part 3 conformant of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Release 4.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 14 below provides a mapping of the objectives to the threats they counter.

Table 14 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.CONFIG An attacker could improperly gain access to TSF data if the product is in an unsecure location, misconfigured, or does not properly identified and authenticated users before enforcing permissions.	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile administrators who are appropriately trained and follow all administrator guidance. Administrators will ensure the system is used securely.	The objective NOE.MANAGE ensures that administrators are competent, non-hostile, follow all administrator guidance, and will use the TOE securely.
	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	The objective NOE.PHYSICAL ensures that the environment is a secure setting that would deter attackers from gaining access to the TOE.
	O.AUTHENTICATE The TOE must ensure administrators are identified and authenticated prior to allowing access to TOE administrative functions and data except when using parts of the TOE that do not require a login. The TOE must handle failed login attempts in a secure manner and display a logon banner to administrators prior to accessing the BI Console UI and BI R&A UI. The TOE must provide multiple authentication mechanisms, a configurable password policy, obfuscated passwords, and be able to store account attributes.	By ensuring that administrators are identified and authenticated prior to accessing the TOE administrative functions and data, O.AUTHENTICATE satisfies this threat.
	O.PERMISSION The TOE must be able to associate administrators with the appropriate permissions after the administrator authenticates.	O.PERMISSION supports the mitigation of this threat by assigning permissions to administrators when they authenticate to the TOE.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
T.EXPLOIT An attacker may attempt to exploit a known vulnerability on a network device to gain access to the TOE.	O.SCAN The TOE must be able to collect information from devices, analyze the information, and generate reports based on the scanning results.	O.SCAN ensures that the TOE will scan and detect vulnerabilities on scanned devices to help administrators fix any open vulnerabilities before they can be used to gain access to the TOE. O.SCAN also ensures that monitored devices will have their data collected for analysis and report generation.
T.LOSS An attacker or administrator may modify or cause the loss of AD objects.	O.ROLLBACK The TOE must be able to backup and restore AD objects that have been deleted or modified.	O.ROLLBACK ensures that the TOE will have a way to rollback changes to AD objects or be able to recover deleted AD objects.
T.UNAUTH An unauthorized administrator may gain access to security data on the TOE, even though the administrator is not authorized in accordance with the TOE security policy.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that administrators with the appropriate privileges, and only those administrators, may exercise such control.	O.ADMIN supports the mitigation of this threat by ensuring that only authorized administrators may configure the TOE security mechanisms.
	O.AUDIT The TOE must record events of security relevance at the “not specified level” of audit, the resulting actions of the security functional policies, and associate the causing administrator to that event (if applicable). The TOE must also restrict read access of the audit trail to only the authorized administrators with the ability to review the audit trail and provide the ability to apply sorting the audit records.	The objective O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE is protected from external interference or tampering.
	O.PERMISSION The TOE must be able to associate administrators with the appropriate permissions after the administrator authenticates.	O.PERMISSION supports the mitigation of this threat by assigning permissions to administrators when they authenticate to the TOE.
	O.SESSION The TOE must terminate an administrator’s session after a defined period of inactivity or after an administrator-initiated session termination.	O.SESSION supports the mitigation of this threat by terminating an administrator's session after 20 minutes of inactivity and by allowing administrators to terminate their own session before an attacker can gain access to their inactive session.
	O.TIMESTAMP The TOE must provide a reliable timestamps to the BI and Retina components.	O.TIMESTAMP ensures that the auditing functionality of the BI and Retina components use the timestamp provided the UVM50 appliance for all BI Administrators accessing security relevant functionality.

Every threat is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8.2.2 Security Objectives Rationale Relating to Policies

Table 15 below gives a mapping of policies and the objectives that support them.

Table 15 – Policies: Objectives Mapping

Policies	Objectives	Rationale
P.ACCESS Administrators who access the TOE through Microsoft Management Console snap-ins must have domain or enterprise administrator access.	O.AUTHENTICATE The TOE must ensure administrators are identified and authenticated prior to allowing access to TOE administrative functions and data except when using parts of the TOE that do not require a login. The TOE must handle failed login attempts in a secure manner and display a logon banner to administrators prior to accessing the BI Console UI and BI R&A UI. The TOE must provide multiple authentication mechanisms, a configurable password policy, obfuscated passwords, and be able to store account attributes.	O.AUTHENTICATE ensures that administrators are able to access the TOE on the Microsoft Management Console snap-ins before being authenticated.
	OE.PERMISSION The TOE environment will provide administrators accessing the TOE through the Microsoft Management Console snap-ins with the Domain/Enterprise Administrator permissions.	OE.PERMISSION ensures that administrators have the appropriate AD permissions when accessing the TOE.
P.MANAGE The TOE may only be managed by authorized administrators.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that administrators with the appropriate privileges, and only those administrators, may exercise such control.	O.ADMIN ensures that the TOE provides the necessary tools to support the P.MANAGE policy.
	O.AUTHENTICATE The TOE must ensure administrators are identified and authenticated prior to allowing access to TOE administrative functions and data except when using parts of the TOE that do not require a login. The TOE must handle failed login attempts in a secure manner and display a logon banner to administrators prior to accessing the BI Console UI and BI R&A UI. The TOE must provide multiple authentication mechanisms, a configurable password policy, obfuscated passwords, and be able to store account attributes.	O.AUTHENTICATE ensures that only authorized administrators are granted access to the tools required to manage the TOE.

Every policy is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 16 below gives a mapping of assumptions and the environmental objectives that uphold them.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 16 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.AUTHENTICATE The TOE environment will provide authentication servers for the identification and authentication of administrators attempting to access the TOE. The TOE environment will also protect communications between the TOE and authentication servers. The authentication servers will support AD, RADIUS and Smart Card authentication.	OE.AUTHENTICATOR The TOE environment will provide authentication servers for the identification and authentication of administrators attempting to access the TOE. Communications with the authentication servers will be protected by the TOE environment.	OE.AUTHENTICATOR satisfies the assumption that the TOE environment will provide the different authentication servers for administrators authenticating with the TOE that will protect the exchanged communications.
A.COMMS The TOE environment will provide secure communications for the PBW, PBA, and PBMS components.	OE.COMMS The TOE environment will provide secure communications when the PBW, PBA, and PBMS components communicate with other parts of the TOE or with parts of the TOE environment.	OE.COMMS upholds the assumption that the underlying OS, which is in the TOE environment, will provide secure communications for the PBW, PBA, and PBMS components when they communicate with other parts of the TOE or with parts of the TOE environment.
A.INSTALL The TOE is installed on the appropriate, dedicated hardware, OS, and runtime environment.	OE.PLATFORM The TOE environment hardware and OS must support all required TOE functions.	OE.PLATFORM satisfies the assumption that the hardware and operating systems in the TOE environment will be able to support the TOE components.
	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL satisfies the assumption that the TOE environment will be to securely support the TOE.
A.LOCATE The TOE and all components of the TOE environment (including the authentication servers, database server, Exchange server, and administrator workstations) are located within a controlled access facility and appropriately located within the network to perform their functions.	OE.AUTHENTICATOR The TOE environment will provide authentication servers for the identification and authentication of administrators attempting to access the TOE. Communications with the authentication servers will be protected by the TOE environment.	OE.AUTHENTICATOR satisfies the assumption that the TOE environment will provide the different authentication servers that are located within the same network.
	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL satisfies the assumption that the TOE environment will be able to securely support the TOE and that it is located appropriately to allow the TOE to perform its functions.
A.NOEVIL There are one or more competent individuals assigned to manage the TOE, its operating environment, and the security of the information it contains. Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration, and management of the TOE in a secure and trusted manner.	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile administrators who are appropriately trained and follow all administrator guidance. Administrators will ensure the system is used securely.	NOE.MANAGE satisfies the assumption that the administrators who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Assumptions	Objectives	Rationale
A.OS_AUTH The TOE environment will provide the identification and authentication of administrators attempting to manage and use the TOE from the Microsoft Management Console.	OE.AUTHENTICATOR The TOE environment will provide authentication servers for the identification and authentication of administrators attempting to access the TOE. Communications with the authentication servers will be protected by the TOE environment.	OE.AUTHENTICATOR satisfies the assumption that the TOE environment will provide the different authentication servers for administrators authenticating with the TOE.
	OE.PLATFORM The TOE environment hardware and OS must support all required TOE functions.	OE.PLATFORM satisfies the assumption that the hardware and operating systems in the TOE environment will be able to support the TOE components.
	OE.PERMISSION The TOE environment will provide administrators accessing the TOE through the Microsoft Management Console snap-ins with the Domain/Enterprise Administrator permissions.	OE.PERMISSION satisfies the assumption that the TOE environment will provide administrators accessing the TOE through the Microsoft Management Console snap-ins with the Domain/Enterprise Administrator permissions.
A.PROTECT The TOE software will be protected from unauthorized modification.	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL ensures that the TOE's IT environment protects the TOE from interference and tampering by untrusted subjects.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
A.TIMESTAMP The TOE and TOE environment will provide the TOE with the necessary reliable timestamps.	OE.TIMESTAMP The TOE environment must provide reliable timestamps to the PBW and PBA components.	OE.TIMESTAMP upholds this assumption by ensuring that the operating system where the TOE is installed will provide reliable time stamps for the PBW and PBA components.

Every assumption is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

A family of EXT_SCR requirements was created to specifically address the TOE's ability to scan devices, analyze the scanned data, and report the detected vulnerabilities. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements involves collecting information from scanned devices, analyzing the data for potential vulnerability and compliance to predefined standards, and providing reports on the findings. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no Extended TOE Security Assurance Requirements.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 17 below shows a mapping of the objectives and the SFRs that support them.

Table 17 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that administrators with the appropriate privileges, and only those administrators, may exercise such control.	FIA_AFL.1 Authentication failure handling	The requirement meets the objective by ensuring that authentication failure thresholds may only be changed by authorized administrators.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that administrators are associated to permissions before they can access TSF management functions and data.
O.AUDIT The TOE must record events of security relevance at the “not specified level” of audit, the resulting actions of the security functional policies, and associate the causing administrator to that event (if applicable). The TOE must also restrict read access of the audit trail to only the authorized administrators with the ability to review the audit trail and provide the ability to apply sorting the audit records.	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User Identity Association	The requirement meets this objective by ensuring that the TOE associates an administrator to each auditable event that the administrator caused within the BI component.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensure that the TOE provides the ability to review logs within the BI component.
	FAU_SAR.2 Restricted audit review	The requirement meets the objective by ensuring that the TOE restricts read access to the audit records to administrators that have been granted explicit read-access within the BI component.
	FAU_SAR.3 Selectable audit review	The requirement meets the objective by ensuring that the TOE provides the ability to sort audit records based on the column headers within the BI component’s User Audit page.
	FPT_STM.1 Reliable time stamps	The requirement meets the objective by ensuring that the TOE provides a reliable timestamp for the BI and Retina components.
O.AUTHENTICATE The TOE must ensure administrators are identified and authenticated administrators prior to allowing access to TOE administrative functions and data except when using parts of the TOE that do not require a login. The TOE	FIA_AFL.1 Authentication failure handling	In order to ensure that administrators are properly authenticated prior to access, the TOE enforces a lockout after a configurable number of unsuccessful authentication attempts. The requirement for authentication failure handling meets the objective by mitigating the risk of a brute force attack on a username and password.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
must handle failed login attempts in a secure manner and display a logon banner to administrators prior to accessing the BI Console UI and BI R&A UI. The TOE must provide multiple authentication mechanisms, a configurable password policy, obfuscated passwords, and be able to store account attributes.	FIA_ATD.1 User attribute definition	The requirement meets the objective by ensuring that security attributes may only be changed by authorized administrators.
	FIA_SOS.1 Verification of secrets	The process that identifies and authenticates administrators also enforces an administrator configured password policy. This requirement meets the objective by mitigating the risk of a brute force attack on a username and password.
	FIA_UAU.1 Timing of authentication	The requirement meets the objective by ensuring that administrators are authenticated before access to TOE administrative functions is allowed, except when resetting a BI password, accessing BI guidance documentation, or viewing the PBW Policy Monitor.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by ensuring that the TOE provides administrators with multiple authentication mechanisms.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by ensuring that the TOE will obfuscate the password during authentication.
	FIA_UID.1 Timing of identification	The requirement meets the objective by ensuring that administrators are identified before access to TOE administrative functions is allowed, except when resetting a BI password, accessing BI guidance documentation, or viewing the PBW Policy Monitor.
	FTA_TAB.1 Default TOE access banners	The requirement meets the objective by ensuring that administrators are prompted with an access banner when attempting to authenticate to the BI Console UI and BI R&A UI.
O.PERMISSION The TOE must be able to associate administrators with the appropriate permissions after the administrator authenticates.	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates administrators with permissions to provide access to TSF management functions and data.
O.ROLLBACK The TOE must be able to backup and restore AD objects that have been deleted or modified.	EXT_SCR_RDR.1 Restricted data review	The requirement meets this objective by ensuring that the TOE will provide an administrator with the means necessary to restore AD objects during the review of collected data.
	EXT_SCR_SDC.1 System data collection	The requirement meets this objective by ensuring that the TOE will backup AD objects to allow an administrator to restore any object within the backup.
O.SCAN The TOE must be able to collect information from devices, analyze the	EXT_SCR_ANL.1 Analytics	The requirement meets this objective by ensuring that the TOE analyzes the information from the network devices.

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
information, and generate reports based on the scanning results.	EXT_SCR_RDR.1 Restricted data review	The requirement meets this objective by ensuring that the TOE generates reports based on the information collected from the network devices.
	EXT_SCR_SDC.1 System data collection	The requirement meets this objective by ensuring that the TOE performs various scans on targeted network devices and monitors selected systems for data collection.
O.SESSION The TOE must terminate an administrator's session after an administrator define period of inactivity or after an administrator-initiated session termination.	FTA_SSL.3 TSF-initiated termination	The requirement meets the objective by ensuring that the TOE provides an inactivity timer that will terminate an inactive administrator session.
	FTA_SSL.4 User-initiated termination	The requirement meets the objective by ensuring that the TOE provides a method for the administrators to terminate their own session.
O.TIMESTAMP The TOE must provide a reliable timestamps to the BI and Retina components.	FPT_STM.1 Reliable time stamps	The requirement meets the objective by ensuring that the TOE provides a reliable timestamp for the BI and Retina components.

8.5.2 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2+, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 18 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 18 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Note that the TOE will provide the reliable timestamp to BI and Retina. The TOE environment will provide the reliable timestamp to PBW and PBA.
FAU_GEN.2	FIA_UID.1	✓	
	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

SFR ID	Dependencies	Dependency Met	Rationale
FAU_SAR.2	FAU_SAR.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FIA_AFL.1	FIA_UAU.1	✓	
FIA_ATD.1	No dependencies	✓	
FIA_SOS.1	No dependencies	✓	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.5	No dependencies	✓	
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.1	No dependencies	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	
FPT_STM.1	No dependencies	✓	
FTA_SSL.3	No dependencies	✓	
FTA_SSL.4	No dependencies	✓	
FTA_TAB.1	No dependencies	✓	
EXT_SCR_ANL.1	EXT_SCR_SDC.1	✓	
EXT_SCR_RDR.1	EXT_SCR_ANL.1	✓	
	FMT_SMR.1	✓	
	EXT_SCR_SDC.1	✓	
EXT_SCR_SDC.1	FPT_STM.1	✓	

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

9. Acronyms

Table 19 defines the acronyms used throughout this document.

Table 19 – Acronyms

Acronym	Definition
2U	Two Units
AD	Active Directory
BI	BeyondInsight
CAC	Common Access Card
CC	Common Criteria
CEM	Common Evaluation Methodology
CIS	Center for Internet Security
CMR	Code of Massachusetts Regulations
COBIT	Control Objectives for Information and Related Technology
CVSS	Common Vulnerability Scoring System
DISA	Defense Information Systems Agency
DSS	Data Security Standard
EAL	Evaluation Assurance Level
FDCC	Federal Desktop Core Configuration
FERC	Federal Energy Regulatory Commission
FISMA	Federal Information Security Management Act
FRS	File Replication Service
GB	Gigabyte
GHz	Gigahertz
GLBA	Gramm-Leach-Bliley Act
GPMC	Group Policy Management Console
GPO	Group Policy Object
HIPAA	Health Insurance Portability and Accountability Act
HITRUST	Health Information Trust Alliance
ID	Identification
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MB	Megabyte
MS	Microsoft
MSI	Microsoft Installer
NERC	North American Electric Reliability Corporation
NetBIOS	Network Basic Input/Output System
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OLAP	Online Analytical Processing
OS	Operating System
OSP	Organizational Security Policy
OU	Organizational Unit
PB	PowerBroker
PBA	PowerBroker Auditor
PBMS	PowerBroker Management Suite
PBW	PowerBroker for Windows
PCI	Payment Card Industry
PDF	Portable Document Format
PID	Process Identification
PIN	Personal Identification Number
PIV	Personal Identification Verification
PP	Protection Profile
R2	Release Two
R&A	Reporting & Analytics
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RDC	Remote Desktop Connection
RFC	Request for Comments
RSAT	Remote Server Administration Tools
SAM	Security Account Manager
SAR	Security Assurance Requirement
SCAP	Security Content Automation Protocol
SCCM	System Center Configuration Manager

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
SFR	Security Functional Requirement
SMB	Server Message Block
SOX	Sarbanes–Oxley
SP1	Service Pack One
SQL	Structured Query Language
SRS	SQL Reporting Services
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
UI	User Interface
USGCB	United States Government Configuration Baseline
UVM50	Unified Vulnerability Manager 50
VBAM	Vulnerability Based Application Management
WSUS	Windows Server Update Service

©2017 BeyondTrust Software, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Prepared by:

Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com