TECH BRIEF

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

Mapping BeyondTrust Solutions to NERC Critical Infrastructure Protection (CIP)

Privileged Access Management and Vulnerability Management

Table of Contents

Purpose of This Document

This guide has been prepared so that IT and security administrators can quickly understand how BeyondTrust solutions for privileged access management and vulnerability management map into the North American Reliability Electric Cooperative (NERC) critical infrastructure protection cybersecurity standards (CIP).

What is NERC CIP?

The NERC CIP[1] plan (currently version 5) is a set of requirements designed to secure the assets required for operating North America's bulk electric system. The NERC CIP plan consists of 9 standards and 45 requirements covering the security of electronic perimeters and the protection of critical cyber assets as well as personnel and training, security management and disaster recovery planning.

The CIP program coordinates all of NERC's efforts to improve the North American power system's security. These efforts include standards development, compliance enforcement, assessments of risk and preparedness, the dissemination of critical information and raised awareness regarding key security issues. NERC's standards for governing critical infrastructure apply to entities that "materially impact" the reliability of the bulk power system. These entities include owners, operators and users of any portion of the system.

Under NERC CIP, covered entities are required to identify critical assets and to regularly perform a risk analysis of those assets. Policies for monitoring and changing the configuration of critical assets need to be defined, as do policies governing access to those assets. In addition, NERC CIP requires the use of firewalls to block vulnerable ports and the implementation of cyber attack monitoring tools. Organizations are also required to enforce IT controls protecting access to critical cyber assets. Systems for monitoring security events must be deployed, and organizations must have comprehensive contingency plans for cyber attacks, natural disasters and other unplanned events. Penalties for non-compliance with NERC CIP can include fines, sanctions or other actions against covered entities.

The objective of this technical brief is to demonstrate how BeyondTrust solutions for privileged access management and vulnerability management map into the NERC CIP standard. For a summary of these mappings, please see the table below.

[1] http://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection

How BeyondTrust Solutions Help Meet NERC CIP Requirements

This section of the tech brief contains a summary table that summarizes how BeyondTrust solutions map to NERC CIP requirements.

Table 1: Summary Mapping of BeyondTrust Solutions to NERC CIP v5

NOTE: For simplicity, all standards that BeyondTrust solutions do not address have been removed from this table.

			Applicable BeyondTrust Products							
Standard Number	**Requirement Number**	**Text of Requirement**	BeyondTrust Platform	PowerBroker Password Safe	PowerBroker for Windows & Mac	PowerBroker for Unix & Linux	PowerBroker for Networks	PowerBroker Identity Services	PowerBroker Auditing & Security Suite	Retina Vulnerability Management
CIP-002-5.1a	R1.	R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: [Violation Risk Factor: High][Time Horizon: Operations Planning] i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above. 1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset; 1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and 1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).	✓							✓

			Applicable BeyondTrust Products							
Standard Number	Requirement Number	Text of Requirement	BeyondTrust Platform	PowerBroker Password Safe	PowerBroker for Windows & Mac	PowerBroker for Unix & Linux	PowerBroker for Networks	PowerBroker Identity Services	PowerBroker Auditing & Security Suite	Retina Vulnerability Management
CIP-002-5.1a	R2.	R2. The Responsible Entity shall: 2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and 2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.	✓							✓

CIP-003-6	R1.	Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics:
		1.1 For its high impact and medium impact BES Cyber Systems, if any:
		1.1.1. Personnel and training (CIP-004);
		1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
		1.1.3. Physical security of BES Cyber Systems (CIP-006);
		1.1.4. System security management (CIP-007);
		1.1.5. Incident reporting and response planning (CIP-008);
		1.1.6. Recovery plans for BES Cyber Systems (CIP-009);
		1.1.7. Configuration change management and vulnerability assessments (CIP-010);
		1.1.8. Information protection (CIP-011); and
		1.1.9. Declaring and responding to CIP Exceptional Circumstances.
		1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:
		1.2.1. Cyber security awareness;
		1.2.2. Physical security controls;
			✓	✓	✓	✓	✓	✓	✓	✓

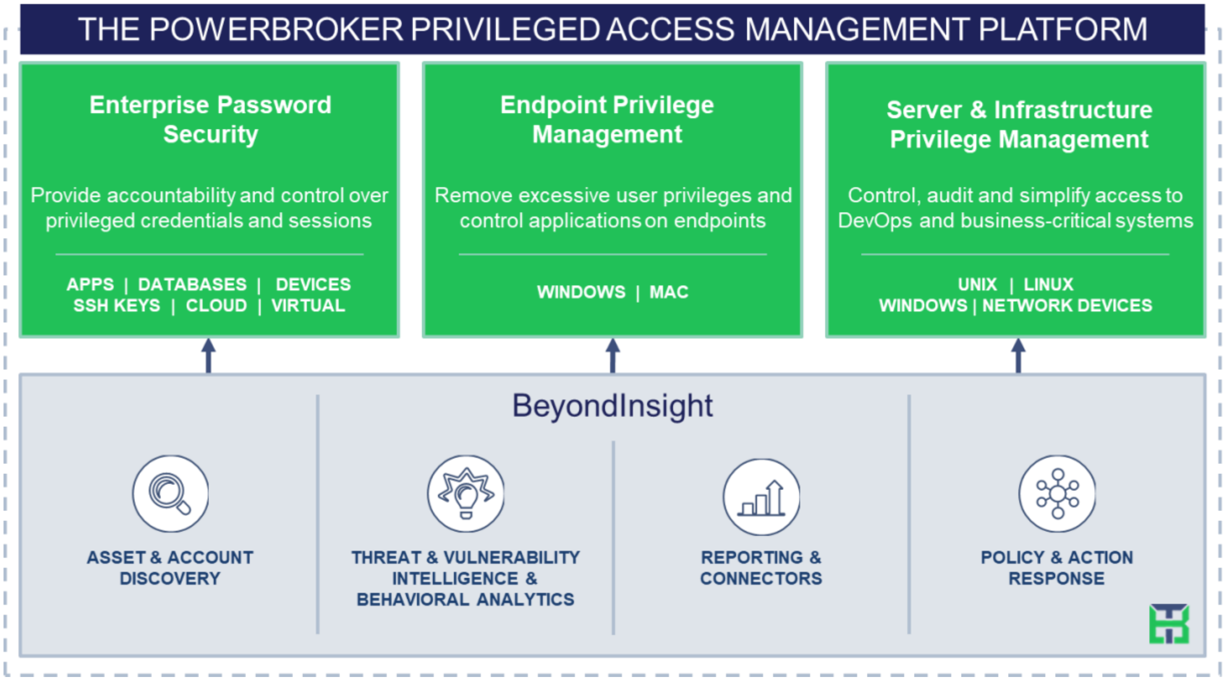
Standard Number	Requirement Number	Text of Requirement	Applicable BeyondTrust Products							
			BeyondTrust Platform	PowerBroker Password Safe	PowerBroker for Windows & Mac	PowerBroker for Unix & Linux	PowerBroker for Networks	PowerBroker Identity Services	PowerBroker Auditing & Security Suite	Retina Vulnerability Management
		1.2.3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and 1.2.4. Cyber Security Incident response								
CIP-003-6	R2.	Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.	✓							✓
CIP-003-6	R3.	Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	✓						✓	✓
CIP-003-6	R4.	The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	✓	✓	✓	✓	✓	✓		
CIP-004-6	R3.	Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program*. (please see standard for sub-req's)	✓	✓	✓	✓	✓	✓	✓	

Standard Number	Requirement Number	Text of Requirement	Applicable BeyondTrust Products							
			BeyondTrust Platform	PowerBroker Password Safe	PowerBroker for Windows & Mac	PowerBroker for Unix & Linux	PowerBroker for Networks	PowerBroker Identity Services	PowerBroker Auditing & Security Suite	Retina Vulnerability Management
CIP-004-6	R4.	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program.* (please see standard for sub-req's)	✓	✓	✓	✓	✓	✓	✓	
CIP-004-6	R5.	Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation*. (please see standard for sub-req's)	✓							✓
CIP-005-5	R1.	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter*.	NA							
CIP-005-5	R2.	Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*.	✓	✓	✓	✓	✓	✓		
CIP-007-6	R1.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services*. (please see standard for sub-req's)	✓							✓
CIP-007-6	R2.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management*. (please see standard for sub-req's)	✓							✓
CIP-007-6	R3.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention*. (please see standard for sub-req's)	✓		✓					✓

Standard Number	Requirement Number	Text of Requirement	Applicable BeyondTrust Products							
			BeyondTrust Platform	PowerBroker Password Safe	PowerBroker for Windows & Mac	PowerBroker for Unix & Linux	PowerBroker for Networks	PowerBroker Identity Services	PowerBroker Auditing & Security Suite	Retina Vulnerability Management
CIP-007-6	R4.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring*. (please see standard for sub-req's)	✓	✓	✓	✓	✓	✓	✓	✓
CIP-007-6	R5.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R5 – System Access Controls*. (please see standard for sub-req's)	✓	✓	✓	✓	✓	✓	✓	
CIP-010-2	R1.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management*. (please see standard for sub-req's)	✓		✓	✓	✓		✓	✓
CIP-010-2	R2.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring.* (please see standard for sub-req's)	✓							✓
CIP-010-2	R3.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3– Vulnerability Assessments*. (please see standard for sub-req's)	✓		✓					✓
CIP-011-2	R1.	Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection*. (please see standard for sub-req's)	✓		✓	✓	✓			

Appendix: PowerBroker Privileged Access Management Platform

The PowerBroker Privileged Access Management Platform is an integrated solution to provide control and visibility over all privileged accounts and users. By uniting best of breed capabilities that many alternative providers offer as disjointed tools, the PowerBroker platform simplifies deployments, reduces costs, improves system security and closes gaps to reduce privileged risks.


THE POWERBROKER PRIVILEGED ACCESS MANAGEMENT PLATFORM
Enterprise Password Security
Provide accountability and control over privileged credentials and sessions
APPS | DATABASES | DEVICES
SSH KEYS | CLOUD | VIRTUAL
Endpoint Privilege Management
Remove excessive user privileges and control applications on endpoints
WINDOWS | MAC
Server & Infrastructure Privilege Management
Control, audit and simplify access to DevOps and business-critical systems
UNIX | LINUX
WINDOWS | NETWORK DEVICES
BeyondInsight
ASSET & ACCOUNT DISCOVERY
THREAT & VULNERABILITY INTELLIGENCE & BEHAVIORAL ANALYTICS
REPORTING & CONNECTORS
POLICY & ACTION RESPONSE

Product Capabilities within the PowerBroker Privileged Access Management Platform

The PowerBroker platform includes the following individual best-of-breed products that are fully integrated into the platform itself. For how these products map into the NERC CIP standard, please reference the detailed chart earlier in this document.

PowerBroker Password Safe	PowerBroker Password Safe is an automated password and privileged session management solution offering secure access control, auditing, alerting and recording for any privileged account – from local or domain shared administrator, to a user's personal admin account (in the case of dual accounts), to service, operating system, network device, database (A2DB) and application (A2A) accounts – even to SSH keys, cloud, and social media accounts. Password Safe offers multiple deployment options, broad and adaptive device support, with session monitoring, application

password management and SSH key management included natively.

PowerBroker for Windows

PowerBroker for Windows (PBW) is a privilege management solution that mitigates the risks of cyber attacks as a result of users having excessive rights. By removing admin rights, protecting the integrity of critical files, and monitoring user behavior, PBW protects organizations without impacting end-user productivity.

PowerBroker for Mac

PowerBroker for Mac reduces the risk of privilege misuse by enabling standard users on Mac OS to perform administrative tasks successfully without entering elevated credentials.

PowerBroker for Unix & Linux

PowerBroker for Unix & Linux is a least privilege solution that enables IT organizations to eliminate the sharing of credentials by delegating Unix and Linux privileges and elevating rights to run specific Unix and Linux commands without providing full root access.

PowerBroker for Sudo

PowerBroker for Sudo provides centralized policy, logging, and version control with change management for multiple sudoers' files. The solution simplifies policy management, improves log security and reliability, and increases visibility into entitlements. This makes it easier for you to securely manage on low-priority servers or in areas where completely replacing sudo is not feasible.

PowerBroker for Networks

PowerBroker for Networks is an agentless privilege management solution that controls, audits, monitors and alerts on activity on network devices, enabling organizations of all sizes to reduce cybersecurity risks and achieve privilege management at scale.

PowerBroker Identity Services

PowerBroker Identity Services centralizes authentication for Unix, Linux, and Mac environments by extending Active Directory's Kerberos authentication and single sign-on capabilities to these platforms. By extending Group Policy to non-Windows platforms, PowerBroker provides centralized configuration management, reducing the risk and complexity of managing a heterogeneous environment.

Retina CS

Retina CS is a vulnerability management software solution designed from the ground up to provide organizations with context-aware

	vulnerability assessment and risk analysis for making better privileged access management decisions.
Platform Capabilities	The PowerBroker platform is built on the shared capabilities found in BeyondInsight, our IT risk management platform. Common components centralized for all products in BeyondInsight include asset and account discovery, threat, vulnerability and behavioral analytics, reporting and connectors to third-party systems, and central management and policy.

Conclusion

By partnering with BeyondTrust, organizations can address their compliance and security requirements as defined in NERC CIP v5, leaving fewer gaps, and improving efficiency over their privileged access management and vulnerability management practices.

About BeyondTrust

BeyondTrust® is a global security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: privileged access management and vulnerability management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.