BeyondTrust

SOLUTION BRIEF

Securing Industrial Control Systems (ICS) with BeyondTrust Solutions

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 Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) recommendations to improve the security of ICS/SCADA systems.

Why Monitoring ICS is Essential

Critical infrastructure systems that span manufacturing, transportation, water supply, and energy all depend heavily on information systems for their monitoring and control. Historically, ICS/SCADA systems have relied considerably on physical separation as the primary means for security. However, modern control system architectures, management processes, and cost control measures have resulted in increasing integration of corporate and ICS/SCADA environments. While these interconnections increase operational visibility and flexible control, they can also increase risks that previously did not occur with isolated ICS/SCADA. Through an interconnected network, the ICS/SCADA system can be exposed to threat actors who have already exploited and compromised the Internet and corporate networking, or by insiders misusing their privileges.

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) provides ICS-CERT alerts to assist owners and operators in monitoring threats and actions that could impact ICS/SCADA systems. To address these risks, ICS-CERT encourages sound security practices using "defense-in-depth principles."

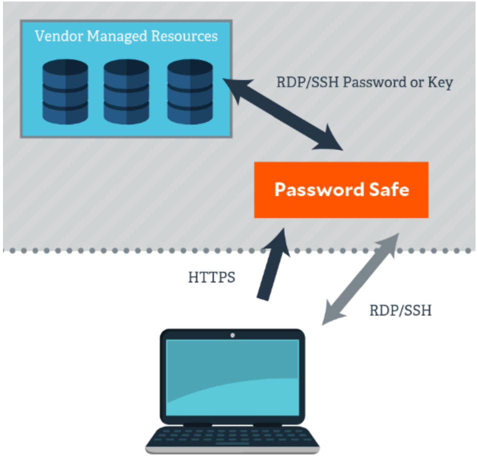
As they are considered fundamental technologies to addressing security best practices, this technical brief maps BeyondTrust privileged access management and vulnerability management solutions into ICS-CERT requirements.

Mapping BeyondTrust Solutions to ICS-CERT Security Recommendations

This section of the tech brief contains a detailed table that summarizes how BeyondTrust solutions map to ICS-CERT security recommendations.

Table 1: Detailed Mapping of BeyondTrust Solutions to ICS-CERT Security Recommendations

Risk Vector	ICS-CERT Recommendation	BeyondTrust Capabilities
Secure Passwords	Remove, disable, or rename any default system accounts wherever possible	Implementing an enterprise password management solution, like Password Safe, that supports enterprise password management, password rotation, active session management, and session recording, is an effective method to eliminate many of these common challenges. Password Safe is an automated password and privileged session management solution offering secure access control, auditing, alerting, and recording for any privileged account. Password Safe strengthens the security of ICS and interconnected environments by: • Ensuring no device has a default password • Guaranteeing each device has a unique, complex password • Automatically rotating passwords based on age and usage • Limiting administrative access and communications
Strong Password Management	Strong Password Management	
Reduce Risks of Brute-Force Attacks	Implement account lockout policies to reduce the risk from brute-force attacks.	
Minimize Network Exposure	This activity includes the implementation of firewalls and network segmentation. This can reduce the attack surface as well as the risk of lateral movement within a compromised environment.	Password Safe can be implemented using a secured enclave model to ensure all privileged accounts (employees, contractors, and third parties) do not have direct access to manage these devices. This model ensures that only approved devices and restricted network paths can be used to communicate with secured resources, which would include control system and HMI (Human-Machine Interface) computers. Using this best practice model for securing sensitive servers and networking devices ensures that all administrative activities are proxied through the management server so that each session is approved, tied to a specific individual, is properly audited, and that passwords are automatically rotated after each session is complete. See the diagram below for a representation of the enclave model. Privilege Management for Networks offers agentless privilege management capabilities to control, audit, monitor and alert on activity on network devices, such as infrastructure, ICS, SCADA, IoT, routers, switches and firewalls.

		When combined with Password Safe, the solution can control access to devices and control what commands can be run, while providing an indelible audit trail of activity through session monitoring and logging.
Secure Remote Access	This activity includes deployment and appropriately updating remote access solutions, such as VPN, if required.	ICS-CERT recognizes that a remote access solution, such as a VPN, is only as secure as the connected devices. With Password Safe, organizations can bulletproof their remote access infrastructure with complete control and audit of access to privileged accounts, such as shared administrative accounts, application accounts, local administrative accounts, service accounts, database accounts, cloud and social media accounts, devices, and SSH keys. BeyondTrust recommends the following architecture for enabling secure remote management:  Vendor Managed Resources RDP/SSH Password or Key Password Safe HTTPS RDP/SSH 1. Vendors access Password Safe directly or through existing remote access facilities and interact with the ICS client systems through the existing secured enclave. 2. Vendors authenticate to Password Safe and request a session to a managed resource, which can include a system running ICS control software. Note that this session can not only be restricted to a specific system but can also be restricted to a specific control system application, further reducing the risks of compromise and lateral movement.
Third Party Vendors	Monitor the creation of administrator-level accounts by third-party vendors.	

		3. Vendors use native remote desktop tools (MSTSC/PuTTY, etc.) or an RDP/SSH session, which is proxied through the Password Safe appliance. 4. All vendor activities are logged and optionally recorded to comply with security and compliance policies. 5. Privilege Management for Networks provides a jump server access to network devices to control, audit, monitor and alert on activity. This provides an optional l layer for third party access and management when segmentation of critical systems is required.
Vulnerability Management	Apply patches in the ICS environment, when possible, to mitigate known vulnerabilities.	BeyondTrust provides the most flexible, scalable, and effective means for identifying security exposures across diverse IT environments. Vulnerability Management enables customers to efficiently reduce IT security risks while adhering to security best practices, internal policies, and regulatory compliance requirements. In addition to providing risk visibility across the corporate network, it also includes in-depth SCADA system and vulnerability scanning encompassing over 75 SCADA systems. For a summary of supported SCADA systems, please see the section of the paper titled, Extending ICS Security with Least Privilege Management and Vulnerability Management.
Threat Detection	ICS-CERT recommends that organizations monitor for suspect activities, and to report their findings to ICS-CERT for incident response support and correlation with other similar incidents.	The BeyondTrust Platform (BeyondInsight) contains a purpose-built analytics engine called Clarity. Clarity is an advanced threat analytics solution that enables IT and security professionals to identify the data breach threats typically missed by other security solutions. Clarity pinpoints specific, high-risk users and assets by correlating low-level privilege, vulnerability, and threat data from a variety of BeyondTrust and third-party solutions. Clarity analyzes information stored in BeyondTrust's centralized database, which contains data gathered from across any or all supported solutions deployed in the customer environment. Clarity then sets baselines for normal behavior, observes changes, and identifies anomalies that signal critical threats via the following steps: • Aggregate users and asset data to centrally baseline and track behavior • Correlate diverse asset, user, and threat activity to reveal critical risks

		• Measure the velocity of asset changes to flag in-progress threats • Isolate users and assets exhibiting deviant behavior • Generate reports to inform and align security decisions Because of its ability to interpret granular and diverse sets of data, Clarity enables IT and security staff to reveal previously overlooked cases of user, account, and asset risk based on real world data.

Extending ICS/SCADA Security with Least Privilege Management and Vulnerability Management

BeyondTrust can provide additional hardening for remotely managed assets by using least privilege solutions like Privilege Management for Unix & Linux, for Networks, and for Windows. When additional tools (including ICS/SCADA third-party applications) are required to manage an infrastructure, whether they are command line-based or have a graphical user interface, Privilege Management can perform least privilege operations with these applications, and reduce the risk by only granting standard user privileges to the administrator.

Vulnerability Management's results-driven architecture works with users to proactively identify security exposures, analyze business impact, and plan to conduct remediation across network, ICS, SCADA, web, mobile, cloud, virtual, and IoT infrastructure.

- Discover network, web, mobile, cloud, virtual, and IoT infrastructure
- Profile asset configuration and risk potential
- Pinpoint vulnerabilities, malware, and attacks
- Analyze threat potential, return on remediation, and more
- Isolate high-risk assets through advanced threat analytics
- Remediate vulnerabilities, including default & weak passwords
- Report on vulnerabilities, compliance, benchmarks, etc.
- Protect approved and shadow devices from attack

Conclusion

By partnering with BeyondTrust, organizations can address ICS/SCADA security requirements as defined by the ICS-CERT, leaving fewer gaps, and improving efficiency over their privileged access management and vulnerability management practices.

Appendix 1: Summary Checklist of ICS-CERT Security Best Practices Requirements

Use this table to compare best practices requirements against your current solution.

	Discover all managed and unmanaged devices across your interconnected corporate and ICS infrastructure.
	Automatically discover and inventory privileged accounts used by third-party vendors.
	Provide central control by securely storing all passwords and SSH keys in a secured database.
	Reduce the risk of lost or stolen vendor credentials by systematically rotating passwords for all managed systems.
	Implement secure vendor enclaves to isolate ICS and vendor devices to reduce the risks of malware and attack.
	Provide verification that no default passwords exist on any managed system or device.
	Manage all devices automatically using Smart Rules and store a unique password per each device.
	Automatically rotate each device’s password based on age or after each remote vendor session.
	Provide a complete workflow for device access, including an approval process for when remote vendor access is required.
	Limit the commands that can be run when accessing network devices, infrastructure, IoT, IIoT, ICS, and SCADA systems.
	Record all, or select, remote sessions with playback to document and review what occurs when a device is accessed.
	Provide detailed reporting of all credentials used and requested when remote activity occurs.
	Deliver patent-pending analytics for abnormal device and credential access in a wide variety of available reports.

Appendix 2: Supported SCADA Systems

Network Security Scanner’s powerful discovery and scanning engine includes risk assessment libraries for more than 75 common SCADA vendors including:

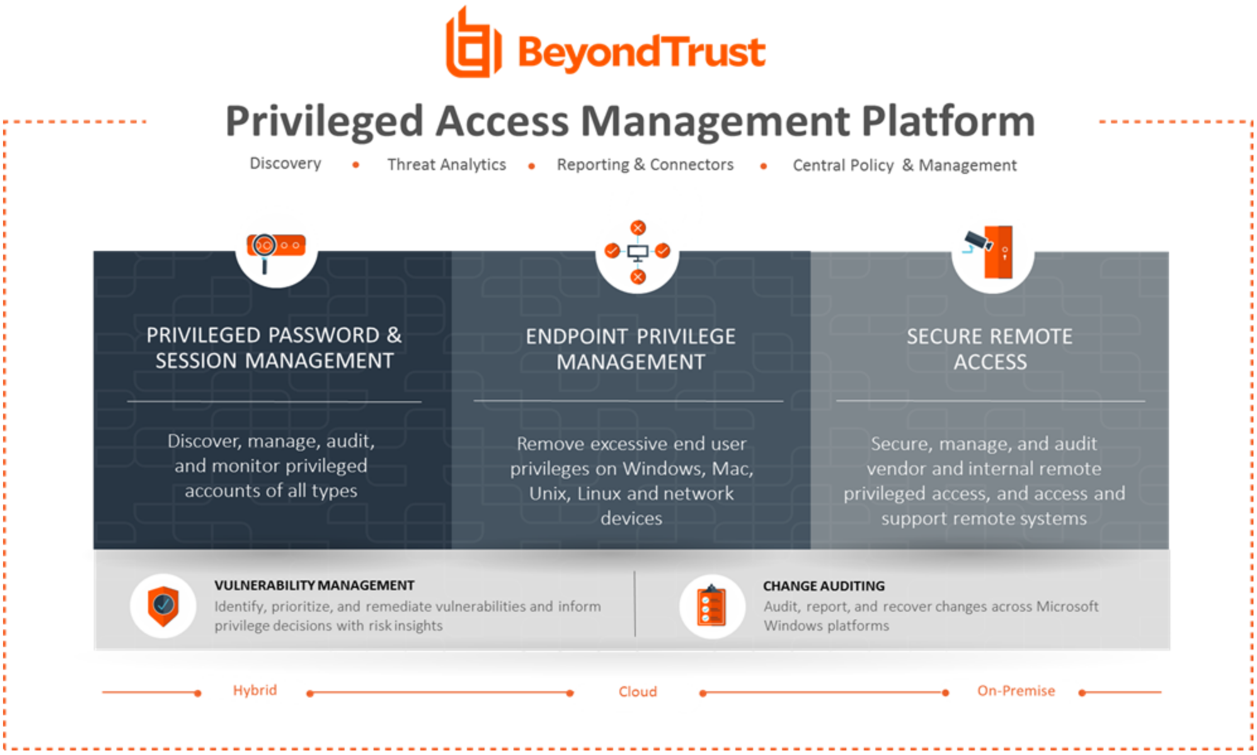
3S CoDeSys
Cortexa
Lantronix
Samsung Data Management
7 Technologies
Daktronics
Matrikon
SCADA Engine BACnet
ABB Stotz
DATAC
Measuresoft
Schneider Electric
Advantech
Delta
Modbus
Sentry
Broadwin
Eaton Powerware
Moxa
Sielco Sistemi
Allen-Bradley
Ecava
National Instruments
Seimens
AREVA
Eltek

Armor Safe Technologies
GarretCom
NIVUS
SISCO
Atop
GE
OPC
SpiderControl
Atvise
HMS
Optima
StruxureWare
Automated Solutions
Honeywell
PDQinc
Systech
AzeoTech
ICONICS
Progea
Takebishi DeviceXplorer
BayTech
InduSoft
Promotic
Telvent OASyS
Neptune
Sierra Raven

Beck
IntegraXor
Prosoft
Triangle MicroWorks
Beckhoff
Intellicom
RealFlex
Tridium Niagra
Borsch Rexroth
IRAI Automgen
Relion
Trihedral VTScada
Carel PlantVisor
Johnson Controls
Rockwell
Tripp Lite
ClearSCADA
Kentrox
RTS
WAGO
Cogent
Kepware
RuggedCom
Wellintech
Control Microsystems

Appendix 3: The BeyondTrust Privileged Access Management Platform

Our 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 PAM platform simplifies deployments, reduces costs, improves system security, and closes gaps to reduce privileged risks.



BeyondTrust

Privileged Access Management Platform

Discovery • Threat Analytics • Reporting & Connectors • Central Policy & Management

PRIVILEGED PASSWORD & SESSION MANAGEMENT

Discover, manage, audit, and monitor privileged accounts of all types

ENDPOINT PRIVILEGE MANAGEMENT

Remove excessive end user privileges on Windows, Mac, Unix, Linux and network devices

SECURE REMOTE ACCESS

Secure, manage, and audit vendor and internal remote privileged access, and access and support remote systems

VULNERABILITY MANAGEMENT

Identify, prioritize, and remediate vulnerabilities and inform privilege decisions with risk insights

CHANGE AUDITING

Audit, report, and recover changes across Microsoft Windows platforms

Hybrid • Cloud • On-Premise

BeyondTrust PAM solutions enable organizations to secure Industrial Control Systems to protect them from the risk of a breach and meet compliance mandates. For more information, visit beyondtrust.com/solutions.

Password Safe

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.

Privilege Management for Windows

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.

Privilege Management for Mac

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

Privilege Management for Unix & Linux, Advanced Edition

Privilege Management 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.

Privilege Management for Sudo, Basic Edition

This 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.

Privilege Management for Networks

Privilege Management 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.

Active Directory Bridge

Active Directory Bridge 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, it provides centralized configuration management, reducing the risk and complexity of managing a heterogeneous environment.

Enterprise Vulnerability Management

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.

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing privilege-related breaches. Our extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. We are trusted by 20,000 customers.

beyondtrust.com

V2019_05_ENG