BeyondTrust

Securing Privileged Access & Remote Access for Federal Agencies & Contractors

How BeyondTrust solutions reduce IT security risk, simplify the path to federal compliance mandates, and enable your organization to confidently embrace innovation

WHITEPAPER

Table of Contents

Secure Your Entire Privilege Universe with BeyondTrust

With over 20,000 worldwide customers, including more than 1,900 across the U.S. Public Sector, and half of the Fortune 100, BeyondTrust delivers a comprehensive, integrated suite of privileged access management (PAM) solutions that have been proven in a wide range of large and complex IT environments.
In both 2018 and 2019, Gartner recognized privileged account management as the #1 IT security project based on its ability to have a big impact in terms of both reducing risk and enabling the enterprise.

BeyondTrust addresses the broadest swathe of privileged access use cases. BeyondTrust solutions help enable our federal customers and federal contractors to:

- ✓ Massively reduce the threat surface and reduce security and data breach risk by securing privileged access, managing remote access, and enforcing least privilege access on any network enabled device.
- ✓ Address federal, state, local, and industry compliance initiatives with security controls, threat analytics, and reporting
- ✓ Securely and confidently embrace new technologies (cloud, IoT, robotic process automation)

This white paper provides an overview of how BeyondTrust solutions help federal agencies and contractors comply with a slew of U.S. federal regulations. As a global (but USA-based) cybersecurity enterprise, we enable customers to address compliance issues regionally and

Cybersecurity Initiatives Addressed by BeyondTrust

FISMA/NIST Compliance
Address FISMA requirements through the NIST Risk Management Framework for key SPs, including SP 800-53, SP 800-171, and SP 800-137. Also address important security and risk management controls of NIST CSIP and the NIST Cybersecurity Framework.

Continuous Diagnostics & Mitigation (CDM) Program
Address the CDM program's functional areas related to endpoint integrity and least-privilege access via a single platform.

Department of Defense (DoD) Cybersecurity Discipline Implementation & Scorecard DoD
Address three of the four Lines of Effort mandated in the DoD Cybersecurity Implementation Plan by employing a unified platform that combats internal and external threats, while managing privileged access for all agency users. By addressing priority cybersecurity controls that support mission assurance and cyber resilience for federal systems, BeyondTrust solutions can help your performance on the DoD Cyber Scorecard.

Cybersecurity Strategy & Implementation Plan (CSIP)
Strengthen cybersecurity across federal civilian agencies by addressing the first three (of five) objectives, critical to eliminating risks and addressing emerging threats.

National Industrial Security Program Operating Manual (NISPOM)
Protect sensitive agency data from unauthorized access from government contractors.

Homeland Security Presidential Directive 12 (HSPD 12)
Utilize smart card authentication for CAC and PIV cards with BeyondTrust's privileged access management solutions.

NERC Critical Infrastructure Protection (CIP)
BeyondTrust solutions help address key standards and critical security requirements necessary for the protection and integrity of the U.S. power grid.

globally. On the whitepapers section of our website, you can find more detailed information on how we address and map to specific federal compliance requirements as well as many other compliance initiatives and frameworks, including GDPR, PCI DSS, HIPAA, and SWIFT, to name just a few.

Government Organizations Must be Vigilant and Proactive

The compliance landscape for government agencies is constantly evolving to keep pace with new threats to public sector systems and new technologies being deployed. There are always emerging requirements that agencies must anticipate, implement, and report on, or be potentially subject to penalties—or worse—security and data breaches.

Government information networks – like their counterparts in public and private enterprises – are constantly vulnerable to both internal and external threats:

- **Internal threats** may be malicious (designed to cause harm) or unintentional (the result of human error), exposing weaknesses in the agency's defenses and policies. Regardless of intent, insiders can wreak significant damage quickly—they have the know-how, and, all too often, they have the access and privileges.
- **External threats** typically exploit credential flaws (embedded/default passwords, configuration errors, faulty code, reused or guessable passwords, weak 2FA or MFA, etc.) in networks and endpoints—often through remote access pathways. Threat actors seek to gain a foothold where they can act as an insider. They then cement their presence and skulk laterally throughout the IT environment—exploring opportunities to escalate their privileges, snag additional credentials, and exercise control over more assets and data.

The collateral damage of such attacks can range from "simple" non-compliance consequences to national security threats. Intellectual property, defense information, personnel records, and other classified information can easily be stolen, sold, and used against the interests of the U.S. government, its citizens, and its allies. BeyondTrust provides solutions that can protect against external and internal threats, whether inadvertent or malicious in intent.

Privileges and remote access pathways represent two of the most common and dangerous cyberthreat vectors. Let's take a brief a look at these attack vectors and how BeyondTrust solutions address them.

1. Privileged Threat Vectors

According to Forrester Research, the misuse or abuse of privileged credentials and access is implicated in roughly 80% of IT security breaches today—and it's no surprise why. Today, privileges are built into operating systems, file systems, applications, databases, hypervisors, cloud management platforms, DevOps tools, robotic automation processes, and more. Simply put, too many people, systems, and applications have far too many privileges. And attackers routinely exploit this tantalizing attack surface.

Cybercriminals covet privileges/privileged access because it can expedite access to an organization's most sensitive targets. With privileged credentials and access in their clutches, a cyberattacker or piece of malware essentially becomes an "insider".

In the aftermath of Edward Snowden's leaking of classified information for which he had excessive access privileges, the NSA announced it would reduce system administrator privileges by 90%. But despite the growing recognition of the substantial role privileges play in expanding the attack surface and leaving organizations vulnerable to damaging attacks, or to the fallout from inadvertent administrative errors, far too many government users have more access than they need to perform their current job functions.

As the 2019 Microsoft Vulnerabilities Report revealed, fully **81% of the 189 Critical Microsoft vulnerabilities reported in 2019 would be mitigated by removing local admin rights from users**. That data alone makes a compelling case for enforcing least privilege and application control, such as via an endpoint privilege management solution. With a least-privilege approach, users receive permissions only to the systems, applications, and data they need based on their current role or profile in the agency. These privileges can be user, system, or role-based as well as time-based (e.g., access granted only for certain days or hours, or for a set duration of time).

All privileged activity should be monitored and audited to ensure appropriate use, and to quickly identify, flag, and prevent misuse. By monitoring privileged users with BeyondTrust privileged access management solutions, which enable proactive alerts and reporting, you can achieve "verifiable compliance" with stated access policies – and gain assurance that your security solution can pass any audit.

2. Securing Remote Access Pathways

According to 2019 research from BeyondTrust as part of the Privileged Access Threat Study, government/public sector organizations have 124 third-party vendors logging into their systems/networks in a typical week. Thus, it's unsurprising that the same

study found that only 10% of government/public organizations believed that third-party vendor access was not a threat to their organizations.

With so many remote access points, and often, sub-optimal visibility, auditing, and security controls over this access, it's only a matter of time before a remote access weak link is compromised—either via an employee or a third-party vendor. Remote access pathways represent those weakest links for most organizations—and cybercriminals know it.

SLAs can help keep your vendor security on the right track, but how do you trust that your vendors are following the right security practices? What can you do to protect your organization if they aren't? Many federal organizations rely on VPNs for third-party access, but VPNs provide far too much access.

Most security vendors providing remote access:

- Do not offer granular access control settings
- Do not provide a comprehensive audit trail
- Do not support all operating systems and scenarios, and thus require the use of multiple products

BeyondTrust can securely address the broadest range of remote access use cases—from remote support to vendor and remote worker access. Our solutions can provide fine-grained access controls, auditing all privileged activities, and can work across an expansive range of systems and use cases. This also means you can consolidate your various remote tools into one solution, saving on admin costs, while also improving security by blacklisting other remote access tools, which are often planted on computers as part of an attack.

Bringing it All Together - How BeyondTrust Enables Security For The Public Sector

Reviewed, Tested, Trusted

Gartner, Forrester, and KuppingerCole have each recognized BeyondTrust as a privileged access management Leader in their most recent industry reports.

The BeyondTrust Privileged Access Management Platform was also named the top 2019 Privileged Access Management Solution in the "ASTORS' Homeland Security Awards. American Security Today's Annual 'ASTORS' Awards program is the largest and most

comprehensive in the industry, highlighting the most cutting-edge and forward-thinking security solutions in the market today. According to American Security Today, "BeyondTrust's unified solutions offer the industry's broadest set of privileged access management capabilities with a flexible design that simplifies integrations, enhances user productivity, and maximizes IT and security investments."

Additionally, BeyondTrust was named a Gold winner in the 2018 Government Security News Homeland Security Awards for "Best Identity Management Platform.

Third-Party Integrations

BeyondTrust's solutions and platform are also elegantly designed to make integrations with important third-party tools as seamless and synergistic as possible. We are proud to have been recognized by McAfee as their Security Innovation Alliance (SIA) partner of the year for two consecutive year (2018 & 2017), selected from 150 SIA partners. We have certified integrations for BeyondTrust Password Safe and Endpoint Privilege Management with McAfee solutions to enable organizations to better control risk and eliminate threats.

Our System for Cross-domain Identity Management (SCIM) integration with SailPoint enables organizations to effectively manage user access for both privileged and non-privileged accounts. IT organizations benefit from full visibility into, not only role assignments and user access, but also all users and ongoing role changes. When changing roles, adding and removing access is provided to ensure the right person has the right access at all times to increase security and reduce risks.

You can learn more about our rich technology partner ecosystem that includes ServiceNow, Okta, FireEye, Palo Alto Networks, and others on our Partners page.

Core Capabilities of BeyondTrust Solutions

- ✓ **Discover, onboard, and securely manage privileged credentials**—for human and non-human accounts across diverse IT environments. This includes privileged account passwords, application/embedded passwords, SSH keys, DevOps secrets, service accounts, and more
- ✓ **Manage and monitor all privileged sessions** (including pausing and/or terminating suspicious sessions in real-time), and audit and report on all privileged activities—even those for third-party (vendor) access.
- ✓ **Control privilege elevation and delegation, and enforce least privilege** across all endpoints (Windows, Mac, Unix, Linux), network devices, etc. For

instance, you can (and should) remove all local admin privileges from most non-IT users and eliminate root and superuser access wherever possible. BeyondTrust enables you to elevate application access—without elevating the user.

- ✓ **Enforce just-in-time access:** This ensures privileged accounts are not always sitting in a privilege-active state, thereby dramatically reducing the threat window. With BeyondTrust solutions, you can approach a state of zero standing privileges.
- ✓ **Securely address the broadest range of secure remote access** use cases. From providing industry leading remote support solutions that are a fixture of IT service management and internal help desks, to securing remote access for vendors and remote workers. No other IT security vendor can help you address secure remote access in all its form as holistically as can BeyondTrust.
- ✓ **Extend privilege management best practices** to vendors and remote employees.
- ✓ **Consistently authenticate users across heterogeneous environments** by extending AD's Kerberos authentication and single sign-on capabilities across platforms (Windows, Mac, Unix, Linux, etc.).
- ✓ **Make better privilege decisions with vulnerability insights:** Leverage patented technology to automatically scan applications for vulnerabilities at runtime, enabling IT and security teams to enforce quarantine, reduce application privileges, or prevent the launch of an application.
- ✓ **Deep reporting and threat analytics:** Delivers deep analytics and reporting to multiple stakeholders, ensuring that all teams have the information and views they need to effectively manage application and asset risk, and prove compliance.
- ✓ **Leverage partner integrations to realize risk management synergies and richer reporting**: Gain a holistic view of enterprise-wide security, including risk from users, accounts and their privileges, and other security solutions, such as SIEMs and firewalls.

Key Benefits of BeyondTrust PAM Solutions for the Public Sector

- Mitigate both external threats (malware, hacker, etc.) and insider threats
- Pass audits, comply with government and industry mandates, and fulfill reporting requirements via privileged access certification reporting
- Ensure accountability through session monitoring and recording, keystroke logging, and real-time auditing
- Stay protected across your entire IT environment—on-premise, cloud, hybrid, DevOps infrastructures; we can also help secure your workloads and containers
- Enable informed, actionable IT risk management decisions from meaningful data gleaned from context-aware security intelligence, including asset, user, and account privilege information

Compliance: How BeyondTrust Holistically Mitigates Risk

BeyondTrust provides important capabilities that support a wide range of government information security requirements. Here we have broken down some of the most common and pressing federal mandates and regulations, showing the extent to which BeyondTrust's PAM solutions can help agencies achieve and maintain compliance around managing, securing and auditing privileged access and remote access.

FISMA/NIST

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to implement information security solutions to protect the information and information systems that support agency operations and assets.

National Institute of Standards and Technology (NIST) is a non-regulatory agency of the U.S. Department of Commerce charged with advancing measurement standards. Special Publications (SPs) are developed and issued by NIST as recommendations and guidance documents. FISMA publications are developed by NIST in accordance with its responsibilities under The Federal Information Security Modernization Act of 2014, which amended the Federal Information Security Management Act of 2002 (FISMA) with modifications that modernize Federal security practices to address evolving security concerns.

The NIST Risk Management Framework (NIST RMF) is the standard for integrating information security and risk management into government agency information systems. The NIST RMF encompasses a range of activities defined by several different NIST SPs. BeyondTrust supports the requirements of four key SPs relating to the NIST RMF: SP 800-53, SP 800-171, SP 800-39, and SP 800-137.

NIST SP 800-53: Security and Privacy Controls for Federal Information Systems & Organizations & NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST SP 800-53 sets forth a comprehensive approach to information security and risk management by providing organizations with a broad set of security controls essential to strengthen their information systems and the environments in which they operate so that they become more resilient in the face of cyberattacks. NIST SP 800-53 outlines a "Build It Right" strategy combined with various security controls for Continuous Monitoring, striving to provide senior leaders of organizations information to support making risk-based decisions related to their critical missions.

NIST SP 800-171 is very similar to, and largely derived from, NIST SP 800-53. While SP 800-53 pertains to federal systems and organizations, SP 800-171 pertains to non-federal systems and organizations that may interface with federal systems. This regulation strives to put protections around the vast amount of federal information that is regularly stored, processed, and transmitted by nonfederal organizations, like contractors, state and local governments, universities, and research organizations. Often, this information is sensitive and, if compromised, would have a direct negative impact on the functioning of the federal government and an agency's ability to achieve their mission. Therefore, protecting that information, both inside and while outside of federal information systems, is critically important.

BeyondTrust's solutions address several individual controls under the following control families across both SP 800-53 and SP 800-171:

- ✓ **Access Control** – Endpoint Privilege Management, Secure Remote Access
- ✓ **Audit & Accountability** – Endpoint Privilege Management, Auditor, Secure Remote Access
- ✓ **Security Assessment and Authorization** – Endpoint Privilege Management
- ✓ **Configuration Management** – Endpoint Privilege Management
- ✓ **Identification and Authentication** – Password Safe
- ✓ **Risk Assessment** – Endpoint Privilege Management
- ✓ **System & Services Acquisition** – Endpoint Privilege Management
- ✓ **System and Communications Protection** – Endpoint Privilege Management, Secure Remote Access
- ✓ **System and Information Integrity** – Endpoint Privileged Management, Auditor

NIST SP 800-137: Information Security Continuous Monitoring (ISCM)

BeyondTrust offers several solutions that enable continuous monitoring, defined by 800-39 as part of the 11 security automation domains that support continuous monitoring. In particular, BeyondTrust provides capabilities around asset and credential inventorying

NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a risk-based framework for critical infrastructure organizations to voluntarily manage their cybersecurity risks. This standard was to be based on industry best practices and international standards. The adoption of the framework has steadily increased since its initial release. The Cybersecurity Framework, developed in partnership between industry and government, was designed to provide a universal standard, yet be flexible enough to address an organization's unique risks and risk tolerance.

The Framework core is a set of desired actions, outcomes, and references across critical infrastructure sectors. This core consists of five functions: **Identify, Protect, Detect, Respond, and Recover**. BeyondTrust PAM solutions, along with the BeyondInsight platform's behavioral and threat analytics, address various controls across each of these five functions.

Cybersecurity Strategy and Implementation Plan (CSIP)

The CSIP was a consequence from a comprehensive review in 2015 of the Federal Government's cybersecurity policies, procedures, and practices by the Cybersecurity Sprint Team. The intent of this process and formulation of the CSIP was to identify and address critical cybersecurity gaps and emerging priorities. The CSIP lays the groundwork for strengthening cybersecurity in federal civilian agencies through five objectives:

1. Prioritized identification and protection of high value information and assets;
2. Timely detection of and rapid response to cyber incidents
3. Rapid recovery from incidents when they occur, and accelerated adoption of lessons learned from the Sprint assessment
4. Recruitment and retention of the most highly-qualified cybersecurity workforce talent the Federal Government can bring to bear
5. Efficient and effective acquisition and deployment of existing and emerging technology

BeyondTrust solutions can address key measures across numbers 1 through 3 of the CSIP.

Department of Homeland Security (DHS)

Continuous Diagnostic and Mitigation (CDM) program

The DHS launched the CDM program to enable it, along with federal, state, local, regional, and tribal governments, to enhance and further automate their existing continuous network monitoring capabilities, correlate and analyze critical security-related information, and improve risk-based decision making at the agency and federal enterprise level.

The CDM program provides capabilities and tools that enable network administrators to know the state of their respective networks at any given time by identifying and ranking problems for priority resolution. Continually monitoring networks for flaws and anomalies will alert network managers to attacks and intrusions, thereby enabling faster responses to fix vulnerabilities that allow attacks.

BeyondTrust privileged access management solutions address more than half of the functional areas of CDM, including for:

- ✓ Manage Trust in People Granted Access
- ✓ Manage Security Related Behavior
- ✓ Manage Credentials and Authentication
- ✓ Manage Privileges
- ✓ Detect Suspicious Events/Patterns

Homeland Security Presidential Directive 12 (HSPD 12): Policy for a Common Identification Standard for Federal Employees and Contractors

HSPD 12 is a strategic initiative designed to improve security, boost government efficiency, minimize identity fraud, and safeguard data privacy. This requires federal agencies to use a standard smart credential to verify the identities of all employees and contractors accessing federal buildings and information systems. The directive also mandates that all government personnel obtain Personal Verification Identification (PIV) cards.

BeyondTrust supports HSPD 12 by enabling smart card authentication for CAC and PIV cards with BeyondTrust's privileged access management solutions.

National Industrial Security Program (NISP)

The National Industrial Security Program (NISP) was established by Executive Order in 1993 to manage the needs of private industry to securely access classified information

National Industrial Security Program Operating Manual (NISPOM)

The NISP Operating Manual (NISPOM) establishes the specific standard procedures and requirements for all government contractors with regards to their ability to access and use classified information. Collectively, BeyondTrust PAM solutions help address various Information System Security controls defined in Chapter 8 of the NISPOM, including for:

- ✓ Identification and Authentication
- ✓ Session Controls
- ✓ Security Testing

Department of Defense (DoD)

DoD Cybersecurity Discipline Implementation Plan & DoD Scorecard

In September 2015, the Secretary of Defense and Chairman of the Joint Chiefs of Staff published a document titled, "Department of Defense Cybersecurity Culture and Compliance Initiative." In it, they identified several key cybersecurity requirements that all agencies must address in order to improve the resilience of the Department of Defense (DoD) IT networks. One of the outcomes was the Cybersecurity Discipline Implementation Plan (amended in 2016). The DoD Cybersecurity Discipline

Implementation Plan is aimed at meeting strong security standards for DoD information networks to provide mission assurance. The Plan identifies four Lines of Effort, each representing a prioritization of all the DoD's cybersecurity requirements.

BeyondTrust solutions can help organization address 3 of the 4 Lines of Effort, which are:

- **Strong authentication** – to degrade the adversaries' ability to maneuver on DoD information networks. [BeyondTrust Password Safe & Endpoint Privilege Management]
- **Reduce attack surface** – to reduce external attack vectors into DoD information networks. [BeyondTrust Privileged Access Management solutions]
- **Alignment to cybersecurity / computer network defense service providers** – to improve detection of and response to adversary activity. [BeyondTrust's BeyondInsight Platform]

The DoD Cyber Scorecard measures how organizations are achieving compliance with cyber basics. Now on version 2.0, this measure was developed in response to the Cybersecurity Discipline Implementation Plan. As such, BeyondTrust PAM solutions can help you address areas that are critical in order to perform well on the DoD Cyber Scorecard.

North American Electric Reliability Corporation (NERC)

NERC Critical Infrastructure Protection (CIP) Plan

NERC CIP (currently on version 5) is a set of requirements designed to secure the assets required for operating North America's bulk electric system. NERC is approved of by the Federal Energy Regulatory Commission (Commission or FERC) authority, which oversees the reliability of the U.S. power grid.

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, including standards development, compliance enforcement, assessments of risk and preparedness, and the dissemination of critical information and raised awareness regarding key security issues.

BeyondTrust solutions help address 12 of the requirements and 6 of the 9 standards across NERC CIP.

Certifications

FIPS 140-2

Federal Information Processing Standards (FIPS) are issued by NIST in accordance with FISMA; they are compulsory and binding for federal agencies. FIPS 140-2 is a U.S government computer security standard used to accredit cryptographic modules. To help address the increasing cybersecurity demands of the federal sector and other critical sectors, the Federal Information Processing Standards Publication (FIPS) 140-2 validation became a requirement for cryptographic products/software used in a U.S. government agency network and other industries to establish encryption standards that protect sensitive data. As a result, programs such as FedRAMP, FISMA, DoDIN APL, Common Criteria, HIPAA and HITECH healthcare regulations inherit the dependency on FIPS 140-2 validation.

- ✓ BeyondTrust Password Safe ships on commercially supported FIPS 140-2 validated components for all encryption over passwords to critical data.
- ✓ BeyondTrust Endpoint Management for Unix & Linux integrates with SafeNet Luna for U.S. and Canadian government agencies requiring FIPS 140-2 Level 2/Level 3 validation.
- ✓ The BeyondTrust Remote Support B-300 appliance is the only remote support solution to obtain FIPS 140-2 Level 2 validation for use in U.S. Government agencies and others

Common Criteria

The National Information Assurance Partnership (NIAP) oversees evaluations of commercial IT products for use in national security systems and is responsible for U.S. implementation of the Common Criteria. The following BeyondTrust products have received Common Criteria certifications:

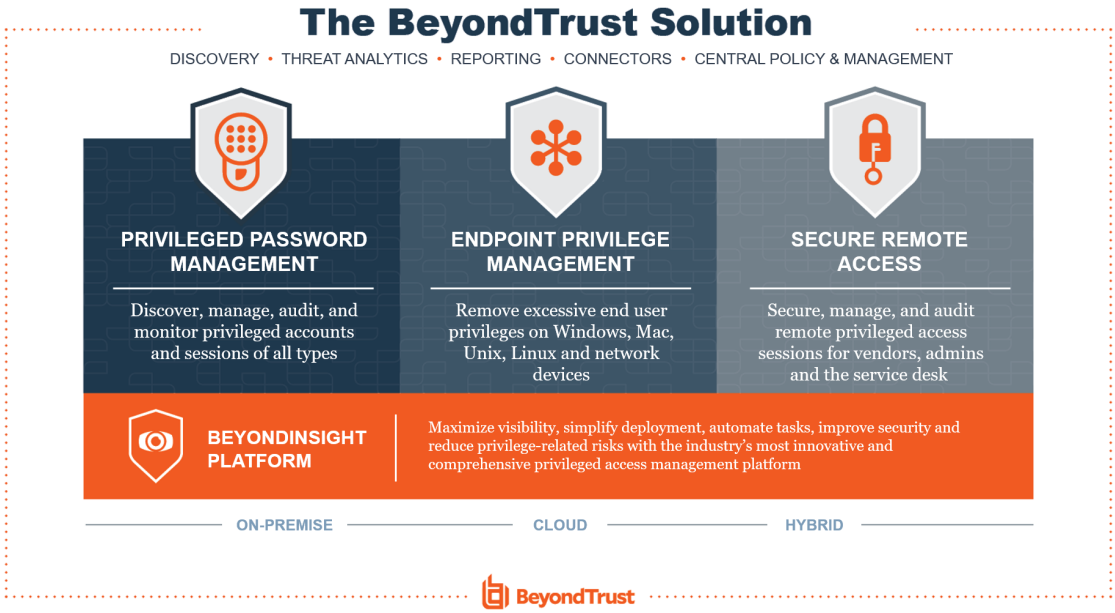
- ✓ Password Safe (formerly named PowerBroker Password Safe)
- ✓ Endpoint Privilege Management for Unix & Linux (formerly named PowerBroker for Unix & Linux)

Overview of BeyondTrust Platform & Solutions

As federal agencies are under pressure to limit the number of discrete vendors, BeyondTrust can handle the bulk of your security initiatives around privileged and remote access—thereby helping reduce your vendor portfolio, while ensuring you have industry-best solutions to protect against some of the most dangerous attack vectors.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace.

BeyondTrust Platform (BeyondInsight): BeyondInsight is the smart console shared across BeyondTrust privileged access management & vulnerability management solutions, providing centralized management and policy control. BeyondInsight provides integrated capabilities such as asset discovery, profiling, smart groups, threat analytics, reporting, and connectors to third-party systems.



BeyondTrust Privileged Password Management solutions enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and auditing of all privileged activities. Security teams can instantly view any active privileged session, and if required, pause or terminate it. Leverage threat analytics that aggregate user and asset data to baseline and track behavior and alert on critical risks. Video recording, keystroke indexing, full text search, and other capabilities make it easy to pinpoint data. Reduce the risk of compromised privileged credentials for both human and non-human accounts while meeting compliance requirements.

BeyondTrust Endpoint Privilege Management combines privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices—without hindering productivity. Elevate applications securely and flexibly with a powerful rules engine and comprehensive exception handling. Centralized auditing and reporting simplify the path to compliance. Enforce

least privilege and eliminate local admin rights with fine-grained control that scales to secure your expanding universe of privileges, while creating a frictionless user experience.

BeyondTrust Secure Remote Access solutions enable organizations to apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks. Users can quickly and securely access any remote system, running any platform, located anywhere, and leverage the integrated password vault to discover, onboard, and manage privileged credentials. Gain absolute visibility and control over internal and external remote access, secure connectivity to managed assets, and create a complete, unimpeachable audit trail that simplifies your path to compliance.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network. Learn more at www.beyondtrust.com.

V2020_01_ENG