WHITE PAPER

UNIVERSAL PRIVILEGE MANAGEMENT

The Journey to Securing Every Privilege, Every Time

BeyondTrust

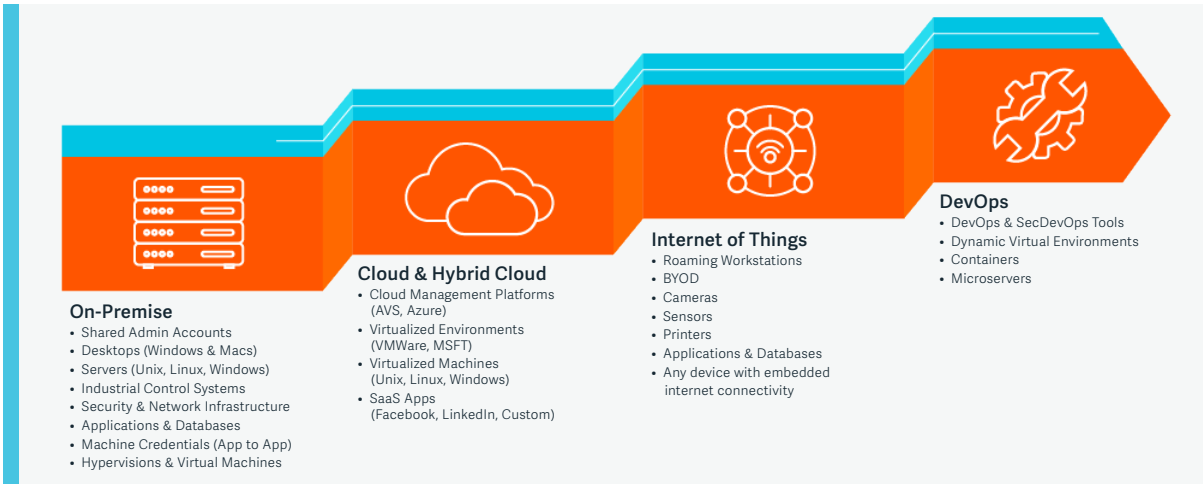
TABLE OF CONTENTS

1 Introduction

In today's vast landscape of cyberattacks, there is a common thread: successful attacks almost always involve compromised or misused privileges. For example, most malware needs privileges to execute and install. Once a threat actor has infiltrated an IT network, privileges are typically needed to access resources or compromise additional identities. With privileged credentials and access in their clutches, a threat actor or piece of malware essentially becomes an "insider". And, outside of Privileged Access Management (PAM), there are few defenses against a rogue insider.

The past few years have seen an explosion in the number and types of privileges arising from human identities (employees, vendors, contractors, etc.), mobile devices and the Internet of Things (IoT), cloud platforms, applications, services, machines, Robotic Process Automation (RPA), and more, as detailed in Figure 1. This privilege explosion gives attackers more opportunities than ever to compromise an environment, and organizations are struggling to shrink their windows of exposure across this rapidly widening attack surface.

Figure 1: The privileged attack surface has exponentially increased as our IT environments have evolved



Your Adversaries Use Automated Tools – So Should You

Almost without exception, today's threat actors leverage readily available automated tools, some of which have their origins within well-funded, nation-state arsenals. Automation increases the speed and probability that the attacker can find and exploit that initial weak link that gives them a "hook" into an environment. Therefore, it is critical to automate the control, monitoring, and auditing of privileges and privileged access for everything that touches your IT environment.

The good news is that organizations increasingly recognize they need automation and purpose-built solutions to protect privileges, and PAM has become a cornerstone of an effective, modern cybersecurity defense. The bad news is that many organizations mistakenly presume that privileged password management alone will solve the problem, when it's only one part of a necessary, comprehensive PAM solution.

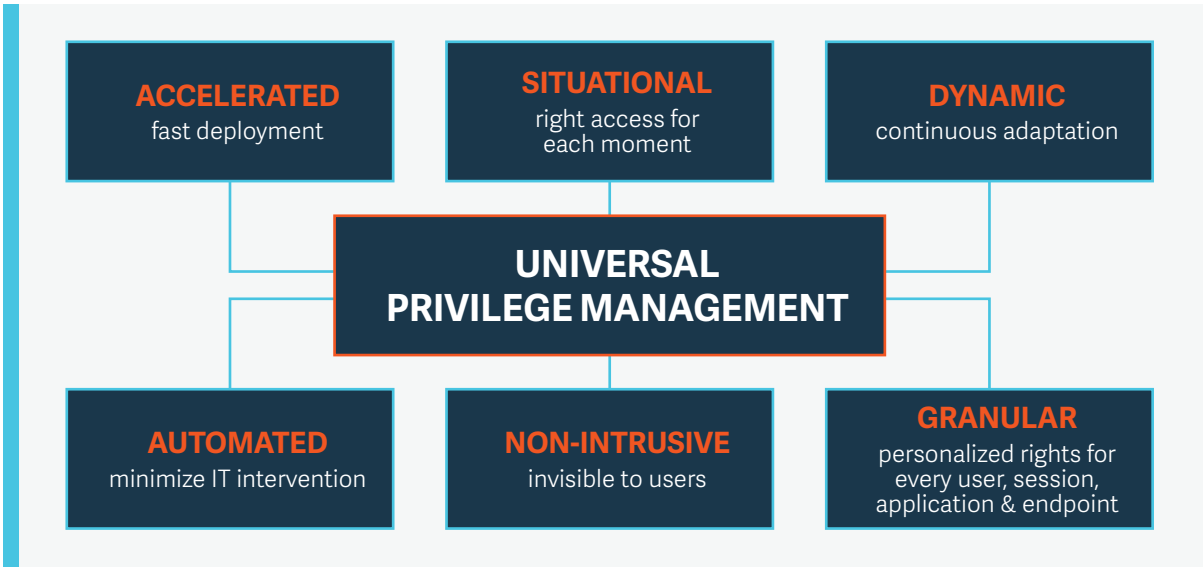
2

A New Era of Universal Privilege Management

As the PAM technology leader, BeyondTrust offers a holistic approach to securing every privileged user, session, and endpoint. This Universal Privilege Management model is an expansive approach to securing your entire universe of privileges along a journey that allows you to quickly address your biggest risk areas and immediately shrink your attack surface.

Working with thousands of customers around the world, we've developed a guide to the most common use cases in an effective PAM solution that can be customized to meet your unique environment and requirements. Wherever you begin your journey, BeyondTrust's powerful capabilities and quick-start innovations enable you to rapidly leap ahead in risk reduction and operational improvements.

Figure 2: Achieve fast security and productivity gains with Universal Privilege Management



The BeyondTrust Universal Privilege Management approach will set you up for success in:

- **Minimizing your attack surface** and windows of exposure by enforcing true least privilege through controlling both time (the duration privileges are granted) and space (the privileges and access pathways).
- **Controlling privileged user, session, and file activities** to prevent unauthorized access or changes that inappropriately affect your organization's sensitive data or normal business operations.
- **Analyzing asset and user behavior** to detect suspicious or malicious activities to secure operations in line with security best practices and regulatory compliance.

- **Adopting a low-impact approach to PAM** across your entire enterprise, protecting privileges while increasing user productivity and minimizing resource consumption.
- **Implementing seamless integrations** to other mission-critical security solutions (e.g. identify governance & administration (IGA), security information and event management (SIEM), IT service management (ITSM), etc.) to maximize value, streamline workflows, and reduce risk for privileged access management.

In today's complex, dynamic environments, it's imperative to adopt a modern PAM approach that goes beyond just managing passwords, to protecting privileges across your entire privilege universe. Consider a typical environment (Figure 3) and all the locations privileged accounts are used to manage and monitor your organization.

Figure 3: Today, it's essential to secure every privilege in your environment

The Universal Privilege Management model secures every user, session, and asset across your IT environment. In this paper, we'll explore:

- The pivotal role PAM plays in disrupting the cyberattack chain
- The core components of the Universal Privilege Management model
- How to quickly improve privilege security with a solution that is frictionless and invisible to end users

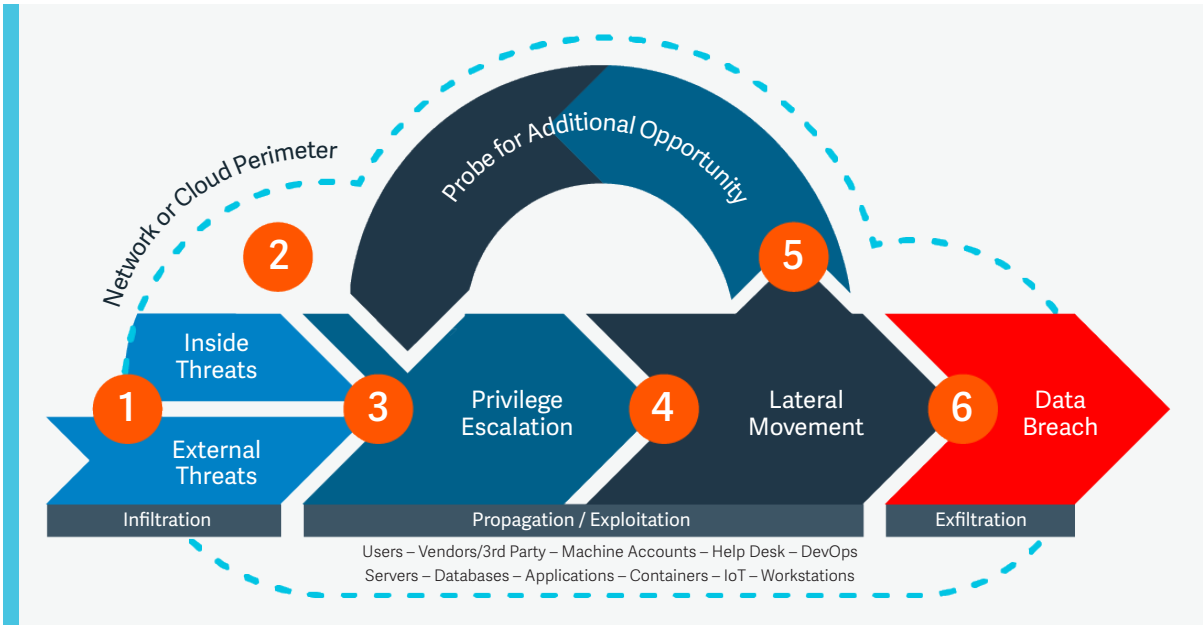
3 Disrupting the Cyberattack Chain

External attack pathways commonly follow a modus operandi, referred to as the cyberattack chain. Attackers exploit vulnerabilities and user privileges to gain a foothold. Next, they expand their presence and move laterally around the IT environment—exploring opportunities to escalate their privileges, grab additional credentials, and assert control over more assets and data.

No single cybersecurity product can provide total protection against every attack vector. However, BeyondTrust's solutions break the attack chain at multiple points to quickly and effectively stop threats, while mitigating damage. Applying a Universal Privilege Management model helps organizations dramatically condense their overall risk surface, while also reducing windows of exposure.

Let's briefly review the key attack chain steps and the crucial part privileged access controls play in blocking or disrupting these steps.

Figure 4: The Cyberattack Chain



INFILTRATION

1. *Insiders and External Threats*

   Threat actors trying to penetrate the perimeter directly are no longer the primary threat to an organization. Instead, it's far more likely that attackers will execute a successful campaign by exploiting misconfigured resources with compromised privileged accounts, or by launching a phishing attack to compromise a user's system. Once infiltration is successful, attackers set up a beachhead inside of an environment to maintain a persistent presence, while flying "under the radar".

BeyondTrust helps reduce your risk surface and prevent attacks from breaching your environment in the first place.

When employees or vendors are over-provisioned with privileges, which is often the case, the potential for damage is high. A 2019 Proofpoint study reported that more than 99 percent of threats observed required human interaction to infect user devices, and the 2019 BeyondTrust Microsoft Vulnerabilities Report found that 81 percent of critical Microsoft vulnerabilities can be eliminated by removing local admin rights from users.

Human and machine identities are central to IT risk. Removing excessive privileges can prevent most attacks from succeeding at even Step 1 of the attack chain.

BeyondTrust helps reduce your risk surface and prevent attacks from breaching your environment in the first place, enabling you to eliminate admin rights, to enforce true least privilege, secure credentials, and protect remote access pathways into your network.

2. *Command and Control Through the Internet*

Unless the attack is ransomware or some other form of automated malware, the attacker quickly establishes a connection to a command and control (C&C) server to download toolkits, additional payloads, and to receive information for the next phase of their attack. This step allows them to assess the environment and decide how to move forward.

PROPAGATION / EXPLOITATION

3. *Identify Privileged Accounts and Attempt Privileged Escalation*

At this stage, threat actors begin to learn about the network, infrastructure, privileged accounts, key identities, and the resources operating within the environment. They explore opportunities to collect additional credentials, upgrade privileges, exploit additional vulnerabilities, or just leverage the privileges that they have to access resources, applications, and data with the mindset of "landing and expanding".

As with Step 1, BeyondTrust's PAM platform prevents misuse of privileges by granting users only the privileges they need at precisely the moment they need them, keeping credentials under tight control, and enabling granular controls for remote employees and vendors.

4. *Lateral Movement Between Assets, Accounts, Resources, and Identities*

Next, threat actors typically leverage these stolen credentials and knowledge gained about the environment to compromise additional resources and identities (accounts) via lateral movement. This continues the campaign of propagation and navigation through the victim's environment. Today, 70 percent of all attacks involve attempts to laterally move across the network. To a threat actor, lateral movement is a crucial strategy. It allows them to move from where they opportunistically landed within an organization via the initial exploit to other more desirable or sensitive resources.

BeyondTrust's Universal Privilege Management approach can drastically curtail lateral movement via mitigating privileged attack vectors. By enforcing just-in-time (JIT) access, zero trust, least-privilege access and removing admin rights, the lateral access pathways are limited in both number and in windows of time and duration in which they can be accessed. BeyondTrust's privileged session monitoring and management capabilities enable you to pause or terminate suspicious activity, which is itself a powerful defensive capability.

BeyondTrust gives you broad, powerful capabilities to ensure that the attacker's initial beachhead within your environment remains a (very) small island, with no routes to other bodies of resources, and no chance to "island hop".

Securing privileged credentials from compromise–whether employee, vendor, or non-human—also helps prevent attackers from expanding privileged access. For example, implementing One-Time Passwords (OTPs) for highly privileged accounts will prevent password re-use attacks, and frequent rotation of credentials minimizes the time a threat window can be compromised. Finally, auto-generating extremely long and complex passwords adds further security by reducing the threat of dictionary or brute force attacks.

BeyondTrust also helps organizations enforce segregation of duties through granular assignment of privilege across users and groups, ensuring specified duties can only be performed with the appropriate accounts. Thus, if an account is compromised, the range of privileges it affords the attacker is vastly restricted in scope.

Finally, BeyondTrust gives you broad, powerful capabilities to ensure that any attacker's beachhead within your environment remains a (very) small island, with no routes to other bodies of resources, and no chance to "island hop". When executed correctly, a defensive posture against privilege escalation and lateral movement leaves attackers marooned, limiting damage while giving you time to detect, and ultimately, eject the attacker from the environment.

5. *Probing for Additional Opportunities*

While continuing to discover weaknesses, like vulnerabilities, misconfigured hosts, and additional privileged credentials, the actor is also trying to remain invisible. If their movement or presence is detected, most organizations will try to mitigate the incident. Therefore, while operating covertly, the threat actor can probe for additional targets, install more malware or hacking tools, and expand their presence.

BeyondTrust's PAM solution protects you during this phase of the attack chain. The same security concepts discussed for restricting lateral movement help here as well. For example, applying a JIT privileged access approach and eliminating persistent privileged access help dramatically reduce the number of privilege-active accounts that an attacker can exploit at any given moment.

EXFILTRATION OR DESTRUCTION

6. *Breach*

Finally, the threat actor—whether internal or external—collects, packages, and exfiltrates the data, or destroys your resources based on their objective (i.e. ransomware).

BeyondTrust offers file integrity monitoring and application control that sends alerts if sensitive data or files have been tampered with or corrupted, and the platform provides a wealth of privileged threat analytics that not only helps you zero in on and disrupt threat actors, but also provide comprehensive forensics to support additional adversary hunting and audits.

4 The Journey to Universal Privilege Management

As you can see, an effective PAM strategy will help you disrupt multiple points in the attack chain. But traditional PAM approaches often require you to start by putting all privileged credentials into a vault, which can be time-consuming from a people and process change management perspective. While privileged password management is a vital step, modern approaches allow you to address PAM in the way that best suits your organization and priorities to gain more immediate benefits in security and productivity.

The Universal Privilege Management model allows you to start with the PAM use cases that are most urgent to your organization, and then seamlessly address remaining use cases over time. For example, organizations that want to start with protecting privileged access from third parties, or eliminating administrative rights from users, can do so without implementing a full password management solution first.

This section covers the core use cases that make up the Universal Privilege Management journey. Each use case, once addressed, will give you enhanced control and accountability over the accounts, assets, users, systems, and activities that comprise your privilege environment, while eliminating and mitigating multiple threat vectors. The more use cases you address, the more PAM synergies emerge, and the more impact you'll realize in reducing enterprise risk and improving operations.

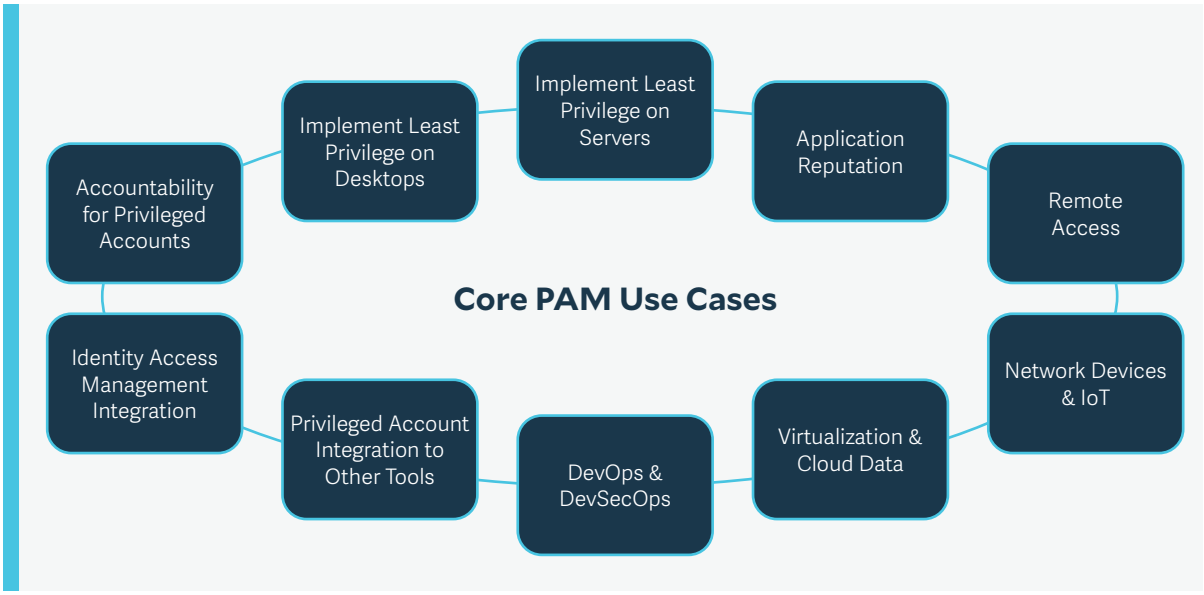


Figure 5: Start anywhere and proceed in any order with BeyondTrust's Universal Privilege Management approach.

Only BeyondTrust provides a complete, highly scalable solution to manage, monitor, and audit all types of privileged credentials and sessions in a centralized and unified way.

ACCOUNTABILITY FOR PRIVILEGED ACCOUNTS

While not mandated, many organizations find discovering and securing privileged accounts the logical starting point for improving privilege security controls. According to Forrester Research, privileged credentials are implicated in 80 percent of data breaches. A Varonis study reported that 65 percent of companies have more than 1,000 stale user accounts. Who is watching out for these stale and/or orphaned accounts? Threat actors certainly are. When these stale accounts are privileged, they can fast-track an attacker's access to sensitive resources. Other vulnerable credentials include shared credentials or those hardcoded in scripts, applications, or devices, which may be missed by basic password tools.

How do organizations ensure security and accountability over all different types of privileged credentials without disrupting administrator productivity or other workflows and processes? This demands a privileged credential management solution that automatically discovers and onboards the ever-expanding list of privileged accounts/credential types (passwords, DevOps secrets, SSH keys, certificates, etc.), and brings those accounts/credentials under management within a centralized password safe. This includes both human (employee, vendor) and non-human (functional, service, application, software robot, etc.) accounts in your environment.

The solution should allow control over which accounts are being shared, by whom, when, where, and why. It should provide mechanisms to find hardcoded credentials and deliver options to replace them with managed credentials. Critically, the solution should monitor, manage, and audit every privileged session regardless of where it originates.

Only BeyondTrust provides a complete, highly scalable solution to achieve all this in a centralized and unified way. The BeyondTrust platform will eliminate outright many privileged credential-based attack vectors, and mitigate many others, to drastically reduce enterprise security exposure.

LEAST PRIVILEGE ON DESKTOPS (WINDOWS & MACOS)

Another important step to achieving Universal Privilege Management is implementing least privilege on end-user machines. Least privilege is defined as, "the minimum privileges/rights/access necessary for the user or process to be fully productive." Starting from the secure base of a standard user account, policy-based privilege can be assigned to the activities the user needs to perform on their system without altering their user account. This involves the removal of local administrative rights potentially invoked by the local user or via a remote session. By eliminating end-user desktop administrator rights and implementing least privilege, users can remain fully productive without the risks carried by administrator privileges.

With a least-privilege approach, users receive permissions only to the systems, applications, and data they need for their current roles. Rather than being enabled, persistent, and always-on, the privileges are only elevated on an as-needed basis and only for the targeted application or process. This is the basis for a just-in-time (JIT) PAM model. Using the default of a standard user and only elevating privileges when needed, you drastically shrink the threat surface, reducing the opportunity for lateral movement, and minimizing the risk of threats, such as phishing and ransomware, landing and expanding.

BeyondTrust enforces least-privilege access and simplifies compliance across physical and virtual Microsoft Windows and macOS desktops in a completely invisible and frictionless way for the end user. Our solution provides deeper capabilities and can be more quickly implemented than competitive solutions, delivering a fast time-to-value.

BeyondTrust offers the gold-standard solution for achieving absolute control over privileged accounts, and also enables just-in-time (JIT) privilege management.

LEAST PRIVILEGE ON SERVERS (UNIX, LINUX & WINDOWS)

Tier-1, or business-critical, applications are attractive targets for threat actors. However, it's rare that a threat actor can compromise these sensitive resources first. Obtaining privileged user credentials via other assets provides access to these systems through lateral movement. Having superuser status is important for administrators and some authorized users to do their jobs. Unfortunately, this practice also presents significant security risks from intentional, accidental, or indirect misuse of those privileged credentials.

With other tools, including sudo, it's impossible to maintain best-practice security and compliance in all but the simplest of IT environments. Organizations must limit, control, and audit who has access to superuser accounts and privileges, without impairing productivity.

Organizations must be able to efficiently and effectively delegate server privileges without disclosing the passwords for root, local, or domain administrator accounts. They should record all privileged sessions to help meet regulatory compliance. This is conceptually like the removal of administrative rights on desktops, but with the added requirements of supporting server-class operating systems in Tier-1 regulated environments.

BeyondTrust offers the gold-standard in solutions for achieving absolute control over server privileges. The BeyondTrust solution offers centralized management, monitoring, and reporting, and delivers JIT privilege management, eliminating persistent privileged access to drastically minimize risk in your environment.

APPLICATION REPUTATION

Application control is essential to preventing advanced malware attacks, such as ransomware. Whitelisting, blacklisting, and greylisting offer application control strategies that enable organizations to restrict applications to only those approved to execute, with the correct privileges, within the appropriate context. Effective application control is key for organizations to manage the risk surface, prohibiting rogue and known malicious software from installing or executing. These strategies also provide seamless, appropriate application access to end users.

Another application reputation capability involves empowering organizations to make better-informed privilege elevation decisions by understanding the vulnerability of an application or an asset with which it interacts. In other words, if an application password is stale, or an asset is potentially compromised, you may not want to allow elevated privileges. Applying real-time risk intelligence to privilege delegation and elevation not only stops exploits from becoming a privileged attack vector, but it also blocks drive-by social engineering threats that can leverage vulnerabilities within the environment.

Similar to application control on Windows, command filtering on Unix and Linux is a critical security, compliance, and reliability control. What commands should be allowed to run and which ones should be explicitly denied? With what privileges should the commands and scripts execute? For both application control and command filtering, a full audit trail of everything attempted and allowed is important.

Application reputation capabilities are integrated within the BeyondTrust solution, complementing its least-privilege management capabilities. Application control and endpoint privilege management work together to improve control and reduce complexity, with a single policy engine for both desktops and servers.

VPNs and many other widely used remote access tools simply don't offer the granular controls needed by security and compliance-conscious organizations.

REMOTE ACCESS

Almost all attacks start externally and involve some form of remote resource access. The exception being insiders initiating attacks directly on a system. The vast majority of remotely launched attacks come from threat actors who are not specifically targeting your organization, but rather through remote contractors, vendors, and, even remote employees, who have themselves been compromised.

Many IT administrators, insiders, and vendors need some sort of privileged access to effectively do their jobs. They also need the ability to elevate privileges. VPNs and other widely used remote access tools simply don't offer the connection isolation, granular controls, and audit capability required by security and compliance-conscious organizations. These technologies are weak links that threat actors exploit to pry their way past the perimeter.

BeyondTrust's Privileged Access Threat Report found that, on average, organizations have 182 vendors logging into their systems every week. Opus & Ponemon reported that, on average, companies share confidential and sensitive information with approximately 583 third parties. Both reports found that 58 to 59 percent of companies have incurred a breach due to a vendor. With so many inadequately protected remote access points, it's unsurprising that organizations are incurring third-party breaches at an alarming rate.

The ideal defense is to extend PAM best practices beyond the perimeter. This ensures only the right identity has access to the right resources in the right context. It eliminates "all or nothing" remote access for vendors by implementing least-privilege access to specific systems for a defined duration of time, potentially requiring a chaperone when appropriate. Vendor credentials should be managed through the solution with policies, mandating rotation or single use passwords, and utilizing credential injection in sessions so that passwords are never exposed to end users. Finally, session management and monitoring should be enforced to audit and control all vendor/remote access activity. This approach is far more secure than traditional protocol routing technologies like VPN.

BeyondTrust is the only PAM vendor that offers mature and tested capabilities for extending privileged access security best practices to vendors, other third parties, and remote workers.

NETWORK DEVICES & IOT

Many PAM tools lack the ability to extend granular privileged access controls to non-traditional endpoints, such as medical or industrial-connected devices and control systems. With potentially hundreds, or thousands, of managed network and IoT devices in an environment, assigning a complex, unique password to each device and securely storing each password poses a logistical nightmare without the help of a centralized, automated password safe. As a shortcut, administrators often choose simple, common, and guessable passwords and assign the same password to every device of the same asset type for ease of management. Unfortunately, threat actors have proven effective at brute-forcing these devices to gain access. If a password has been reused for multiple devices, it can be leveraged across the enterprise for multiple points of control.

BeyondTrust delivers the capability of least privilege to those endpoints by allowing fine-grained control over the commands sent and the responses received over SSH sessions. This offers the ability to control the operation of functions like tab completion, restricting access to only those aspects of the endpoint that are appropriate for the user. Administrators and vendors can be constrained within their area of responsibility without impacting their productivity.

BeyondTrust enables you to extend PAM best practices to the expanding universe of non-traditional endpoints. Our integrated solution allows you to:

The BeyondTrust solution not only protects the full spectrum of privilege use cases for your entire cloud environment, but also can be deployed in the cloud (as SaaS, PaaS, or IaaS) as well as on-premises.

- **Discover and onboard** all accounts across all devices
- **Enforce password management best practices**, such as eliminating embedded/hardcoded credentials, enforcing unique passwords, and securing credentials in a centralized, tamper-proof safe
- **Apply fine-grained least-privilege control**, allowing you to control which commands users can run
- **Monitor and records sessions** to provide a complete audit trail of user activity
- **Analyze behavior** to detect suspicious user activity

THE CLOUD AND VIRTUALIZATION

With the ever-growing (and accelerating) use of virtualized data centers and cloud environments for processing, storage, application hosting and development, organizations have opened new avenues for threat actors to access sensitive data and cause disruption. As with traditional desktops and servers, unknown or undermanaged virtualized and cloud environments can create a security gap that poses significant security and compliance risks. Ephemeral privileged accounts and credentials are rapidly instantiated and then disposed of at tremendous scale when new cloud and virtual instances are spun up and, just as easily, spun down.

When managing any privileged account, discovery is the critical first step to gaining control over these assets and the many planes of privileges strewn across cloud environments. Once cloud and virtualized instances are found, they must be managed to limit exposure. From a privileged access management perspective, the options to secure these assets are like traditional desktops and servers as described above. However, here are a few unique privileged security use cases for the cloud:

- Utilize a password management solution to manage the passwords and keys that are unique to the cloud environment, like the hypervisor, API's, and management consoles.
- Implement a PAM solution with session monitoring for all administrative or root access into cloud providers, regardless of whether they are SaaS, PaaS, or IaaS-based.
- When performing RPA or variations on DevOps, utilize a password management or secrets store to protect application-to-application secrets used in the cloud.

The BeyondTrust solution not only protects the full spectrum of privilege use cases for your entire cloud environment, but also can be deployed in the cloud (as SaaS, PaaS, or IaaS) as well as on-premises.

DEVOPS & DEVSECOPS

DevOps delivers condensed development and deployment cycles through automation, frequently leveraging the scale of the cloud. The downside is that DevOps processes can also "automate insecurity," creating massive risks as well as compliance and operational gaps. Some common DevOps risks include:

- Insecure code, hardcoded passwords, and other privilege exposures
- Scripts or vulnerabilities in Continuous Integration/Continuous Deployment (CI/CD) tools, which could deploy malware or sabotage code
- Excessive provisioning of privileges across the DevOps landscape
- Sharing of secrets

BeyondTrust's solutions can discover all privileged automation accounts (including for CI/CD tools, service accounts, RPA, etc.) and replace the credentials with trusted API calls. The automatic retrieval and injection of the proper tool credentials helps protect developers, operations teams, and applications from attacks when privilege accounts are used for automation.

By unifying privileged access management and other IT and security management solutions, IT teams benefit from a single, contextual lens through which to view and address risk by activity, asset, user, identity, and privilege.

PRIVILEGED ACCOUNT INTEGRATION TO OTHER TOOLS

Modern PAM solutions must communicate with the rest of your IT security environment. By unifying privileged access management and other IT and security management solutions, IT teams benefit from a single, contextual lens through which to view and address risk by activity, asset, user, identity, and privilege.

For example, integrating privileged account data with vulnerability management solutions will enable you to pinpoint specific, high-risk users and assets by correlating threat data and log data from a variety of third-party solutions. Integrating PAM with change or service management workflows will allow you to automatically provision and deprovision privileges, just-in-time.

Learn more about BeyondTrust's Third-Party Integrations.

IDENTITY ACCESS MANAGEMENT INTEGRATION

Access to an organization's resources is ideally managed through an Identity and Access Management (IAM) solution, which offers capabilities such as single sign-on, user provisioning/deprovisioning, role-based user management, access control, and governance. IAM solutions help IT teams answer, "Who has access to what?", but to achieve complete user visibility and accountability, privilege management solutions are required to address the remaining questions, "Is that access appropriate?" and "Is that access being used appropriately?" IAM solutions will add users to a system or applications group, but lack the session activity details, whether operating locally or via remote access, to monitor activity. Bi-directional IAM and privileged access management integration is imperative to holistically manage, secure, and audit users and roles to ensure activity is appropriate.

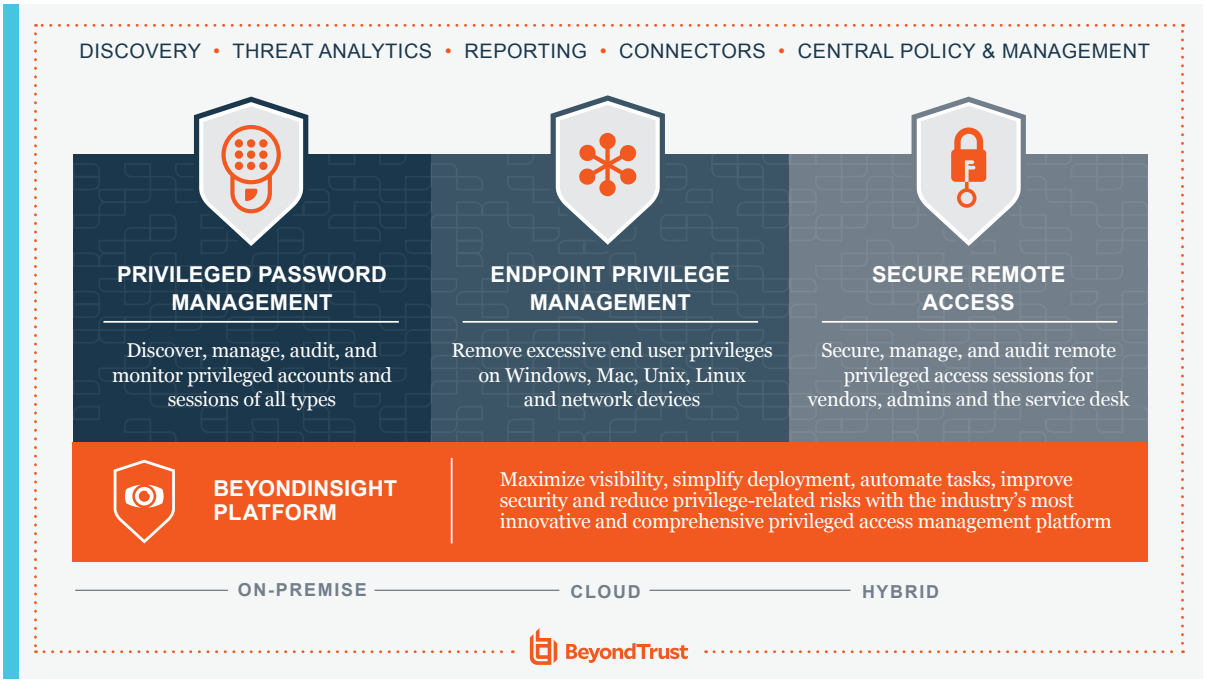
In addition, Unix, Linux, and macOS have traditionally been managed as standalone systems; each a silo with its own set of users, groups, access control policies, configuration files, and passwords to remember. Managing a heterogeneous environment that contains these silos, plus a Microsoft or cloud environment, leads to inconsistent administration for IT, unnecessary complexity for end users, and a vast sprawling of alias accounts. The ideal solution is to centralize identity management and authentication and provide single sign on across Windows, Unix, Linux, and macOS environments by extending a directory store like Microsoft's Active Directory with single sign-on capabilities to non-Windows platforms.

BeyondTrust accomplishes this for enterprise environments by extending Group Policy to non-Windows platforms. IT environments benefit from centralized configuration and consistent policy management for accounts, while eliminating the sprawl of local alias accounts. In addition to reducing security risk, BeyondTrust helps boost productivity for users and server administrators.

5 BeyondTrust Universal Privilege Management Solution

The integrated BeyondTrust Universal Privilege Management portfolio provides visibility and control over the entire, ever-expanding universe of privileged identities, endpoints, and sessions, with the industry's only extensible PAM platform. As outlined above, our unique approach enables you to address your organization's most pressing pain points first or secure your entire universe of privileges at once with our integrated solution set.

Figure 6: The BeyondTrust Universal Privilege Management Platform



BEYONDTRUST SOLUTION & PRODUCT DESCRIPTIONS

BEYONDINSIGHT PLATFORM

BeyondInsight is the industry's most innovative, comprehensive privileged access management platform that maximizes visibility, simplifies deployment, automates tasks, improves security, and reduces privilege-related risks. Administrators gain a comprehensive view of the privileged vulnerabilities that provide doors into an environment, as well as the privileges that present corridors to sensitive assets. The security team benefits from a "universal" awareness and enforcement approach to privilege management, while IT gains a clearer view of how privilege policies impact overall security. This fusion of asset and user intelligence enables IT and security to collectively reduce risk across complex environments.

PRIVILEGED PASSWORD MANAGEMENT

BeyondTrust's 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 activity

BeyondTrust's 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 activity. 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.

Password Safe combines privileged password and session management to discover, manage, and audit all privileged credential activity. Scan, identify, and profile all assets for automated onboarding, ensuring no credentials are left unmanaged. Control privileged user accounts, applications, SSH keys, cloud admin accounts, and more, with a searchable audit trail for compliance and forensics. Achieve complete control and accountability over privileged accounts.

DevOps Secrets Safe enables secure, centralized management and auditing of secrets and other privileged credentials used by applications, tools, and other non-human identities. Drive peak agility while controlling credentials and other secrets used across the CI/CD toolchain, including passwords, keys, certificates, applications, and other automated processes.

Cloud Vault unifies comprehensive session management and essential credential vaulting for internal and third-party privileged users with a simple, fast, cloud-based solution. Control the management of privileged passwords and sessions across your environment to reduce threats from privileged credential or access misuse and enable complete accountability and compliance.

Combine privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices

ENDPOINT PRIVILEGE MANAGMENT

Combine privilege management and application control to efficiently manage admin rights on Windows, macOS, 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.

Privilege Management for Windows & Mac is the leader for enforcing least privilege, with unmatched granular, policy-based controls and unimpeachable audit trails. Simplified deployment models and a single, comprehensive audit trail drive quick time-to-value and streamline compliance for immediate risk reduction and productivity improvements.

Privilege Management for Unix & Linux is the unrivaled solution for enforcing least privilege on servers with extensive, granular, policy-based controls and unimpeachable audit trails. Extend capabilities far beyond sudo with centralized administration, session monitoring and management, file integrity monitoring, and powerful productivity enhancements.

Active Directory (AD) Bridge centralizes authentication for Unix, Linux, and Mac environments by extending Microsoft AD's Kerberos authentication and single sign-on. Extending Microsoft Group Policy to these non-Windows platforms enables centralized configuration management and reduces the risk and complexity of managing a heterogeneous environment.

Apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks

SECURE REMOTE ACCESS

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.

Privileged Remote Access empowers IT teams to control, manage, and audit remote privileged access by authorized employees, contractors, and vendors. Enforce least privilege and exert granular control and visibility over remote access for both insiders and third parties, while enabling user productivity.

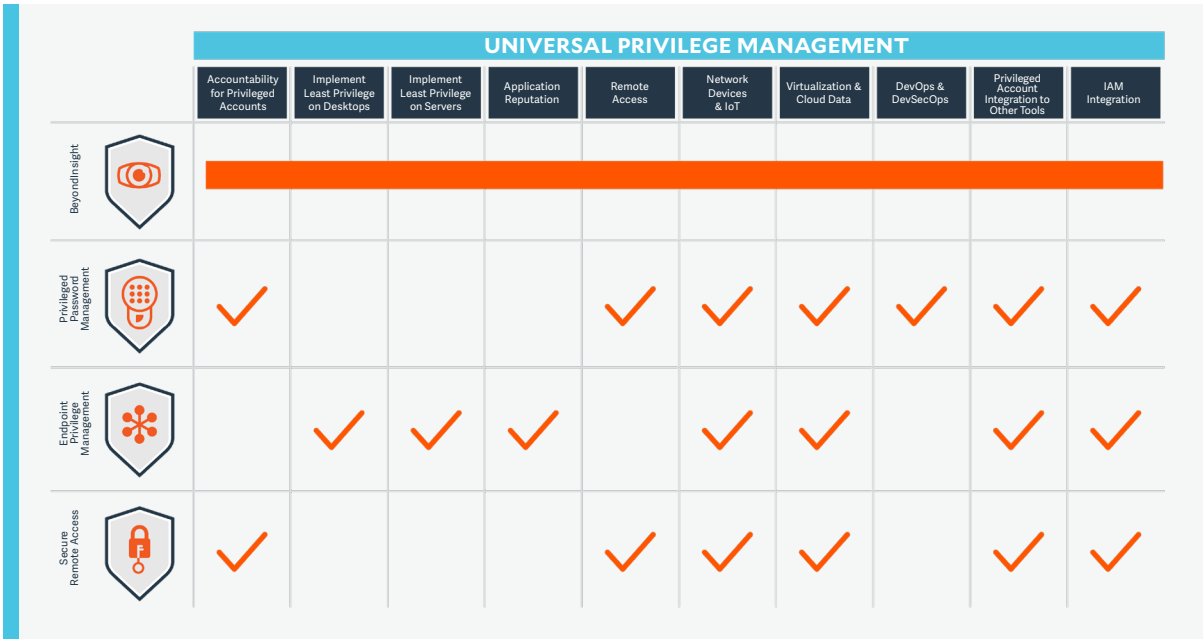
Remote Support empowers service desks to quickly and securely access and fix any remote device anywhere, running any platform, with a single solution. Organizations of all sizes can boost service desk productivity, efficiency, and security by consolidating and standardizing help desk support with BeyondTrust.

Transform Your Privileged Security Posture with Universal Privilege Management

BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities, accounts, passwords and secrets, and sessions by iimplementing comprehensive layers of security, control, and monitoring.

The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management as well as mitigate threats at multiple points in the privilege attack chain.

Figure 7: How BeyondTrust's solutions address the Universal Privilege Management core use case.



6 Next Steps

By evolving your PAM capabilities, you will not only reduce the threat surface, eliminate security gaps, improve your response capabilities, and ease compliance, you will also deter many attackers, who are still largely opportunistic in seeking to exploit the easiest prey.

Contact BeyondTrust today to schedule a time to discuss and develop your customized path to Universal Privilege Management, and view these additional resources to help you on your PAM journey.

- PAM Buyer's Guide
- BeyondTrust Solutions

Resources:

"Human Factor Report", Proofpoint, Inc., 2019

"Microsoft Vulnerabilities Report", BeyondTrust, April 2019

"Global Incident Response Threat Report", Carbon Black, April 2019

"The Forrester Wave™: Privileged Identity Management, Q4 2018", Forrester Research, November 2018

"2018 Varonis Global Data Risk Report", Varonis, April 2018

"Privileged Access Threat Report", BeyondTrust, June 2019

"Data Risk in the Third-Party Ecosystem", Opus & Ponemon Institute, November 2018

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 **beyondtrust.com**

V2020_02_ENG