WHITEPAPER

Windows & Mac Privilege Management for Government Agencies

Building a Strong Security Foundation for ICAM & CDM

BeyondTrust

CONTENTS

Introduction

Technological advances and an increased shift to remote work are driving a new era of digital transformation across government agencies. Consequently, privileged access management (PAM) has become imperative to the success of the federal government's mission to securely deliver services to the public.

In this white paper, you will learn:

- Security implications of the “new normal”
- Benefits of least privilege
- Benefits of advanced application control
- What endpoint privilege management is and how it applies to ICAM
- How BeyondTrust Endpoint Privilege Management (EPM) delivers powerful endpoint protection, while enabling users to be their most productive

BeyondTrust is the worldwide leader in Privileged Access Management. Our innovative Universal Privilege Management approach to PAM goes beyond simply managing passwords in a vault for a limited set of privileged users. The company’s integrated PAM solutions enable security and IT professionals to manage the explosion of privileges across their entire enterprise to drastically reduce the attack surface. BeyondTrust’s unique approach to PAM is more relevant than ever amid the challenges of the coronavirus pandemic and the largescale shift to remote work.

Understanding the Cyber Security Implications of the New Normal

The sudden transition to remote working caused many agency IT managers to rethink how to secure networks, as they implemented policies and tools to protect employees working from home. Remote working is certain to become a fixture across the public sector long after the COVID-19 pandemic subsides. Recognizing this shift, government managers are adjusting to the new reality that employees are going to work remotely and, in many cases, use their own devices.

At the same time, agencies will have to rethink endpoint security. Endpoints are no longer just desktops, laptops, and servers, but include smartphones, tablets, wearables, Internet of Things (IoT) technologies, and other non-traditional devices that may connect to corporate systems or the Internet. To ensure secure and efficient operations, government agencies must be able to identify, credential, monitor, and manage all people and devices that access their IT resources and data assets.

According to Verizon's 2020 Data Breach Investigations Report (DBIR), ransomware looms as an outsized problem for public sector agencies, with financially motivated attackers leveraging it to target a diverse array of government entities. While the Verizon report indicated that ransomware accounted for 27% of malware incidents across all industries, within the public sector and education verticals it accounted for 60% and 80% of all malware incidents, respectively.

Cyber attackers stepped up efforts to gain access to government networks and IT systems in response to the massive shift to remote working. Several major hacker groups launched COVID-19 related phishing scams to steal user credentials, according to a joint alert issued by the Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), and the United Kingdom's National Cyber Security Centre (NCSC). The Verizon report also shows that phishing remains one of the most significant threat vectors across all industries.

And it's not just employees. Contractors also need secure access to government networks. This means agencies must have visibility and control over who is on their networks and what they are doing on those networks, at all times. According to BeyondTrust research, public sector organizations have 124 third-party vendors logging into their systems/networks in a typical week. The report also found that 58% of organizations had experienced a breach relating to third-party access.

IT environments continue to become more decentralized, creating new attack pathways. This has put renewed focus on managing identities, credentials, and access to resources for federal decision-makers. Within this environment, privileged identities and privileged access demand the most attention. According to Forrester, 80% of IT breaches today are the result of privileged credential abuse or misuse.

Identity, Credential, and Access Management (ICAM)

The surge in government workers remotely logging on to agency networks raises concerns about whether they have the proper credentials to access the right data, at the right time, for the right purpose. But even before the COVID-19 outbreak pushed millions of people into remote working, the federal government has been focused on strengthening its Identity, Credential, and Access Management (ICAM) policies.

In May 2019, the Office of Management and Budget (OMB) issued updates to the federal government's ICAM policy. The policy calls on agencies to take a risk management approach to identity management and align with the National Institute of Standards and Technology (NIST) guidelines, as well as related identity management guidance issued by the Office of Personnel Management and DHS. This will give agencies a comprehensive approach to identity-based security that also safeguards data privacy, according to the OMB.

Current reviews of federal ICAM policies are raising awareness that identity, credential, and access management must be an integral part of cyber security. Many agency managers lack a clear sense of who has access to their systems or are not fully aware of the ramifications of giving administrative privileges to a wide range of staff and contractors. The primary concept behind this more recent ICAM push is to go beyond traditional viewpoints around perimeter-based security and access, and to approach network access from a more holistic governance and management perspective.

Identity, credential, and access management all combine in unique ways to create threat vectors that require mitigation by federal agencies. One example of a multi-vector threat is when a vendor has access to sensitive networks *and* employs contractors who should not be credentialed to access those assets. Clearly, this is a situation in which IT and security managers need full visibility and granular control over contractor and subcontractor access, including the ability to enforce least privilege access to prevent opening risky pathways into their environment.

The ICAM policy recognizes the importance of protecting, managing, and monitoring privileged and administrative accounts, including the ability to revoke or destroy credentials in a timely manner. Privileged credential and session management is a core capability of the BeyondTrust Password Safe solution.

However, there is also importance in having a firm grasp on the "access" pillar of ICAM. While it begins with verifying identity, and then ensuring that those appropriate identities have been credentialed, managing the access these accounts have to sensitive systems and data cannot be an afterthought. DHS has determined that these identity-centric concepts all maintain an integrated relationship, yet, need to be considered separately for the purpose of determining the appropriate federated strategy to strengthen cyber security efforts as a whole.

Understanding the Least Privilege Concept

The principle of least privilege (PoLP) is at the heart of the ICAM "access" concept, and enforcing it is arguably the most cost-effective way to improve security and increase both IT and end-user productivity.

When a user has local administrator rights, it means that they have the privileges to perform most, if not all, functions within an operating system on a computer. These privileges can include such tasks as installing software and hardware drivers, changing system settings, or installing system updates. Privileges can also enable the creation of user accounts and changing of passwords. Privileges provide attackers the means they need to make system changes, access resources, and cover their tracks.

Overprovisioning of privileges also has security implications for applications. Some applications in use at an agency may be unknown ("shadow IT") to the IT team. And the shadow IT problem has become even more pronounced with the increase in remote work and digital transformation. Malware can run with the same privileges of the exploited user or application. When malware exploits an asset or user with full admin rights, security controls can be bypassed, and software can be installed and run.

While many organizations freely assign local admin rights to ease the need for IT support, they are leaving themselves at high risk of a security breach. Applying least privilege allows a user, application, asset, etc. the minimum amount of permissions required to execute a specific task or function, for the least amount of time necessary.

Restricting usage based on time or completion of a specific task is referred to as just-in-time (JIT) access. Least privilege is recognized as one of the most fundamental security IT strategies, yet, agencies have lagged in fully implementing it across endpoints, especially when it comes to enforcing just-in-time access.

What is Endpoint Privilege Management?

Endpoint privilege management technologies allow organizations to control exactly what actions can and cannot be performed by any given endpoint. Gartner refers to the capabilities conferred by these tools as privilege elevation and delegation management (PEDM). As mentioned earlier, an endpoint can be any type of connected device, such as desktop, laptop, server, mobile device, and even IoT. However, this white paper is focused primarily on the concepts around securing Windows and Mac endpoints.

As opposed to signature-based tools, such as antivirus (AV), which rely on code matches and heuristics, endpoint privilege management solutions are policy-driven. These solutions enable the precise level of privilege a user or endpoint needs, and nothing more.

The BeyondTrust Microsoft Vulnerabilities Report showed that removing admin rights would mitigate 77% of all Critical Microsoft vulnerabilities in 2019, 100% of Critical vulnerabilities in Internet Explorer & Edge, and 80% of Critical vulnerabilities affecting Windows 7, 8.1, and 10. Other research has also demonstrated a similar risk reduction across third-party applications when removing admin rights.

By enforcing least privilege via an endpoint privilege management solution, agencies can dramatically reduce the threat surface against both internal and external attacks, while allowing employees just enough access to remain productive in their roles. Modern solutions, such as the one from BeyondTrust, can elevate access to applications without provisioning extra privileges to the end-users themselves.

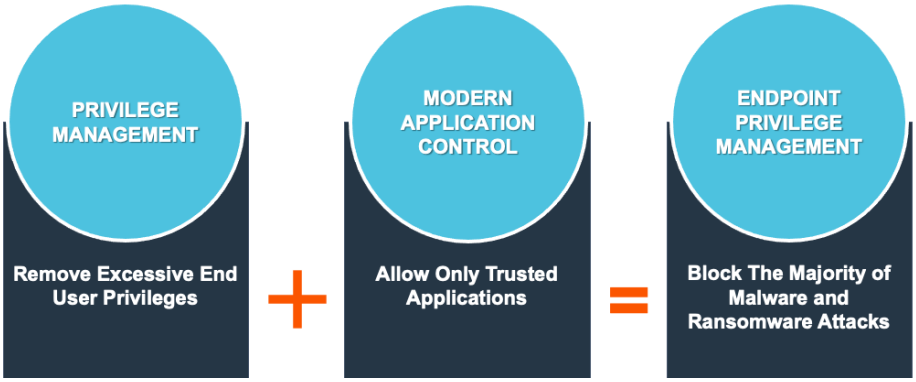


Figure: Endpoint privilege management solutions provide the combined capabilities of privilege elevation/delegation management and application control.

Modern endpoint privilege management solutions also include application control capabilities, which apply such functionalities as block lists, allow lists, and grey lists to ensure users have seamless access to the applications they need, while being protected from malicious software and executables.

Protecting Windows & Mac Endpoints with BeyondTrust

BeyondTrust Endpoint Privilege Management, which is comprised of Privilege Management for Windows & Mac and Privilege Management for Unix & Linux, is widely recognized by analysts as the most comprehensive endpoint solution currently available.

Privilege Management for Windows & Mac can often be applied in just hours or days, and at tremendous scale. Our solution also complements the traditional privilege elevation and delegation capabilities expected of an endpoint privilege management solution with advanced application control and protection. Together, these capabilities dramatically condense an agency's attack surface, while also boosting operational productivity. Today, our solution secures over 50 million endpoints worldwide.

Outlined below are the ways that BeyondTrust Privilege Management for Windows & Mac protects agencies from internal and external attacks, while enhancing productivity:

- ***Enables Least Privilege:*** Restricts admin rights for users, accounts, applications, and computing processes to only those capabilities/resources absolutely required to perform routine, legitimate activities. This aligns perfectly with the CDM program, which pertains to functional areas related to endpoint integrity, least-privilege access, and infrastructure.

- ***Applies Pragmatic Application Control Capabilities:*** Delivers trust-based pragmatic application control, with a flexible policy engine to set broad rules. Agencies can choose automatic approval for advanced users – protected by full audit trails – or utilize challenge-response codes. These capabilities align with several security controls across NIST Special Publications (SP) 800-53 and SP 800-171 covering access control and risk assessment.

- ***Provides Trusted Application Protection (TAP) Capability:*** Trusted Application Protection adds context to the process tree across Windows, allowing restriction of common attack chain tools, such as PowerShell and wscript that are spawned from commonly used applications, such as browsers or document handlers (Word, PowerPoint, Excel). TAP does not rely on reputation or signatures.

- ***Integrates with your IT/Security Ecosystem:*** By leveraging built-in connectors to third-party solutions, including ITSM applications and SIEM (security information and event management) tools, agencies can benefit from many technology synergies and improve their security solution ROI.

- ***Enables Rapid Leaps in Risk Reduction and Productivity:*** The BeyondTrust Quick Start feature can be configured to deliver risk-reduction power in hours, with out-of-the-box workstyle templates that provide unmatched time-to-value. This means achieving least privilege has never been easier or less obtrusive to end-user productivity, which also helps ease the stress and workload of IT administrators.

With comprehensive features available via both on-premises and cloud offerings, agencies have a choice of deployment methods to suit their unique needs. BeyondTrust's cloud-based solution delivers the same high availability, security, access, and scalability as our market-leading on-premises offering, while removing the overhead of managing infrastructure.

ICAM, CDM, and the Evolving Security Landscape

In the updated ICAM policy, OMB acknowledged that while hardening the network perimeter is important, "agencies must shift from simply managing access inside and outside of the perimeter to using identity as the underpinning for managing the risk posed by attempts to access federal resources made by users and information systems."

To achieve this outcome, agency managers need better visibility into what is happening on their networks. Each agency must define and maintain a single, comprehensive ICAM policy, process, and technology solution roadmap that is consistent with their operational mission needs. It must also align with the government's Continuous Diagnostics and Mitigation (CDM) program.

Managed by DHS, the CDM program works to ensure that federal agencies always know:

- What is on their network
- Who is on their network
- What is happening on their network

Satisfying these three needs is important for establishing a strong network visibility and data protection baseline across the federal government. This level of visibility must be met for agencies to effectively monitor, defend, and rapidly respond to cyber incidents. CDM helps drive achievement of this baseline by working with agencies to deploy tools that provide enterprise-wide visibility of the assets, users, and activities on their networks.

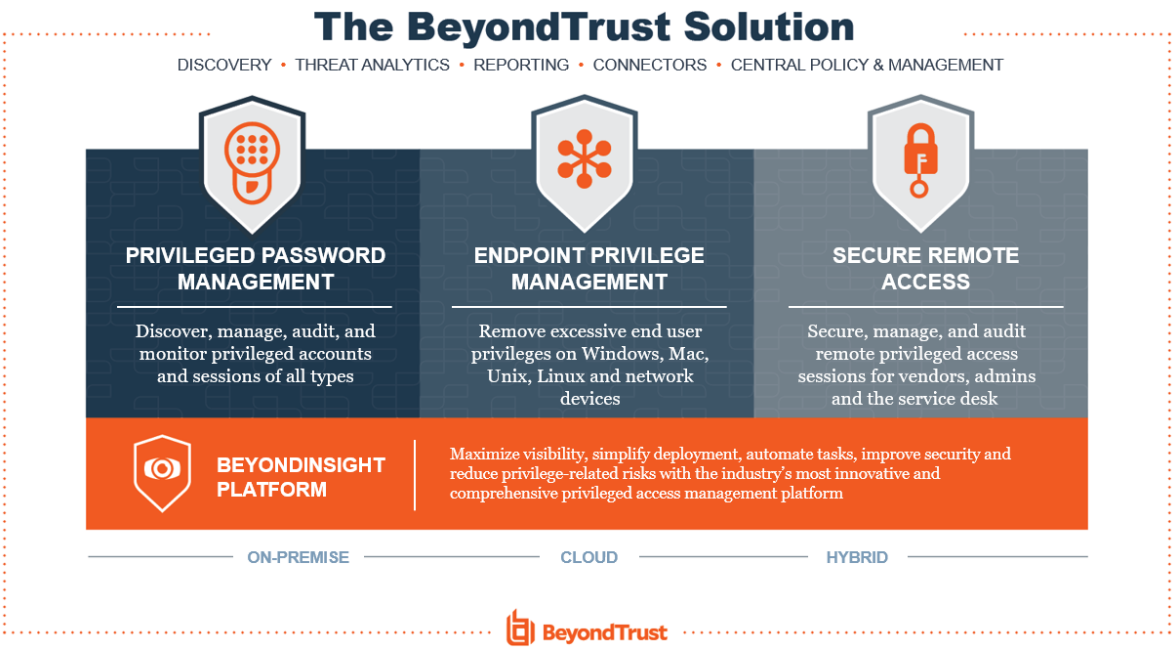
The BeyondTrust Privileged Access Management Platform

While the focus of this white paper was primarily on endpoint privilege management for Windows & Macs, BeyondTrust provides a holistic PAM platform that enables agencies to secure every endpoint, asset, and privileged session across their entire on-premises and cloud environments, including Windows, Mac, Unix, Linux, etc.

BeyondTrust solutions help you align with federal ICAM policies and the CDM program, meet compliance requirements, and significantly improve operational efficiency. The BeyondTrust PAM platform—which is comprised of Endpoint Privilege Management, Privileged Password Management, and Secure Remote Access—helps agencies see and control what's on their network, what is connected to their network, and what devices and identities are accessing resources on their network.

This holistic approach condenses the attack surface, limits lateral movement, and protects against any type of threat actor—whether insider, external attacker, machine, malware, or human. Moreover, BeyondTrust has built powerful application programming interfaces (APIs) into our solutions. These APIs link to a wide range of tools and devices, helping to gather and communicate data to elastic dashboards for real-time analysis and orchestration. This is extremely important in today's government environment in which remote and mobile access is the default way many people work.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. 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's Universal Privilege Management model provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

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_12_ENG