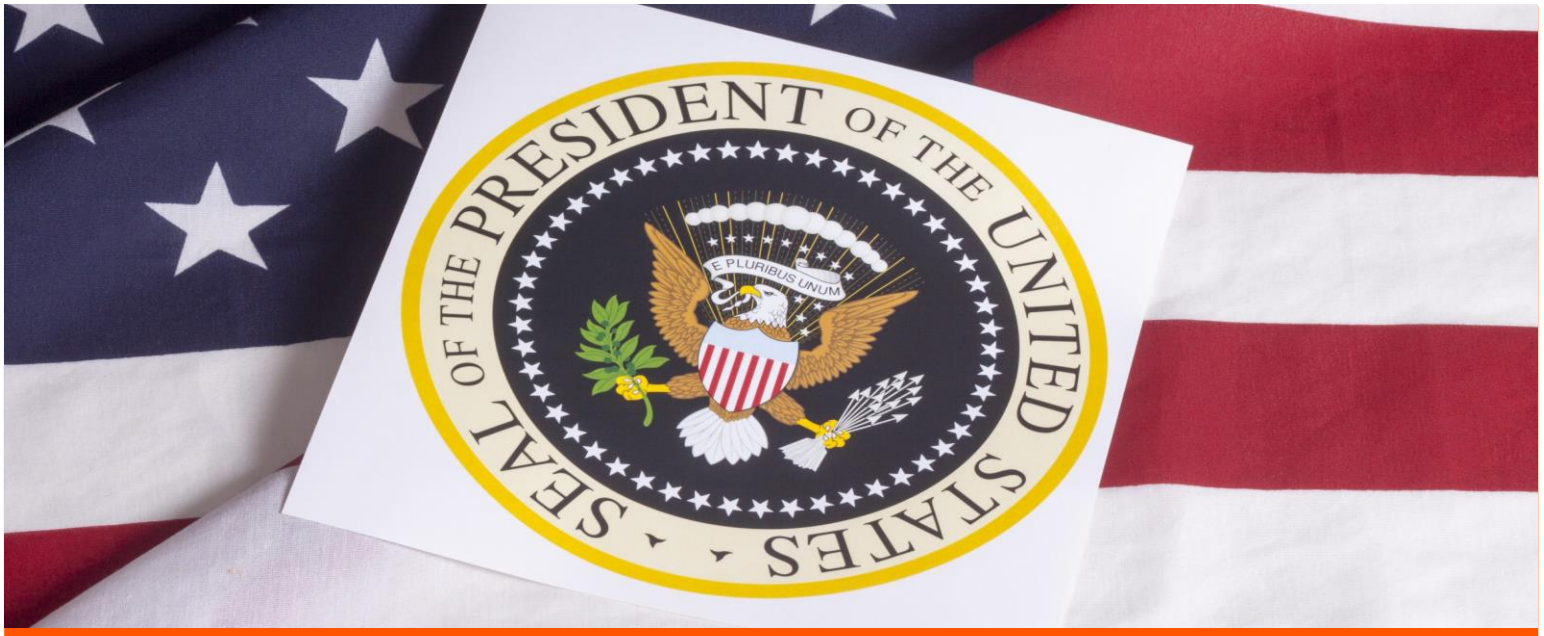
SOLUTION BRIEF



EXECUTIVE ORDER
ON IMPROVING THE NATION'S CYBERSECURITY

The Role of Privileged Access Management

BeyondTrust

The Executive Order on Improving the Nation's Cybersecurity

President Biden's May 12, 2021 Executive Order (EO) has accelerated and highlighted the crucial need to improve U.S. cybersecurity. The EO is inclusive of both guidelines and timelines that agencies must meet to keep pace with the evolving threat landscape. Biden's 2022 Fiscal Budget allocates $9.8 billion in cybersecurity funding to secure federal agencies.

The EO is a direct response to a wave of widely disruptive cyberattacks in the first half of 2021. According to a White House statement, "Recent cybersecurity incidents such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident are a sobering reminder that U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals. These incidents share commonalities, including insufficient cybersecurity defenses that leave public and private sector entities more vulnerable to incidents."

The Executive Order is an important step for the Biden administration's efforts to enhance cybersecurity at the federal government level, including standardizing cybersecurity requirements and policies among agencies, and strengthening collaboration and cybersecurity information sharing with government contractors.

Zero Trust and Software Supply Chain security approaches have been gaining momentum within the federal sector and are key focus areas in the cybersecurity EO.

Zero Trust

Within 60 days (of May 12, 2021), each agency must, "develop a plan to implement a Zero Trust Architecture, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance."

Software Supply Chain Security

Another noteworthy component of the EO in Section 4: Enhancing Software Supply Chain Security is the focus on securing privileged accounts and credentials. The EO states, "The security and integrity of 'critical software' — software that performs functions critical to trust (such as affording or requiring elevated system privileges or

direct access to networking and computing resources) — is a particular concern. Accordingly, the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software."

In collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), the Office of Management and Budget (OMB), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA), NIST was charged with publishing an updated definition of "critical software, conceptualizing a phased implementation, and a developing a preliminary list of common categories of software that would fall within the scope for the initial phase.

NIST defines "critical software" as "any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

- Is designed to run with elevated privilege or manage privileges;
- Has direct or privileged access to networking or computing resources;
- Is designed to control access to data or operational technology;
- Performs a function critical to trust; or,
- Operates outside of normal trust boundaries with privileged access.

While this EO is targeted at federal agencies, it is anticipated that other sectors will quickly adopt the requirements as embodying industry best practices.

The Role of Privileged Access Management

As highlighted by NIST, Privileged Access Management (PAM) is arguably one of the most critical cybersecurity areas to get right. No identities are more imperative to secure than those with privileged access to systems, data, applications, and other sensitive resources. Almost every attack today requires privilege for the initial exploit or to laterally move within a network.

PAM protects privileged credentials, granularly enforces least privilege, and monitors and manages every session involving privileged access -- whether human, machine, employee or vendor.

PAM solutions can protect agencies by:

- Implementing credential management best practices to prevent credentials from being stolen or misused.

- Enforcing least-privilege across users, applications, systems, etc. to drastically reduce the attack surface and minimize potential lateral access pathways.

- Ensuring elevated access is only given when contextual parameters are met and is immediately revoked after the activity is performed or the context has changed.

- Securing remote access for employees or contractors -- without a VPN -- and enabling agencies to lock down access to cloud, virtual and DevOps control planes and other consoles.

- Monitoring and managing every privileged session, providing an unimpeachable audit trail, and the ability to pause or terminate suspicious sessions.

These core capabilities of a robust Privileged Access Management solution also help enable a zero trust security posture. PAM reduces the threat surface and minimizes the threat windows during which attackers can inflict damage, helping to protect against everything from simple malware to advanced persistent threats.

Mapping BeyondTrust PAM Solutions to the Executive Order

BeyondTrust is the worldwide leader in Privileged Access Management, empowering organizations to secure and manage their entire universe of privileges.

The EO requirements outlined in the following table are mapped to the BeyondTrust solutions that help you meet the corresponding requirements:

- (PPM) Privileged Password Management - Enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and audit all privileged activities.

- (SRA) Secure Remote Access - Apply least privilege and robust audit controls to all remote access required by employees, vendors, contractors, and service desks.

- (EPM) Endpoint Privilege Management - Combine privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices, without hindering productivity.

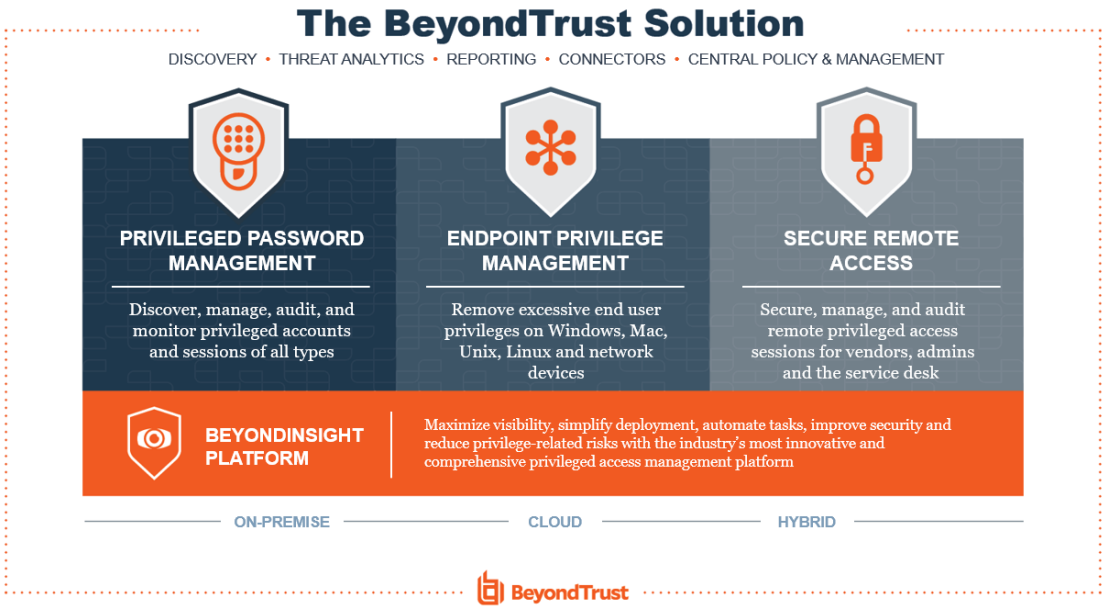
Requirement	How BeyondTrust Can Help	BeyondTrust Solutions		
		PPM	SRA	EPM
Zero Trust Architecture (3.a)	BeyondTrust solutions deliver identity-centric security that secures against both external and internal threats and stands at the core of any Zero Trust strategy. These solutions work together with our BeyondInsight console to give agencies a unified view of actions, key stroke, analytics and reporting.	■	■	■
Advancement of Cloud-based Solutions (3.a)	All of BeyondTrust's solutions are available as cloud-based deployments, and BeyondTrust has more PAM cloud customers than any other vendor.	■	■	■
Planning for ZTA (3.b.ii)	This section requires the development of a plan to implement a Zero Trust Architecture, including prioritizing what needs to be done to make the biggest impact. BeyondTrust's network of federal integrators and partners will work together with an agency to develop a plan to implement a Zero Trust Architecture. Because each solution can stand alone, these plans can be customized to prioritize individual agency needs.	■	■	■
Cloud with ZTA (3.c)	This section states that, as agencies make cloud migration a priority, they shall implement cloud solutions a with Zero Trust Architecture. Not only are all BeyondTrust solutions available as cloud deployments with features that enable Zero Trust goals, BeyondTrust Cloud Privilege Broker is an entitlements and permissions management solution that enables agencies to visualize and manage cloud access risk in hybrid and multicloud environments—all from a single interface *(available 2H 2021).*	■		
Multi-Factor Authentication (3.d)	BeyondTrust's Password Safe solution enables agencies to implement segmentation rules to legacy devices that may not currently support MFA. By leveraging BeyondTrust, devices without native support for MFA can only be accessed	■	■	

Requirement	How BeyondTrust Can Help	BeyondTrust Solutions		
		PPM	SRA	EPM
	leveraging an MFA-enabled solution. This allows the continued use of devices that would otherwise be non-compliant.			
Risk Based Authentication (4.e.i.C)	This section requires NIST to publish preliminary guidelines for the security of the software supply chain, and specifically dictates establishing "multi-factor, risk-based authentication and conditional access across the enterprise. " BeyondTrust's solution not only support MFA, but also can support integration with solutions like Virus Total. These capabilities, along with location awareness on login, allow for supporting risk-based authentication and conditional access.	■	■	■
Least Privilege (4.i)	This section requires NIST to publish guidelines for critical software including "applying practices of least privilege." Enabling least privilege is a fundamental capability of the BeyondTrust PAM solution, removing excessive end user privileges and eliminating local admin rights and root access.	■		■

The Beyondtrust Privileged Access Management Solution

The BeyondTrust Privileged Access Management portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. In the Gartner Magic Quadrant for Privileged Access Management, BeyondTrust is named as a leader for all solution categories in the PAM market.



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 agencies 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.

V2021_06_ENG