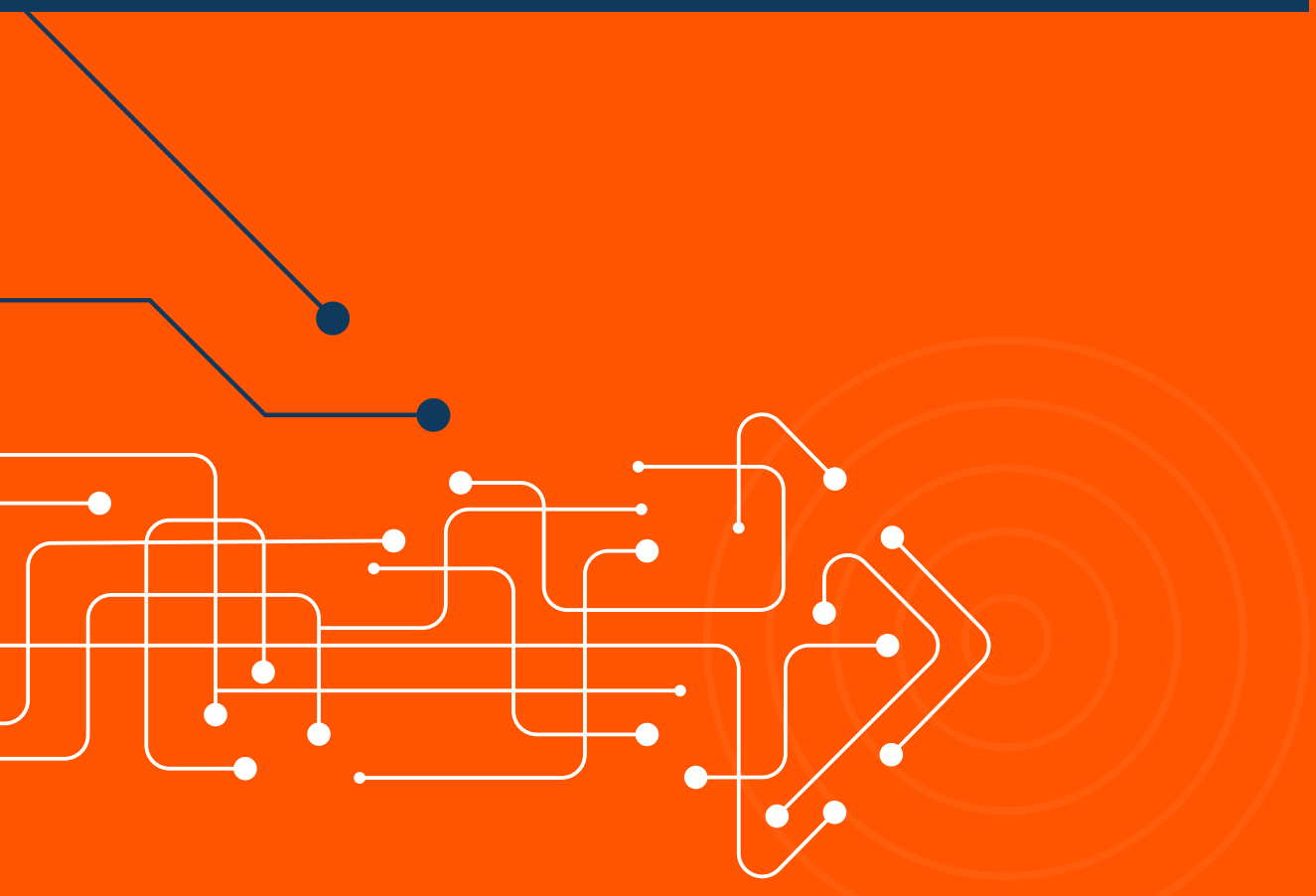
BeyondTrust

Mapping PAM to the Canadian Centre for Cyber Security's ITSM.10.089

Top 10 IT Security Actions to protect internet-connected networks and information



BeyondTrust

TABLE OF CONTENTS

Overview 3

About the BeyondTrust Pathfinder Platform & The Canadian Centre for Cyber Security's ITSM.10.089 4

The Top 10 IT Security Actions & BeyondTrust 5

1. Consolidate, Monitor, and Defend Internet Gateways 5

2. Patch Operating Systems and Applications 6

3. Enforce the Management of Administrative Privileges 7

7. Protect Information at the Enterprise Level 8

8. App Protection at the Host Level 9

9. Isolate Web-Facing Applications 9

10. Implement Application Allow Lists 10

Mapping BeyondTrust PAM to the ITSM.10.089 Security Actions 11

Conclusion: BeyondTrust Satisfies Multiple Top 10 IT Security Recommendations by the CCCS 16

Ready for the Next Step? 16

The BeyondTrust Pathfinder Platform 17

About BeyondTrust 18

This document is informational and is intended to provide guidance on how organizations may use BeyondTrust solutions to better meet or align to the Canadian Centre for Cyber Security's ITSM.10.089—Top 10 IT Security Actions to protect internet-connected networks and information. We are not representing that we are subject to or compliant with the security actions referenced within ITSM.10.089.

Overview

On September 21, 2021, the Canadian Centre for Cyber Security (CCCS) released Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information (ITSM.10.089), replacing previous guidance (ITSM.10.189 and ITSB-89 v3). This publication outlines key cybersecurity actions Canadian organizations should implement to safeguard internet-connected networks and sensitive information from evolving threats.

The 10 recommended actions serve as a baseline for strengthening IT infrastructure. While CCCS advises organizations to follow the order of recommendations for optimal protection, adjustments may be necessary based on specific architectures and security needs. A risk assessment is encouraged to tailor these measures accordingly, particularly for cloud and managed service environments.

The Top 10 IT Security Actions include:

1. Consolidate, Monitor, and Defend Internet Gateways
2. Patch Operating Systems and Applications
3. Enforce the Management of Administrative Privileges
4. Harden Operating Systems and Applications
5. Segment and Separate Information
6. Provide Tailored Training
7. Protect Information at the Enterprise Level
8. Apply Protection at the Host Level
9. Isolate Web-Facing Applications
10. Implement Application Allow Lists

About the BeyondTrust Pathfinder Platform & The Canadian Centre for Cyber Security's ITSM.10.089

ITSM.10.089 emphasizes the importance of conducting a risk assessment to identify security priorities and tailor recommended actions to an organization's unique environment. While these ten actions provide a strong security foundation, CCCS acknowledges that no single strategy can fully prevent cyber incidents, particularly as threat landscapes evolve. Additionally, the application of these recommendations may vary depending on how an organization utilizes cloud and managed services.

The BeyondTrust Pathfinder Platform supports alignment with ITSM.10.089 recommendations by providing holistic visibility and control over an organization's identity attack surface. By unifying identity security management, governance, and enforcement, Pathfinder enables organizations to:

- Proactively identify and close security gaps across identities, entitlements, and access
- Extend security controls, such as least privilege enforcement and access governance, across all environments
- Rapidly detect and respond to identity-based threats
- Streamline security operations, enhancing compliance readiness and administrative efficiency

When examining the security recommendations laid forth in the CCCS's Top 10 IT security actions to protect Government of Canada internet-connected networks and information, it becomes evident that identity security capabilities, including privileged access management (PAM), play a significant role across most actions in the publication.

In this document, we focus on the ITSM.10.089 actions where BeyondTrust solutions can help provide alignment or support—specifically actions 1-3 and 7-10. We'll outline how our Pathfinder platform and security solutions help organizations implement these recommendations, highlighting the key features and capabilities that strengthen identity security and reduce risk.

The Top 10 IT Security Actions & BeyondTrust

Consolidate, Monitor, and Defend Internet Gateways

> "GC departments and agencies should reduce the number of discrete external connections to their departmental networks by using Shared Services Canada's consolidated Internet gateways. Your organization should also monitor its domain name system (DNS) server. The Canadian Internet Registration Authority (CIRA) offers a free protected DNS service, Canadian Shield, that prevents you from connecting to malicious websites that might infect devices or steal personal information.
>
> Your organization is responsible for monitoring all incoming and outgoing traffic at these gateways, even if you are using cloud services. To simplify this task, reduce the number of external connections to your network. You should establish a baseline of normal traffic patterns first, which enables you to detect and react to changes in these patterns."
>
> **— Canadian Centre for Cyber Security, Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089), 2.1**

This action focuses primarily on consolidation of internet gateways and the number of discrete external connections, while monitoring domain name servers and monitoring for malicious websites that might infect devices or steal information. Though BeyondTrust doesn't directly address this action, our PAM solutions can be configured to allow secure access to and from devices. However, PAM does not offer any direct DNS monitoring, monitoring of incoming or outgoing traffic, or reduction of external connections.

Patch Operating Systems and Applications

> "Implement a patch management policy for operating systems and third-party applications to reduce your organization's exposure to publicly known vulnerabilities. When a vendor issues a security patch, you should follow your patch management process to apply the patch as soon as possible. You can use an automatic patch management system to apply patches in a timely manner.
>
> Use supported, up-to-date, and tested versions of operating systems and applications. Using unsupported operating systems or applications, for which updates are not provided, increases your risk of exposure to exploitation because there is no mechanism available to mitigate vulnerabilities."
>
> **— Canadian Centre for Cyber Security, Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089), 2.2**

BeyondTrust Password Safe can support partial alignment to recommendation 2.2 because it auto-discovers endpoint data of local accounts (servers, desktops, laptops, work stations, etc.). While not a patch management solution, the inventorying aspect and versioning enumeration partially aligns with this control.

Threat actors seek elevated privileges to gain an initial foothold and then move laterally across networks. BeyondTrust Endpoint Privilege Management (EPM) helps reduce this risk by discovering unmanaged endpoints and enforcing least privilege across devices. While EPM does not perform patch management, it complements those tools by controlling the privileges that can be exploited by unpatched vulnerabilities. By limiting admin rights and restricting application execution, EPM helps prevent the exploitation of both known and zero-day vulnerabilities, providing a protective layer of defense in alignment with sections of 2.2.

#3 Enforce the Management of Administrative Privileges

> "Apply the principle of least privilege to ensure that users only have the access and the privileges they need to carry out their job functions. You should limit the number of administrative or privileged users for operating systems and applications. Create different levels of administrative accounts so that, if an administrative account is compromised, the level of exposure is limited. To prevent exposure from phishing attacks or malware, administrators should perform administrative functions on dedicated workstations that do not have Internet or open email access, or that have Internet and email disabled from administrative accounts.
>
> Administrators should have separate administrative accounts and general user accounts; administrators should use their administrator accounts only for administrative tasks and use their general user accounts for other tasks (e.g. checking emails). Your organization should implement an administrative password solution to protect passwords. Frequently review and revalidate your organization's list of administrative users; you should ensure that privileges are revoked when users no longer require them (e.g. personnel and role changes)."
>
> **— Canadian Centre for Cyber Security, Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089), 2.3**

The BeyondTrust Pathfinder platform can help support organizations' alignment with many aspects of this action. BeyondTrust helps organizations enforce the principle of least privilege and manage administrative access effectively through three key, integrated solutions: Identity Security Insights, Entitle, and Endpoint Privilege Management (EPM). Together, these solutions provide the visibility, control, and automation needed to minimize privilege-related risks across the enterprise.

- **Identity Security Insights®** provides a unified view of all identities, accounts, and privileged access, entitlements, and permissions across the environment. By continuously analyzing identity relationships, risk levels, and anomalous activity, organizations can proactively harden their environment and detect and remediate privilege escalation threats before they lead to compromise.

- **Entitle** ensures that privileged access is granted only when necessary, using just-in-time access controls to prevent excessive standing privileges. Organizations can apply the principle of least privilege, sharply reducing the number of unused permissions in their IaaS, PaaS, and SaaS environment. Self-service and access request automation, auto-revoke policies, and automated user access reviews streamline administrative work, simplifying the proper management of privileged identities.

- **Endpoint Privilege Management (EPM)** enforces least privilege at the operating system level, allowing users to perform necessary tasks without requiring full administrative rights. EPM controls application access, blocks unauthorized executables, and restricts privilege elevation, helping prevent lateral movement and reducing the risk of compromise. Administrators can use separate accounts for privileged tasks and general use, with policies that isolate admin activity from everyday computing.

By combining real-time visibility, just-in-time (JIT) privilege enforcement, and granular least privilege controls, BeyondTrust solutions can support organizations' alignment with ITSM.10.089 security action 2.3, strengthening defenses against credential-based attacks and unauthorized privilege escalation. Our ability to provide least privilege defense-in-depth can also proactively mitigate many vulnerabilities, even in the absence of patching.

#7 Protect Information at the Enterprise Level

> "Your organization's information is valuable to your continued operation, but it is also a valuable target to threat actors. You should ensure that you are managing information appropriately through its lifecycle (e.g. data labelling, handling, retention, and destruction."
>
> **— Canadian Centre for Cyber Security, Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089), 2.7**

BeyondTrust's entire Pathfinder platform supports alignment with this recommended action by providing the foundational capabilities of least privilege access enforcement and granular application controls across systems and devices like servers, workstations, desktops, laptops, mobile devices, POS devices, and other assets used to access enterprise resources.

#8 App Protection at the Host Level

> "You should deploy a host-based intrusion prevention system (HIPS) to protect your organization's systems against both known and unknown malicious attacks, such as viruses and malware. There are many commercial vendors that provide HIPS services."
>
> **— Canadian Centre for Cyber Security, Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089), 2.8**

Though our solutions don't directly enable the HIPS capabilities this action recommends, BeyondTrust solutions offer features that can help support the operating systems and visibility component of this action. BeyondTrust solutions can be deployed on various hosts to protect against malware that leverages privilege and Paths to Privilege™ to execute on the host.

BeyondTrust's total PASM solution, comprised of Privileged Remote Access and Password Safe, along with Entitle, have permission management capabilities in Saas/IaaS environments that allow control access to AV and firewall consoles.

When it comes to malicious attacks, BeyondTrust solutions can be deployed to provide visibility for identity-based threats and used to protect and alert an organization when a threat is detected. Additionally, it is important to note that ensuring HIPS configurations cannot be changed by a comprised user account.

#9 Isolate Web-Facing Applications

> "Your organization should use virtualization to create an environment where web-facing applications can run in isolation (i.e. in a sandbox). By isolating these applications, malware, for example, is confined to your virtualized environment and cannot spread and infect the host or enterprise."
>
> **— Canadian Centre for Cyber Security, Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089), 2.9**

BeyondTrust provides various approaches to this action, including enabling segmented access to server-hosted, web-facing applications, or the applications themselves. BeyondTrust solutions can help support alignment with this action at the operating system level via our Endpoint Privilege Management product's ability to restrict access and application usage, while minimizing malware-related threats.

Implement Application Allow Lists

> "Your organization should create this list of applications that are authorized for use in the workplace and that are known to be from trustworthy vendors. All other applications and application components should be denied by default. You can define your allow list by using file and folder attributes (e.g. file path, file name, file size, digital signature or publisher, or cryptographic hash). You should define and deploy policies on allow lists across the organization. Remember to update your allow list when you patch or install an update for an application or when you start or stop using software."
>
> **— Canadian Centre for Cyber Security, Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089), 2.10**

The BeyondTrust Platform can help support alignment with this action at the operating system level by providing control over which applications / executables can be run based upon policy. Additionally, BeyondTrust Endpoint Privilege Management offers unique command-line restrictions when leveraging session management with Unix / Linux (SSH) sessions when configured.

Mapping BeyondTrust PAM to the ITSM.10.089 Security Actions

Action Title	Action Description	Password Safe	Privileged Remote Access	Remote Support	Endpoint Privilege Management	Identity Security Insights	Entitle	Active Directory Bridge
2.1 Consolidate, Monitor, and Defend Internet Gateways	GC departments and agencies should reduce the number of discrete external connections to their departmental networks by using Shared Services Canada's consolidated Internet gateways. Your organization should also monitor its domain name system (DNS) server. The Canadian Internet Registration Authority (CIRA) offers a free protected DNS service, Canadian Shield, that prevents you from connecting to malicious websites that might infect devices or steal personal information. Your organization is responsible for monitoring all incoming and outgoing traffic at these gateways, even if you are using cloud services. To simplify this task, reduce the number of external connections to your network. You should establish a baseline of normal traffic patterns first, which enables you to detect and react to changes in these patterns.							

Action Title	Action Description	Password Safe	Privileged Remote Access	Remote Support	Endpoint Privilege Management	Identity Security Insights	Entitle	Active Directory Bridge
2.2 Patch Operating Systems and Applications	Implement a patch management policy for operating systems and third-party applications to reduce your organization's exposure to publicly known vulnerabilities. When a vendor issues a security patch, you should follow your patch management process to apply the patch as soon as possible. You can use an automatic patch management system to apply patches in a timely manner. Use supported, up-to-date, and tested versions of operating systems and applications. Using unsupported operating systems or applications, for which updates are not provided, increases your risk of exposure to exploitation because there is no mechanism available to mitigate vulnerabilities	Partial			Partial			

Action Title	Action Description	Password Safe	Privileged Remote Access	Remote Support	Endpoint Privilege Management	Identity Security Insights	Entitle	Active Directory Bridge
2.3 Enforce the Management of Administrative Privileges	Apply the principle of least privilege to ensure that users only have the access and the privileges they need to carry out their job functions. You should limit the number of administrative or privileged users for operating systems and applications. Create different levels of administrative accounts so that, if an administrative account is compromised, the level of exposure is limited. To prevent exposure from phishing attacks or malware, administrators should perform administrative functions on dedicated workstations that do not have Internet or open email access, or that have Internet and email disabled from administrative accounts. Administrators should have separate administrative accounts and general user accounts; administrators should use their administrator accounts only for administrative tasks and use their general user accounts for other tasks (e.g. checking emails). Your organization should implement an administrative password solution to protect passwords. Frequently review and revalidate your organization's list of administrative users; you should ensure that privileges are revoked when users no longer require them (e.g. personnel and role changes).	Full	Full	Partial	Full	Partial	Full	Full

Action Title	Action Description	Password Safe	Privileged Remote Access	Remote Support	Endpoint Privilege Management	Identity Security Insights	Entitle	Active Directory Bridge
2.7 Protect Information at the Enterprise Level	When deploying mobile devices in your organization, you should consider the risks and benefits of various deployment models. If it makes business sense, your organization should provide equipment (e.g. servers, desktops, laptops, mobile devices) to employees, using a device management framework and a configuration change management process. If your organization chooses to allow employees to use their personal devices for business, you should implement a strict control policy and review technologies and legal requirements for segregating business and personal information. Your organization can use unified endpoint management (UEM) to maintain the security of mobile devices. UEM combines features from mobile device management and enterprise mobility management processes.	Partial	Partial	Partial	Partial	Partial		Partial
2.8 App Protection at the Host Level	You should deploy a host-based intrusion prevention system (HIPS) to protect your organization's systems against both known and unknown malicious attacks, such as viruses and malware. There are many commercial vendors that provide HIPS services.				Partial	Partial		

Action Title	Action Description	Password Safe	Privileged Remote Access	Remote Support	Endpoint Privilege Management	Identity Security Insights	Entitle	Active Directory Bridge
2.9 Isolate Web-Facing Applications	Your organization should use virtualization to create an environment where web-facing applications can run in isolation (i.e. in a sandbox). By isolating these applications, malware, for example, is confined to your virtualized environment and cannot spread and infect the host or enterprise.	Partial	Partial	Partial	Full			
2.10 Implement Application Allow Lists	Your organization should create this list of applications that are authorized for use in the workplace and that are known to be from trustworthy vendors. All other applications and application components should be denied by default. You can define your allow list by using file and folder attributes (e.g. file path, file name, file size, digital signature or publisher, or cryptographic hash). You should define and deploy policies on allow lists across the organization. Remember to update your allow list when you patch or install an update for an application or when you start or stop using software.	Partial			Full			

Conclusion: BeyondTrust Solutions Support Alignment with Multiple Top 10 IT Security Recommendations by the CCCS

Why Partner with BeyondTrust?

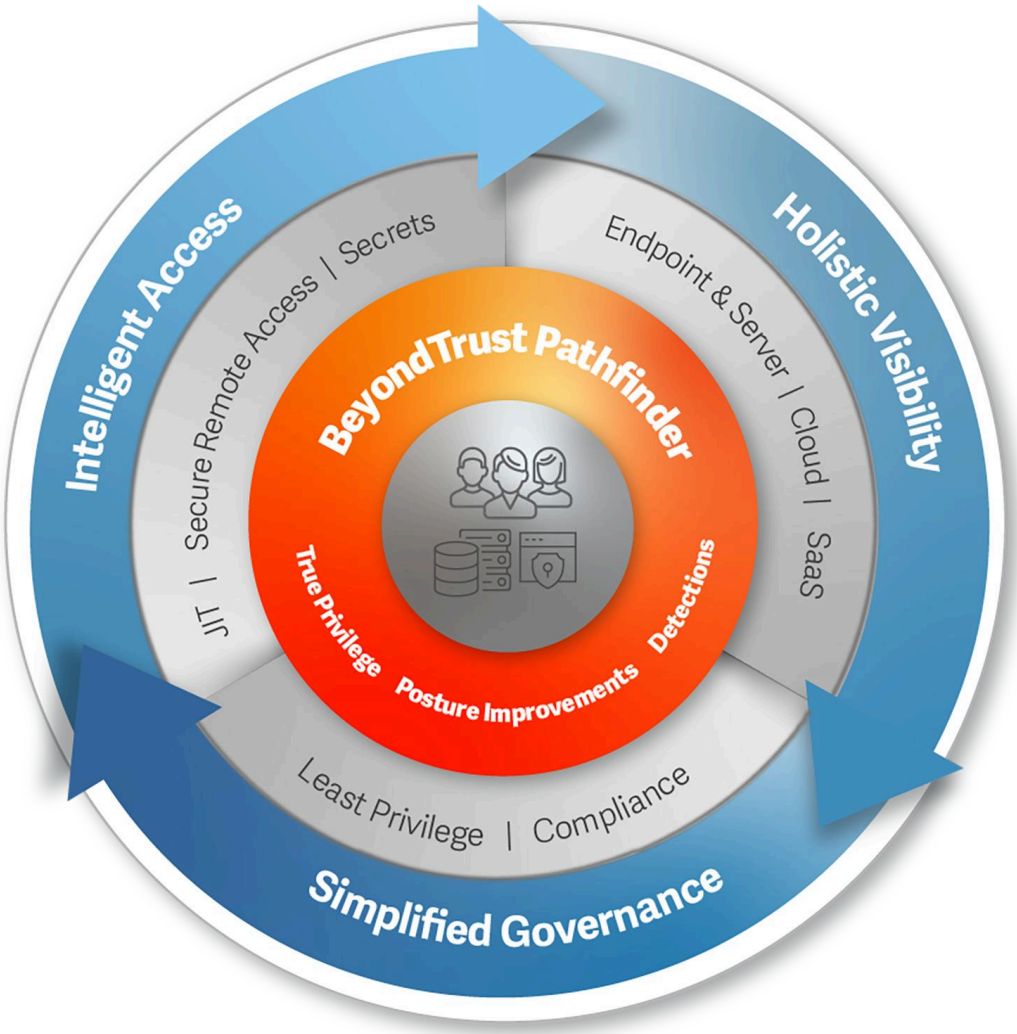
- BeyondTrust addresses major identity security use cases, including privileged access management (PAM), secrets management, identity threat detection and response (ITDR), cloud infrastructure entitlement management (CIEM), remote support, and more. Our comprehensive solutions include substantive capabilities no other vendor delivers.
- Our next-generation capabilities extend your line-of-sight to privileged threat pathways and identity-based attack chains far beyond the capabilities offered by other solutions on the market.
- The breadth of our solutions and the flexibility of our offerings enable you to handle today's threat scenarios and prepare for tomorrow's possibilities.
- You can choose from the deployment model that best suits your needs. No other identity security vendor provides more choices.

Ready for the Next Step?

Contact our team of experts to learn more about BeyondTrust identity security solutions. Get started today with an identity security snapshot of your organization with a free identity security risk assessment today.

Contact our team of experts today.

The BeyondTrust Pathfinder Platform



Identity Security Insights
Gain a centralized view of identities, accounts, entitlements, and privileged access across your IT estate. Detect threats resulting from compromised identities and privileged access misuse.

Entitle
Secure your IaaS, PaaS, and SaaS environments with least privilege by providing granular, just-in-time access when needed. Automate identity management in the cloud to simplify access requests and reach zero standing privileges.

Endpoint Privilege Management
Remove local admin rights, enforce least privilege, prevent malware and phishing attacks, and control applications without compromising productivity.

Password Safe
Manage privileged passwords, accounts, keys, secrets, and sessions for people and machines. Secure non-privileged employee passwords for business applications.

Privileged Remote Access

Extend privileged access security best practices beyond the perimeter by granularly controlling, managing, and auditing remote privileged access for employees, vendors, developers, and cloud ops engineers. Privileged Remote Access has achieved Federal Risk and Authorization Management Program (FedRAMP®) authorization to operate (ATO) at the moderate impact level.

Remote Support

Supercharge your service desk with secure access and support for any devices, across any system, from anywhere – including Windows, macOS, Linux, Android, and iOS. Remote Support has achieved Federal Risk and Authorization Management Program (FedRAMP®) authorization to operate (ATO) at the moderate impact level.

Active Directory Bridge

Achieve streamlined identity management and access control across your hybrid environment by extending Microsoft AD authentication, SSO capabilities, and Group Policy configuration management to Unix and Linux systems.

>>> About BeyondTrust

BeyondTrust is the global identity security leader protecting Paths to Privilege™. Our identity-centric approach goes beyond securing privileges and access, empowering organizations with the most effective solution to manage the entire identity attack surface and neutralize threats, whether from external attacks or insiders.

BeyondTrust is leading the charge in transforming identity security to prevent breaches and limit the blast radius of attacks, while creating a superior customer experience and operational efficiencies. We are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at **www.beyondtrust.com.**