BeyondTrust

Ensure Remote Access Software Integrity & Enable Zero Trust with BeyondTrust.

Addressing CISA, NSA, & FBI Guidance for "Securing Remote Access Software" with BeyondTrust

Introduction

Remote access use cases have exploded, and so has the deployment of remote access software. However, much of this remote access technology, even if not deployed urgently, was not deployed with security at top-of-mind. Other times, the software is stretched for inappropriate use cases (such as VPNs used with BYOD or for vendor access).

And of course, just like any other software, remote access software could be misused or co-opted by threat actors. This is something that federal agencies, such as CISA, NSA, and FBI in particular have warned about and provided recent guidance.

For instance, illegitimate remote support software is sometimes planted on a target endpoint by a threat actor and then leveraged as a foothold to expand attacks across the network, or even on the victim's customers, in the case of supply chain-style attacks. Other typical attacks simply exploit weak security controls around existing remote access software, such as by stealing credentials, or misusing the excess access or privileges of the software.

With this remote access threat top-of-mind, the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing & Analysis Center (MS-ISAC), and Israel National Cyber Directorate (INCD), with contributions from private sector partners, published a joint **Guide to Securing Remote Access Software.**

In the joint guide, the authoring organizations state, "Many of the beneficial features of remote access software make it an easy and powerful tool for malicious actors to leverage, thereby rendering these businesses vulnerable."

The joint Guide to Securing Remote Access Software covers why remote access software is a target of threat actors, tactics used by those attackers, and the cyber defense and hygiene recommendations government agencies and other organizations should undertake to ensure they reap the benefits of remote access software, while minimizing the risk of the software's compromise or rogue deployment on their systems.

About This Paper

This brief explores how BeyondTrust solutions help organizations meet the CISA, NSA, FBI, MS-ISAC, and INCD objectives for secure remote access software.

This paper provides an overview of how:

- Native security capabilities in **BeyondTrust Privileged Remote Access** and **Remote Support** help make them resistant to misuse by insiders or compromise by attackers

- BeyondTrust's broader Identity Security and Privileged Access Management capabilities not only help protect the integrity of critical software, such as for remote support and remote access, but also minimize the risk of any rogue software (remote access, etc.) being implemented and allowed to execute.

BeyondTrust Solutions are Built with Security from the Ground Up

BeyondTrust is the leader in Secure Remote Access and Privileged Access Management. BeyondTrust Remote Support and Privileged Remote Access are the only solutions in their respective classes to meet the rigorous requirements of Federal Information Processing Standards (FIPS) 140-2 Level 1 validation.

BeyondTrust has also achieved **Federal Risk and Authorization Management Program (FedRAMP®)** authorization to operate (ATO) at the moderate impact level for its Secure Remote Access (SRA) solutions, which includes Remote Support and Privileged Remote Access.

These BeyondTrust solutions will now be officially listed on the FedRAMP Marketplace, the central online portal of approved cloud service offerings available for federal government use.

Remote Support and Privileged Remote Access can uniquely address the increasing cybersecurity demands of the public sector and other highly regulated industries like healthcare, finance, legal, etc. These products also enable a zero trust architecture (ZTA).

We understand the significance of using the right tool for the right job. That's why we offer specific products tailored to your requirements:

- BeyondTrust **Privileged Remote Access** enables agencies, contractors, managed service providers (MSPs), and other network administrators to provision privileged access.
- BeyondTrust **Remote Support** enables administrators and IT help desks to remotely access, service, and repair endpoints.

Both products are mature, comprehensive offerings that provide best-in-class security capabilities.

Let's now look at six areas where BeyondTrust Privileged Remote Access and Remote Support products are built to withstand attacks and protect against compromise, while securing access and enabling workers.

1. Robust Security Architecture

With BeyondTrust, each customer gets a segmented, single-tenant environment. Your data is never co-mingled with data from any other customer.

BeyondTrust remote access software itself is uniquely built for each customer, and each organization has its own unique URL and customer client.

Moreover, BeyondTrust remote access works through firewalls without VPN tunneling, so your perimeter security can remain intact. Outbound-only session traffic uses TCP Port 443. BeyondTrust's infrastructure has minimal port exposure, which drastically reduces the potential exposed attack surface.

Additionally, BeyondTrust Remote Support and Privileged Remote Access are the only solutions in their respective classes that meet the rigorous requirements of Federal Information Processing Standards (FIPS) 140-2 Level 1 validation.

The Federal Information Processing Standards Publication (FIPS) 140-2 Level 1 validation is a requirement for cryptographic products and software used in a U.S. government agency network and other industries to establish encryption standards that protect sensitive data. As a result, programs such as FedRAMP, FISMA, DoDIN APL, Common Criteria, HIPAA and HITECH healthcare regulations inherit the dependency on FIPS validation. BeyondTrust is proud to offer a purpose-built remote support and privileged remote access solution with FedRAMP certification.

2. Secure Authentication & Credential Management

In line with BeyondTrust's leadership in intelligent identity and access security, our Remote Support and Privileged Remote Access products both provide native capabilities around strong authentication and credential management that go beyond that of other solutions in their classes.

Most remote support solutions require you to create support rep accounts manually or via complicated processes. BeyondTrust's Remote Support and Privileged Remote Access products integrate seamlessly with external user directories, such as LDAP, for simple and secure user management. You can also enforce the networks and devices on which your support technicians can use BeyondTrust Remote Support.

In the case of the Colonial Pipeline breach, the Darkside cybercriminal group found stolen credentials that provided access on a dormant Colonial Pipeline VPN account that was still connected to the network. It's likely the credentials found by Darkside were re-used across multiple systems. BeyondTrust enables strong password security and management controls to prevent password re-use attacks and other threats caused by poor credential hygiene.

BeyondTrust's secure remote access products also provide native two-factor authentication (2FA). Implementing 2FA increases the security of remote access and the integrity of the remote access software by requiring a second factor (one time passcode) to login, in addition to the password. If you are already using a 2FA solution, you can use it with BeyondTrust, too.

Credentials are the gateway to critical resources, making their secure handling paramount in remote access scenarios. Privileged Remote Access and Remote Support each have a built-in password vault, enabling the storing, rotation, and tracking for privileged credentials by end users, such as IT service desks, vendors, or remote employees.

Credentials can be injected directly into remote sessions, ensuring they are never revealed to end users and establishing a further layer of obfuscation and security.

In addition, within environments where security implementations require smart card use for authentication, Privileged Remote Access and Remote Support enable the representative to share a local smart card within a support session so that it can be used as an authentication source on the customer system.

3. Enforce Least Privilege

With many remote access protocols (VPN, etc.) and third-party solutions, it is impossible to enforce the best practice of least privilege. As an analyst recognized Privileged Access Management (PAM) leader, BeyondTrust has pioneered an approach of extending PAM best practices, including zero trust least privilege, beyond the perimeter to remote access.

Privileged Remote Access and Remote Support provide the ability to provision access with granularity to ensure the right levels of access are granted to those who need it, enforcing the concept of "least privilege" in your service desk. Set access policies for users, groups, or sessions.

Session permission policies enable building a security model for each specific support scenario. In addition, group policies integrate easily with external directory stores to assign permissions based on your existing structures. You can also restrict logins to certain times of day and enable a just-in-time access model.

As an example, with BeyondTrust Remote Support, you can enforce granular permissions over which features a service desk representative has access to. You can even require end-user prompting so that the user receiving support must approve representative actions.

Moreover, Privileged Remote Access can enable further zero trust controls, such as helping implement segmentation and microsegmentation.

4. Session Management and Monitoring

Another analyst-recognized strength of Privileged Remote Access and Remote Support are their robust session management and monitoring capabilities.

These capabilities ensure all remote access activities are tracked and controlled. Session auditing and management capabilities enable you to identify and shut down any sessions that show signs of misuse or compromise.

With a centralized console, administrators gain complete visibility into active sessions, user actions, and system events.

Both products offer real-time session monitoring and screen recording, enabling security teams to quickly pinpoint suspicious behavior or potential security incidents. Suspicious sessions can be immediately terminated or paused for further review, helping you protect against potentially hijacked sessions and accounts.

The ability to review session recordings proves invaluable for post-incident investigations and compliance purposes. This comprehensive session management approach aligns with CISA's emphasis on robust auditing, enabling organizations to meet stringent security requirements and demonstrate adherence to best practices.

In addition to compliance benefits, many organizations further enable security best practices by utilizing recorded sessions as training for other admins. This practice ensures training for teams is standardized, and that administrators are well-equipped for all scenarios with well-documented sessions that are automatically recorded and stored.

5. Consolidated Access Pathways

Managing many different remote access solutions is not only cumbersome, but may also introduce security gaps. This sprawl of products also makes it more difficult to identify rogue and shadow IT remote access implementations.

BeyondTrust Privileged Remote Access and Remote Support each streamline access pathways by providing a single, unified platform for managing remote connections. Regardless of the target operating system—Windows, Linux, macOS, Chrome OS, iOS, or others—administrators can efficiently access and control remote systems seamlessly from a central, user-friendly BeyondTrust product console. This cross-platform support allows organizations to accommodate diverse user preferences and maintain productivity across diverse devices and environments, while offering a more comprehensive solution.

Moreover, BeyondTrust Privileged Remote Access and Remote Support are designed to handle large-scale remote access scenarios, making them suitable for organizations of all sizes. Both products provide robust performance capabilities that ensure remote sessions are smooth and responsive. Yet the architectures of these products are lightweight enough to perform in bandwidth-constrained environments.

Because BeyondTrust Remote Support and Privileged Remote Access products are so comprehensive in use case coverage, most BeyondTrust customers find they can standardize remote access with BeyondTrust, and thus, consolidate tools. This comes in addition to being the most secure products in their classes.

This consolidated approach simplifies administration, reduces the complexity of remote access infrastructure, and ensures a consistent and secure experience for network administrators and remote users alike. Being able to standardize remote access across a handful of solutions versus many makes it substantially easier for your agency to blocklist other remote access tools across the organization. This further minimizes the risk of rogue software deployment on an endpoint.BeyondTrust Privileged Remote Access is optimized to support OT environments, allowing administrators to securely manage and monitor critical systems.

6. Operational Technology (OT) Support

BeyondTrust is also recognized as a leading solution provider for securing OT systems. Operational Technology (OT) systems, used in critical infrastructures such as manufacturing, utilities, and transportation, and an increasing number of other environments, also require robust remote access security controls.

BeyondTrust Privileged Remote Access is optimized to support OT environments, allowing administrators to securely manage and monitor critical systems.

This capability is particularly crucial for industries where operational uptime and reliability are paramount to business continuity.

With Privileged Remote Access, network administrators can securely manage OT systems remotely, reducing downtime and minimizing the need for onsite visits, ultimately leading to cost savings, and increased operational efficiency.

Keyways that Privileged Remote Access secures OT environments, while protecting against co-option or compromise, includes:

- Enforcing the principle of least privilege for remote access sessions
- Treating managed devices with the same level of trust as an unmanaged device – which is zero
- Providing application access independent of network access
- Recording all activities performed using remote access and disabling functionality such as copy/paste
- Enabling API security to protect the integrity of data being sent from IoT devices to back-end systems
- Enforcing 2FA
- Encrypting all communications between the user and the remote systems using TLS 1.3

Protect Against Shadow IT and Misuse of Software with the BeyondTrust Identity Security Platform

Privileged Remote Access and Remote Support stand above other remote access solutions in their classes, not only by providing superior control and security around remote access, but also in the security of their own architecture and native controls that help them resist being co-opted or misused.

As a leader in Intelligent Identity and Access Security, BeyondTrust provides many additional security controls to protect the integrity of remote access software, as well as other critical systems, applications, and endpoints. BeyondTrust's Privileged Access Management (PAM) and Identity Security products also provide powerful controls at detecting and preventing the deployment of rogue remote access software and other tools, as we will briefly cover in this section.

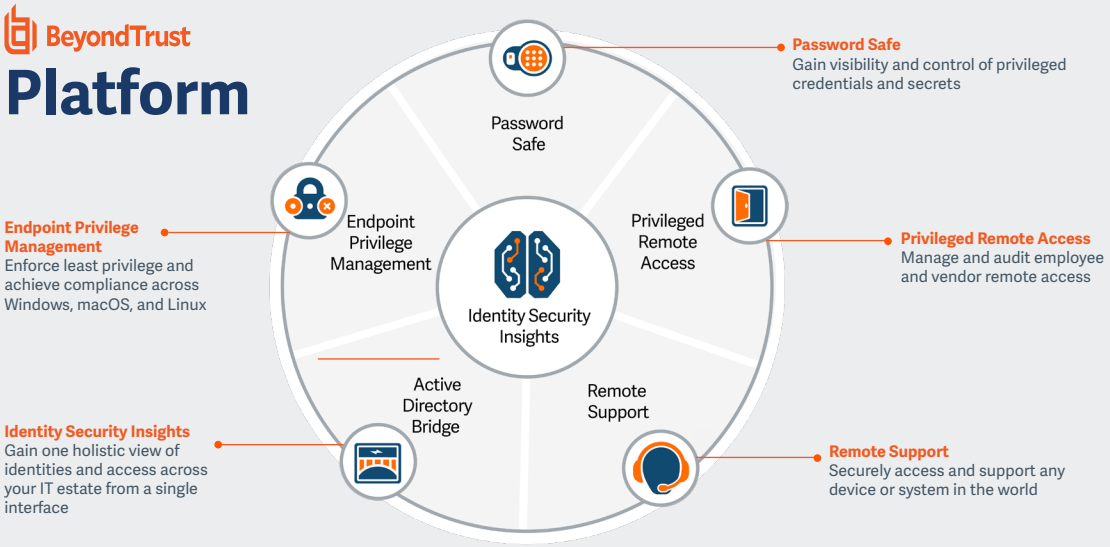
Discover Remote Access Software & Identity-Based Threats for Free

First, BeyondTrust offers a free tool, the **Privileged Access Discovery Application**, which many organizations use to find unwanted remote access software across their environment. Sometimes, this unwanted software is shadow IT that was provisioned by end users to get their work done, but in other instances, it's possible such software was deployed by a threat actor. In addition, the tool also shines a light on privileged credential and identity-based risks. You can learn more about this free application, and start using it at any time, by visiting here: **https://www.beyondtrust.com/tools/discovery**

Beyond that, BeyondTrust PAM and Identity Security products provide blended protection against threats and help implement zero trust security controls to protect infrastructure and critical applications, while also preventing the deployment and use of rogue software (i.e., remote access).

Here are some core BeyondTrust security controls that align with guidance from the joint agencyguide on protecting against co-option or rogue use of remote access software:

- **Condenses the attack surface and protect against unwanted lateral movement** by enforcing least privilege across all endpoints and users—human, machine, employee, and vendor
- **Protects against identity and account hijacking** by securing privileged credentials, keys, secrets, and workforce passwords
- **Prevents unwanted / rogue remote access installations and sessions** by blocklisting applications
- **Defends against tricky fileless threats that may seek to misuse legitimate software and tooling**, with powerful, context-based protection (such as by controlling DLLs and child processes—even those created out of hierarchy)
- **Protects against privilege creep that may provide footholds for attackers** by visualizing and right-sizing entitlements and permissions across clouds
- **Illuminates attack pathways you would otherwise miss and enables you to act proactively to reduce risk, or detect in-progress attacks and shut them down fast**, by unlocking powerful identity threat detection and response (ITDR) capabilities.



Mapping BeyondTrust to Federal Agency Secure Remote Access Recommendations

In this section, we provide a high-level mapping of BeyondTrust solutions to specific recommendations in the joint Guide to Securing Remote Access Software published by CISA, NSA, FBI, MS-ISAC, and INCD.

Architecture, Accounts, & Policy Recommendations	BeyondTrust's Approach to Address the Recommendations
Maintain a robust risk management strategy based on common standards, such as the National Institute of Standards and Technology Cybersecurity Framework	BeyondTrust's approach to robust risk management is rooted in aligning with the NIST SP 800-53 requirements, focusing on privileged access management (PAM) and identity security, to ensure controlled policy implementation and adherence to least privilege principles. Key strategies include: • **Controlled Policy Implementation:** Employing multiple methods to manage policies through their lifecycle, including change control and deployment, ensuring controlled and authorized access modifications. • **Role-Based Access Control (RBAC):** Utilizing RBAC policies to restrict access to authorized users, enhancing control over privilege assignments based on organizational roles and responsibilities. • **Least Privilege Principle:** Designing PAM solutions around this principle to manage user access privileges, application launches, and associated rights, thereby enforcing least privilege across network-connected assets. • **Auditing and Monitoring:** Implementing monitoring capabilities to audit privileged actions, assess login attempts, and control sessions based on defined security attributes, ensuring a thorough review and analysis of access activities for security assurance. • **Cross-Platform Policy Application:** Extending policies across diverse operating systems and network infrastructures, enforcing consistent security controls, and minimizing the risk of privilege abuse. • **Integration with Third-Party Solutions:** Integrating with external identity governance solutions to enhance authentication models and apply context-aware policies for refined access control. • **Remote and Wireless Access Control:** Incorporating policies to monitor, limit, and restrict remote and wireless access, including hardening end-user wireless activity to prevent unauthorized access. Through these strategies, BeyondTrust demonstrates a structured approach towards managing cybersecurity risks, adhering to common standards such as the NIST Framework to foster a secure and controlled operational environment. Learn more in our guide: **Addressing NIST SP800-53 Requirements with BeyondTrust Solutions**

When possible, employ zero trust solutions— or least-privilege-use configurations— which can be endpoint or identity-based	BeyondTrust Privileged Remote Access and Remote Support solutions take a least-privilege approach to remote access privileges. This ensures that users of remote access tooling can only perform activities specified in the security policies. To control the privilege of identities on the endpoint, BeyondTrust Privilege Managment for Windows & Mac elevates privileges to known, trusted applications that require them, controls application usage, and logs and reports on privileged activities using security tools already in place. In addition, BeyondTrust Privilege Management for Unix & Linux can eliminate use of root, enforce least privilege and granular control over commands, and layer on monitoring.
Work with a security operations center (SOC) team that can assist with monitoring systems	All BeyondTrust products integrate with SIEM tooling, and also have rich API's to collect data. Privileged Remote Access and Remote Support products also provide a comprehensive audit trail of all activity, which enriches connection data to show exactly what happened and by who. This also includes full video recordings of all sessions.
Audit Active Directory for inactive and obsolete accounts or misconfigurations	Often, administrator accounts are missed from joiners-movers-leavers (JML) processes. This is common in enterprise service desk environments. BeyondTrust Privileged Remote Access and Remote Support use a policy template that can connect to AD and leverage groups. These BeyondTrust products allow you to securely store and use credentials using their built-in vault — eliminating the need to share privileged identities manually and reducing the amount of operational complexity.
Enable just-in-time access and/or two-factor authentication based on the level of risks	BeyondTrust PAM products can all enable a just-in-time access model to implement true least privilege (eliminating persistent, always-on privileges) and minimize the attack surface and threat windows. Privileged Remote Access integrates with Active Directory, Microsoft Entra ID (formerly called AzureAD), and other Identity Providers (IdP) using SAML2. It also has built-in MFA capabilities. This means you can easily manage identities from your existing IdP, and integrate with existing MFA processes — or use the built-in capabilities at no extra cost. Within both Remote Support and Privileged Remote Access, you can define scheduling for external vendors.
Use safeguards for mass scripting and a script approval process. For example, if an account attempts to push commands to 10 or more devices within an hour, retrigger security protocols, such as multifactor authentication (MFA), to ensure the source is legitimate	Across the BeyondTrust portfolio of solutions, administrators can add a library of scripts and give technicians access to use them during remote desktop support sessions. You can use the security policies to determine who has access to the scripts. This also makes it easy to report on; if scripts are being used outside of these controlled/governed scripts, then you can investigate a threat faster. This is simple for a techician to use, only requiring the appropriate script to be selected from a list and run through the command line interface.

Recommendations for Host-Based Controls	BeyondTrust Controls
Audit remote access software and their configurations on devices on your network to identify currently used and/or authorized RMM software [CPG 1 .A]	BeyondTrust Privileged Remote Access allows you to centralize the configuration of the remote access software, ensuring all systems remain in a compliant state
Use security software to detect instances of RMM software only being loaded in memory	Each BeyondTrust remote access or remote support deployment is unique. This makes it far faster to spot rogue and/or anomalous remote access tools, and prevents the tool from being abused by threat actors. All software must come from your deployment in order to work successfully.
Review logs with complete data, including executing binary, request types, IP addresses, and date/time for execution of remote access software, all to detect abnormal use of programs running as a portable executable	Records in BeyondTrust are centrally accessed, identify unique users, and display which systems were connected, delineating the specific actions taken over the remote connection. Detailed reports and video recordings provide historical insight into remote access activity. Sessions can be monitored in real time.
Implement application controls, including zero-trust principles and segmentation, to manage and control execution of software, including allowlisting RMM programs and limiting actions the software can take [CPG 2 .Q]	BeyondTrust provides the leading capabilities for endpoint privilege management, applying application control, and least privilege across your entire endpoint estate. In addition, each BeyondTrust Remote Support and Privileged Remote Access deployment is unique, so this makes it far faster to allow list just your approved remote access tool, and prevents the tool from being abused by threat actors. All software must come from your deployment in order to work successfully. This can be done at a software package-level as you control the deployment, or at a network-level; the software uses a unique single tenant appliance with a unique hostname to connect.
Establish a regular frequency for patching, prioritizing software and systems that directly access or are accessed from the Internet, including remote access, management servers, and agents	BeyondTrust solutions periodically check for critical updates and emails admin contacts when updates are available. These updates can either be automatically deployed or installed manually.

Recommendations for Network-Based Controls	BeyondTrust Controls
Implement network segmentation to minimize lateral movement and restrict access to devices, data, and applications [CPG 2 .F]	BeyondTrust PAM products, including Privileged Remote Access, can enable agencies to implement segmentation and microsegmentation. Each BeyondTrust Remote Support and Privileged Remote Access deployment is unique, making it far faster to allow list your approved remote access tool and prevent the tool from being abused by threat actors. All software must come from your deployment in order to work successfully. This can be done at a software package-level, as you control the deployment, or at a network-level because the software uses a unique single tenant appliance, with a unique hostname to connect. All connections to the OT network are denied, by IP address and port, for specific system functionality. All communications paths between the IT and OT networks must pass through a bastion host or jump box, which is closely monitored, captures network logs, and saves video recordings.

Block both inbound and outbound connections on common RMM ports and protocols at the network perimeter and enforce only legitimate use of the tools employing those ports. Remote access software should have local instances in the environment and avoid operating over HTTPS port 443	This may be a challenge for some organizations, particularly if you want to support remote users. Enforcing the legitimate use of BeyondTrust is fairly straightforward due to the unique, single-tenant architecture. All traffic does operate over HTTPS, however it is all outbound from the device you wish to connect to — there are no listening ports or services on the endpoint!
Require authorized RMM solutions only be used from within your network over approved remote access solutions, such as VPNs or virtual desktop interfaces (VDIs) [CPG 2 .F].	While BeyondTrust remote access products will work over any connection, pragmatically this is difficult for organizations that support customers (as you're connecting to a customer device, not your own organization) and BYOD situations.

Recommendations for MSP and SaaS Customers	How BeyondTrust Addresses the Recommendations for MSP and SaaS Customers
Enable effective monitoring and logging of their systems. If customers choose to engage an MSP or SaaS provider to perform monitoring and logging, they should ensure that their contractual arrangements require their providers to [CPGs 1 .I, 1 .G, 1 .H]: Implement comprehensive security event management that enables appropriate monitoring and logging of provider-managed customer systems Provide visibility — as specified in the contractual arrangement — to customers of logging activities, including provider's presence, activities, and connections to the customer networks Note: Customers should ensure that MSP accounts are properly monitored and audited	Records in BeyondTrust are centrally accessed, and will identify unique users, show which systems were connected, and delineate what actions were taken over the remote connection. Detailed reports and even video recordings, give you historical insight into remote access and privileged user activity. Plus, you can monitor sessions in real time. This information can be shared both with the customer, and also the service desk — even integrated automatically into ITSM workflows in ITSM platforms, like ServiceNow.
Notify MSP of confirmed or suspected security events and incidents occurring on the provider's infrastructure and administrative networks and send these to a SOC for analysis and triage	All BeyondTrust records can be pulled into a SIEM using the API, or using the native SIEM integrations for analysis and triage.
Keep direct access to log servers — and the ability to delete or alter logs — out of reach of RMM tools	Records in BeyondTrust are centrally accessed and will identify unique users, show which systems were connected, and delineate what actions were taken over the remote connection. These records cannot be deleted or removed by the administrators of the system, and are held for 90 days. Extended retention can be achieved using the integration client, or integrating into ITSM platforms such as ServiceNow.

Recommendations for MSPs and IT Administratiors	How BeyondTrust Addresses the Recommendations for MSPs and IT Administrators
Improving the security of vulnerable devices and hardening appliances to vendor best practices. For more information, see the joint Cybersecurity Information Sheet Selecting and Hardening Remote Access VPN Solutions	BeyondTrust is the only secure remote access provider that meets the rigorous requirements of Federal Information Processing Standards (FIPS) 140-2 Level 1 validation. Privileged Remote Access and Remote Support can uniquely address the increasing cybersecurity demands of the public sector and other highly-regulated industries like healthcare, finance, legal, etc. **Learn more**
Adopting of MFA across all customer services and products [CPG 2 .H]. Note: MSPs should also implement MFA on all accounts that have access to customer environments and should treat those accounts as privileged	BeyondTrust Privileged Remote Access and Remote Support integrate with Active Directory, Microsoft Entra ID/Azure AD, and other Identity Providers (IdP) using SAML2. They also have built-in MFA capabilities. This means you can easily manage identities from your existing IdP, and integrate with existing MFA processes; or, use the built-in capabilities at no extra cost.
Configuring "reduced privilege" RMM tools for common uses, like read-only monitoring	BeyondTrust Privileged Remote Access and Remote Support products allow you to centralize the configuration of the remote access software, ensuring all identities can follow the prinicple of least privilege. This will allow adminstrators to control which tools and features a technician will have access to.
Managing internal architecture risks and segregating internal networks	All connections that BeyondTrust' Privileged Remote Access facilitates are egress, not ingress. This makes the architecture very simple and secure. No listening ports and no inbound connections to your clients' networks.
While zero trust is the ultimate goal, segregating customer data sets (and services, where applicable) from each other — as well as from internal company networks — can limit the impact of a single vector of attack [CPG 2 .F]	Each deployment of BeyondTrust Privileged Remote Access and Remote Support is single-tenant, and the software will only connect to the appliance it has been deployed from. This means the clients cannot be misused and abused to connect to other customer deployments. All connections to the OT network are denied by IP address and port for specific system functionality. All communications paths between the IT and OT networks must pass through a bastion host or jump box, which is closely monitored, captures network logs, and saves video recordings. In addition, the rest of the BeyondTrust PAM platform can enable core zero trust principles, and segmentation/microsegmentation to prevent lateral movement.
Do not reuse admin credentials across multiple customers [CPG 2 .E, 2 .C].	A credential vault is integrated directly with BeyondTrust's Remote Support and Privileged Remote Access products, so your technicians don't have to use another tool or even exit BeyondTrust to retrieve passwords. The included privilege identity discovery and rotation capabilities means that you can also automatically onboard, rotate, and inject credentials. For even broader capabilities, Remote Support and Privileged Remote Access integrate with BeyondTrust Password Safe, the leading solution for managing all types of privileged credentials, passwords, DevOps secrets, keys, certificates, workforce passwords, and more.

Zero Trust Security & Remote Access with BeyondTrust

As remote work continues to reshape the modern workplace, delivering secure remote access to networks has become a critical agency priority.

By adopting BeyondTrust solutions, agencies, contractors, MSPs, IT help desks, network administrators, and security teams can enjoy the benefits of streamlined administration, optimized performance across various operating systems, and strengthened security posture.

This, in turn, enables organizations to confidently navigate the challenges of secure remote access, empowering their workforce with the flexibility to work from anywhere while ensuring the highest levels of data protection and compliance with regulatory requirements.

Contact us to learn more about how BeyondTrust can help you ensure secure, legitimate remote access, while also supporting zero trust security principles.

Recommended Reading

Advancing Zero Trust with Privileged Access Management (PAM) (guide): Bridge the principles of zero trust as scoped by NIST, into real-world privileged access management (PAM) and secure remote access product capabilities that can enable zero trust across the public or private enterprise

Access Management: Core to CISA's Zero Trust Maturity Model 2.0 (guide): Explore access management best practices, get analyses of the new zero trust access management maturity category, and discover the substantial impact Privileged Access Management capabilities can have for organizations on their journey towards a mature Zero Trust Architecture.

Buyer's Guide for Complete Privileged Access Management (PAM) (guide and checklist template): Learn the six steps of must-have PAM capabilities necessary to properly secure identities and access across your agency and advance along your PAM journey.

Remote Support Checklist and Buyer's Guide: Learn everything you need to consider when evaluating remote support solutions, and also get a checklist to compare vendors.