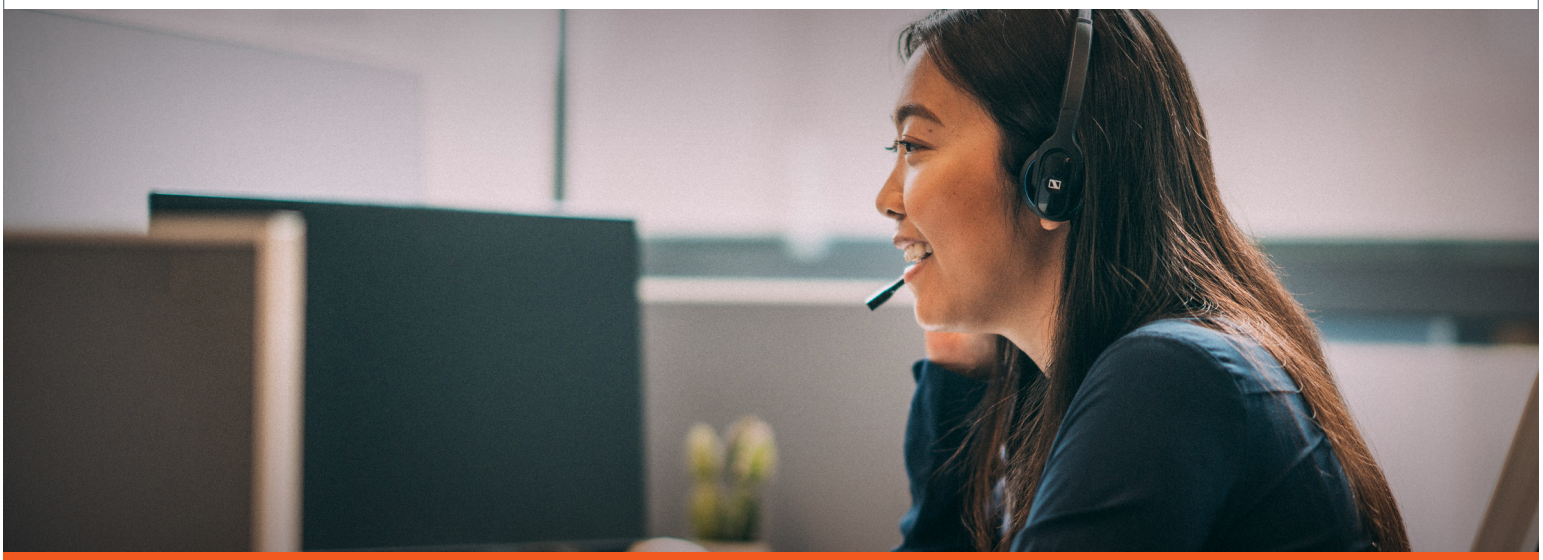
WHITE PAPER



REMOTE SUPPORT BUYER'S GUIDE

Key vendor and product criteria for selecting the right solution for your help desk

BeyondTrust

TABLE OF CONTENTS

1 Introduction

IT help desks face an increasingly complex support environment, requiring flexible remote support options that scale, adapt, and continue to meet rigorous security requirements. Whether you're a small IT business owner or part of a large enterprise organization's technical support team, choosing the right remote support software is pivotal to the productivity and security of your service desk.

Choosing the right remote support software is pivotal to the productivity and security of your service desk.

An audit of the remote support tools in your organization may reveal a mixture of remote access products that are being used for different support scenarios, including:

- Helping users inside and outside the traditional network perimeter
- Remotely accessing servers and workstations, and other unattended systems
- Maintaining network devices (switches, routers, etc.)
- Supporting a number of platforms, including Windows, Linux, and Mac systems
- Supporting a wide variety of mobile devices running iOS and Android
- Facilitating remote access for vendors and other third parties
- Fixing off-network devices, such as robots, machines, and any other devices not connected to the Internet

For Remote Support, Less Truly is More

Many service desks use multiple tools for remote support, but technicians can be hampered as they switch between tools for different tasks. Some tools only support a narrow set of systems or platforms and lack advanced integration features. In these instances, your support tool ecosystem can actually stifle innovation and hold your organization back from upgrading to better systems or bringing on new enterprise technologies and applications for fear of integration challenges, increased administrative burden, or heightened cyber risk or compliance exposure.

Simply put, organizations need remote support solutions that can cover an expansive list of use cases, while making your entire service desk experience better.

2 Remote Support Defined

Remote support software allows one computer to remotely access and view the screen of another computer or device via an internet connection, specifically to provide support-based functions. These tools can be deployed as SaaS, licensed software, and physical and virtual appliances.

Remote support solutions should give IT support specialists the ability to remotely control systems from almost any computer or mobile device that can access the web, allowing them to support PC- and Mac-based desktops, mobile devices, and other network assets, such as servers and point-of-sale (POS) systems.

Remote support software allows one computer to remotely access and view the screen of another computer or device via an internet connection.

Remote support solutions may or may not require client software to be pre-installed on the machine receiving support in order to be accessed by the support technician. They also should not require virtual private networks (VPNs) or open ports to be utilized to make the connection.

Attended & Unattended Sessions

Remote support can be provided via either attended or unattended sessions. Attended sessions, the most typical method, are support sessions where assistance is provided live to a service customer (either internal or external). Unattended remote support sessions refer to sessions where the support technician connects to a device or system without requiring the presence of another human being on the supported device or system. Unattended sessions are a non-intrusive way for technicians to remotely assess the health status of endpoints (desktops, servers, mobile devices, etc.) applications, and systems, as well as perform updates and maintenance across one or many endpoints, applications, or systems.

3 Remote Access Security

Remote support tools are now on the radar of hackers and your CISO. Remote access tools and pathways are increasingly being exploited by cyberattacks as backdoors into end-user and customer environments, so organizations should take a security-conscious approach to the evaluation of any remote support/remote access solutions.

Traditional remote connectivity methods can be easily exploited via stolen credentials and session hijacking.

Traditional remote connectivity methods, such as VPNs, or free remote access tools, lack granular access management controls and can be easily exploited via stolen credentials and session hijacking. They typically lack granular permission setting options, firewall settings are weakened, and there is no ability to log or record remote support sessions.

Attackers have also been effective at using legitimate remote support tools on service desk machines. For instances, attackers have exploited remote support and other remote access tools on the employee devices of a number of IT services providers (including MSPs and MSSPs) and used the tools as backdoors to launch third-party attacks on the services providers' customers. Standardizing to one, highly secure remote support solution across the enterprise will make it easier to blanket blacklist other such tools, reducing the likelihood of rogue remote access software and shadow IT.

Is Your Help Desk Vulnerable?

Security experts often refer to help desks as a company's biggest security vulnerability because help desk technicians are often inadequately trained to identify social engineering attacks. They are simply doing what they've been trained to do — help resolve user issues. Help desk agents are frequent targets for phishing campaigns. With help desks commonly failing to monitor their technicians (track call logs, keep record of authentication changes, etc.) it's a good bet that hackers will continue to be opportunistic with their help desk phishing exploits.

You must closely consider how remote support tools will impact the security, flexibility, reliability, and the reputation of your organization.

4

What Is Your Ideal Remote Support Solution?

There are many different remote support use cases, but no matter who or what you are supporting, remote support technology users want a solution that is easy to use, reliable, and secure.

The right remote support solution enables users to quickly access and fix nearly any remote device, running on any platform, located anywhere in the world. It should also provide absolute visibility and control over internal and external remote access, secure connectivity to managed assets, and a complete, unimpeachable audit trail for compliance.

The right remote support solution enables users to quickly access and fix nearly any remote device, running on any platform, located anywhere in the world.

The Right Remote Support Solution Delivers Results

- Increase customer satisfaction and FCR (First Call Resolution)
- Reduce incident handling time
- Boost agent productivity job satisfaction
- Streamline processes and improve existing workflows
- Extract more value from your other service desk tools, such as ITSM and CRM
- Address security concerns and mitigate risk

This white paper provides in-depth information and serves as a guide to selecting the right remote support solution for your business.

5 How To Use This Guide

Remote Support buyers should be looking for a mature, feature-rich product. What exactly does that mean? This Buyer's Guide will focus on features and functionalities you should consider essential to enabling a modern service desk environment—whether your organization is a small business, a large enterprise, or an IT services provider.

This Buyer's Guide will focus on features and functionalities you should consider essential to enabling a modern service desk environment.

Throughout the process of assessing remote support solutions, keep in mind these business requirements:

- **Total Cost of Ownership**

  Does it result in time-savings (such as replacing manual processes with automation) and allow you to re-deploy resources for other initiatives?

- **Time-to-Value**

  How soon does it help you measurably improve service desk performance? How long will it take to achieve your end-state goals with the solution?

- **Integrations**

  How does it integrate with the rest of your ITSM ecosystem? If it only works well as a standalone or point solution and for a limited range of use cases, it probably isn't viable as a long-term solution. On the other hand, if the solution has synergies with your other service desk tools, it will help you maximize existing IT investments.

- **Longevity**

  Will the solution vendor grow with you or even propel you towards growth through service desk enablement? Is the vendor resourced to evolve capabilities and deepen feature-richness to meet emerging use cases of tomorrow? As your organization expands, your solution should expand with you!

Addressing the most critical requirements empowers your service desk.

6

The 6 Key Components of a Complete Remote Support Solution

First and foremost, your remote support solution should enable your service desk as a whole to be more powerful, more efficient, and more effective. This section covers the top capabilities across 6 categories to consider in a remote support solution.

1. BROAD PLATFORM SUPPORT

Modern remote support solutions should enable technicians to provide support regardless of either their platform or the end-user's platform. When support technicians are on the go, they should be able to seamlessly provide support via their mobile device. Sometimes support technicians need to quickly connect through a web browser, such as Chrome. In these instances, having an HTML 5-based console can be particularly beneficial.

Your remote support solution should enable your service desk as a whole to be more powerful, more efficient, and more effective.

The broader the platform support, the better you will be able to standardize support using a single tool to improve incident handling time, technician productivity, and reap other efficiencies.

Key Platforms to Support

- Windows
- Mac
- Linux
- Android
- iOS
- Chrome OS
- Other devices, kiosks, or machines, on or off a network

Questions to Ask the Vendor

- What platforms do you support?
- Is this all included in the core product, or do we have to pay extra, such as mobile support?
- Does this include supporting the end user platform only, or can I provide support from those platforms as well?

2. COLLABORATION

Features in this category are central to the customer support experience and help drive faster incident resolution.

Features like chat support, remote camera sharing, intelligent collaboration, and other features in this category are central to the customer support experience and help drive faster incident resolution.

Top Collaboration & Efficiency Capabilities

- **Streamlined Workflows**
  - Define escalation paths to skilled resources to enable intelligent collaboration and quickly transfer remote support sessions to the right resources
  - Provide canned scripts, which can be used to run patches or installers on remote desktops and servers
  - Allow secure access to the command line for network troubleshooting, system diagnostics, and/or network device support with recording of command line sessions for security and auditing.
  - Allow secure usage on remote networks, without requiring VPN tunneling or firewall changes.
  - Create and administer surveys to customers as well as to support technicians.
- **Multi Platform Support & Chat**
  - Enable support technicians to efficiently provide help from your website
  - Screen sharing of Android and MacOS mobile devices
  - Use remote camera sharing to support for anything your customer can see, including hardware and peripherals
  - Embed chat and other remote support tools in your app
  - Provides augmented reality capabilities that allows technicians to see exactly what the customer sees in real-time and annotate over it via live stream
- **Scale**
  - Enable support to manage unattended access to hundreds or thousands of systems
  - Create mass installer packages for both the Representative Console and unattended endpoints
- **Advanced Capabilities**
  - Enable troubleshooting beneath the operating system by leveraging Intel vPro technology to power a remote PC on/off, reboot to BIOS, re-image a remote computer, and access remote desktops - regardless of operating system state
  - Provide access to the remote registry editor on Windows PCs without interrupting the remote customer or requiring a screen sharing session.
  - Able to kill processes; start, stop, pause, resume, and restart services; and uninstall programs on remote PCs or mobile devices.

3. INTEGRATIONS

You've already invested in solutions for your service desk or support center to more efficiently track issues and end-user requests. Your remote support software should fit seamlessly into your environment and unlock synergies with the other solutions in your ecosystem.

Remote support solutions that come with out-of-the-box integrations for the leading ITSM, CRM, and systems management solutions reduce administrative burden.

Powerful remote support and ITSM integrations enable organizations to deliver services more efficiently, reduce demand on operations, and manage processes, workflows, and service experiences. For a seamless incident resolution and management process, your technicians should be able to launch a remote support session directly from the support ticket or change record, automatically update tickets with details from the support session, and include the chat transcript and session recording in the ticket. This requires integrating your remote support tools with your incident and case management systems.

The stronger the integrations of remote support with the rest of your service desk, the better the experience for both your service desk technicians and its customers.

The higher the interoperability and the stronger the integrations of remote support with the rest of your service desk, the better the experience for both your service desk technicians and its customers.

Top ITSM Integration Capabilities

- Pre-built integrations with ITSM, CRM, and systems management solution, such as ServiceNow, Cherwell Software, Remedy, SaleForce, etc
- Integrations with external directories, like LDAP, Active Directory, and RADIUS and SAML so you can manage users, groups, MFA authentication, and permissions using existing administrative processes, and support single sign on (SSO)
- Custom integration capabilities and robust APIs
- Ability to initiate a chat or remote support session directly from any ITSM tool
- One-click elevation from chat to a full remote support session
- Auto-population of incident records with remote support session details including post-session survey if completed
- Automatic routing of incoming remote support requests to the least busy technician

Questions to Ask the Vendor

- How often are the integrations updated?
- How easy is it to access and set up the integration?
- Does the application provide APIs for custom integrations?
- Are APIs available to help automate onboarding new users and assets? ow easy is it to access and set up the integration?
- What capabilities are supported? Ask for details!

4. SECURITY, AUDITING & COMPLIANCE

As remote work has increased, so too has the number of data breaches through point-to-point remote access tools like pcAnywhere, RDP, VNC, and free non-secure access tools. The limited use cases for these tools are frequently stretched beyond what is safe or efficient and their security features (or lack thereof) should be a red flag. Problems with these tools are manifold. The most pressing shortcomings are the dangerous lack of visibility into remote access sessions and the inability to apply the principle of least privilege for access.

Service desk technicians are often required to use admin credentials with elevated privileges to resolve support issues. Although privileged account credentials are a common target for hackers, credential management best practices are commonly sacrificed trying to quickly resolve issues. In fact, many service desk teams share and store credentials in plain text. It's imperative to provide technicians with the credentials and authentication they need quickly for expedited access to IT systems, while always enforcing credential management best practices.

Today's threat environment and regulations demand that enterprises be able to identify and record the who, what, where, and when around remote access activities. These are questions only the best enterprise-class remote support tools are purpose-built to answer. Yet, even amongst enterprise tools, there can be substantive differences in security maturity and capability completeness.

Enabling a robust, integrated password vault enables your organization to securely store, share, and track the use of privileged credentials by the IT service desk.

Whether you're subject to PCI, HIPAA, ISO, GDPR, NIST, CJIS, FFIEC, or other stringent regulations, the right solution should help you easily produce the detailed attestation reports to prove compliance. Security features that support those measures include advanced encryption, least privilege enforcement and granular control of access to sensitive data (such as PII), audit logs, and recordings of all sessions.

Top Security, Auditing, and Compliance Capabilities

The service desk can be a significantly vulnerability when it comes to security. Remote access tools and pathways are increasingly being exploited by cyberattacks as backdoors into end-user and customer environments. Any remote support tool under consideration should mitigate these risks.

- **Secure Architecture**
  - Enforces robust encryption, including the use of SSL for every session connection; ideally all data should be encrypted in transit using TLSv1.2, and you should be able to configure (enable, disable, reorder etc.) cipher suites as desired
  - Offers the ability to use SSL certificates
  - Able to work through firewalls - without VPN tunneling - so your perimeter security can remain intact
  - Uses outbound-only session traffic using TCP Port 443; by minimizing port exposure, you drastically reduce the potential exposed attack surface of your support site
  - Segments each remote support customer via single-tenant environments, so your data is never co-mingled with other customer data
- **Audit Trails & Reporting**
  - Logs every session, allowing for the complete auditing and review of all customer and support technician interactions, including permissions granted by the customer, chat transcripts, system information, and any other actions taken by the technician

- Retains full session logs in an un-editable format for up to 90 days
- Records session videos of the visible user interface of the endpoint screen for the entire screen sharing session including metadata to identify who is in control of the mouse and keyboard at any given time

- **Authentication & Permissions**
  - Ability to define and enforce different policies for attended and unattended remote support sessions
  - Secure authentication through seamless integration with external user directories, such as LDAP
  - Native two-factor authentication or via 2FA integration from an existing solution
  - Passing of local smart card or common access card (CAC) credentials to a remote computer
  - Integrated password vaults enable technicians to securely store, share, and track the use of privileged credentials by the IT service desk.

The Role of Credential Vaults

Remote access tools and pathways are increasingly being exploited by cyberattacks and any remote support tool under consideration should mitigate this risk.

The ideal password management solution should fit seamlessly with your service desk workflow while mitigating the threats in your service desk related to stolen credentials and passwords. Key features to seek include:

- Discovers and onboards all remote support credentials
- Masks plain-text passwords so they are never revealed to the end-user or customer
- Rotates credentials frequently
- Automatically injects credentials into the system, application, etc., where access is needed
- Checks out password from the secure vault when access is needed and authentication are met and returns password (checks in) to the vault when the session has expired
- Applies least privileges and granular permissions so that precisely the right levels of access are granted to those who need it

Questions to Ask the Vendor

- Is 2FA added as an extra cost?
- Do you support data-at-rest encryption?
- Is data encrypted at rest in their cloud offering?
- Is there a tamper-proof audit log?
- Has the solution received FIPS or other security certifications?
- Can I track privileged accounts commonly used in the service desk?
- Does the solution hide plain text passwords from users?
- Is there automatic or manual rotation of passwords after each use?
- Can I export session recordings? In what format?

5. BRANDING & CUSTOMIZATION

A branded and customized support experience fosters end-user trust.

Support customers can be wary about allowing a remote connection to their devices. One important way for support organizations to reinforce positive brand awareness and foster trust is by branding and customizing the support experience for their customers. Ideally, your remote support solution should allow you to create custom portals for each customer, group, and/or product your users support.

Top Branding and Customization Capabilities

- Provides ability to brand portal with your logo and other features
- Permits customization of support invitations
- Allows use of a custom watermark
- Offers multiple customization elements, including public sites, agreements and messages, customer client, exit surveys
- Enables the importing of technician photos from Active Directory to personalize the support experience

Questions to Ask the Vendor

- How can we drive support requests to the web?
- If I support multiple business customers, can I create a custom user experience for each customer business?
- Can I customize support agreements and messages?
- Can I customize the chat window?

6. FLEXIBLE DEPLOYMENT OPTIONS

Deployment and licensing options vary widely and should align to your needs.

Seek out a solution that offers the deployment and licensing options that best fit the needs and requirements of your organization. Common deployment options include cloud subscriptions as well as physical and virtual appliances. Some vendors may offer only a single option. Other vendors may offer several options. However, sometimes capabilities and features may vary or be lacking across different deployment scenarios from the same vendor, so verify that the deployment model you choose includes the features and capabilities that you expect.

Additionally, if you are with a federal agency or another organization with particularly stringent security and regulatory needs to meet, consider a solution that has met Federal Information Processing Standards Publications (FIPS) validation.

Deployment Options to Consider

- Physical or virtual appliances
- Hosted cloud / SaaS
- IaaS in your environment, including AWS, Azure, VMWare ESXi, Microsoft Hyper-V

Questions to Ask the Vendor

- How easy is it to set up?
- Does the solution require changes to my firewall?
- What virtual platforms are supported?
- Are there any feature/capability differences across the various deployment models you offer?
- Do you have a cloud-based offering? Is it single tenant?
- Can I move from one deployment method to another if my requirements change?

BENEFITS OF CONSOLIDATING TO ONE SUPPORT SOLUTION

Consolidating to one support tool saves time and money.

Buyers should be looking for a vendor that provides a comprehensive, integrated approach to secure remote support delivery.

By using one product, a support organization eliminates overlapping costs. Much of the time once spent installing, maintaining, troubleshooting, or managing multiple tools can now be used resolving incidents.

Benefits of Consolidation

- Direct cost-savings in the provisioning of IT support
- Savings in the productive time of employees
- Fewer on-site support visits
- Reduction of tool sprawl and security risk
- Simplified auditing and reporting

7 BeyondTrust Remote Support

BeyondTrust Remote Support is built to make your entire service desk work better. Our solution covers the broadest number of remote support use cases with the most robust remote access security available. In fact, BeyondTrust has the only Remote Support solution that meets the rigorous requirements of FIPS 140-2 Level 2. Connect anywhere (on the local network, over the Internet, etc.) to support any device, across any platform, while unlocking powerful synergies with key service desk integrations.

If you want to maximize other IT investments in your organization while increasing efficiency, BeyondTrust Remote Support is the best option for your business. Our Remote Support solution boasts the best renewal rate in the industry.

*The **#1 solution for leading enterprises** to securely access and support any device or system, anywhere in the world*

Schedule a demo or set up a free trial at beyondtrust.com/remote-support.

8

Appendix: Remote Support Checklist

Collaboration & Efficiency	BeyondTrust	Vendor A	Vendor B
Chat	✓		
Intelligent collaboration (defined escalation paths, request routing)	✓		
iPhone, iPad, and Android screen sharing	✓		
Canned scripts	✓		
Scalable remote support to access hundreds or thousands of systems	✓		
Remote camera sharing	✓		
Embedded chat and support for your apps	✓		
Command line sessions	✓		
Troubleshooting beneath the operating system by leveraging Intel vPro technology to access remote desktops—regardless of operating system state	✓		
Augemented reality	✓		
Remote registry editor	✓		
Post session surveys	✓		

Appendix: Remote Support Checklist

Supported Platforms	BeyondTrust	Vendor A	Vendor B
Windows	✓		
Mac	✓		
Linux	✓		
Android	✓		
iOS	✓		
Chrome OS	✓		
Access and control any remote computer or device, on or off the network	✓		

Appendix: Remote Support Checklist

ITSM Integration Features	BeyondTrust	Vendor A	Vendor B
Pre-built integration for your ITSM solution	✓		
Pre-built integration with external directories, like LDAP, Active Directory, and RADIUS and SAML and/or SSO	✓		
Custom integration capabilities and robust APIs	✓		
Chat or support sessions initiation right from the ITSM tool	✓		
One-click elevation from chat to full remote support session	✓		
Auto-populates incident records with remote support session details	✓		

Appendix: Remote Support Checklist

Security, Audit & Compliance	BeyondTrust	Vendor A	Vendor B
Works through firewalls—**without VPN tunneling**—so your perimeter security can remain intact	✓		
Outbound-only session traffic via TCP Port 443	✓		
Segments each remote support customer via single-tenant environments	✓		
Offers the ability to define and enforce different policies for attended and unattended remote support sessions	✓		
Applies robust and granular permissions to define how technicians, customers, and remote systems interact	✓		
Allows admins to pass local smart card or common access card (CAC) credentials to a remote computer	✓		
Securely authenticates users by seamlessly integrating with external user directories, such as LDAP	✓		
Either natively provides two-factor authentication or supports 2FA integration from an existing solution	✓		
Password vault to store, share, and track the use of privileged credentials, that includes more advanced features include discovery, rotation, and workflow automation	✓		
Applies least privilege and granular permissions so that precisely the right levels of access are granted to those who need it	✓		
Initiates end-user prompting, as desired, so that the user receiving support must approve certain actions	✓		

Appendix: Remote Support Checklist

Security, Audit & Compliance	BeyondTrust	Vendor A	Vendor B
Enforces robust encryption, including the use of SSL for every session connection	✓		
Logs every session, allowing for the complete auditing and review of all customer and support representative interactions. Session data logged should include representatives involved, permissions granted by the customer, chat transcripts, system information, and any other actions taken by the representative	✓		
Retention of full session logs in an un-editable format for up to 90 days	✓		
Session recording of the visible user interface of the endpoint screen for the entire screen sharing session. The recording should include metadata to identify who is in control of the mouse and keyboard at any given time	✓		
Ability to use SSL certificates	✓		

Appendix: Remote Support Checklist

Branding & Customization	BeyondTrust	Vendor A	Vendor B
Support site branding with your logo and other options	✓		
Customized support invitations	✓		
Use of a custom watermark	✓		
Customization of agreements and messages, customer client, exit surveys	✓		
Technician photo uploading - manually or from Active Directory	✓		

Appendix: Remote Support Checklist

Deployment Options	BeyondTrust	Vendor A	Vendor B
Physical appliance	✓		
Virtual appliance	✓		
Hosted cloud / SaaS	✓		
IaaS in your environment, including AWS, Azure, VMWare ESXi, Microsoft Hyper-V	✓		

ABOUT REMOTE SUPPORT

BeyondTrust Remote Support enables help desk teams to quickly and securely access and fix any remote device anywhere, on any platform, with a single solution. BeyondTrust enables the greatest number of remote support use cases with the most built-in security features, while unlocking powerful synergies with key service desk integrations. Gain absolute visibility and control over internal and external remote access, secure connectivity to managed assets, and create a complete, unimpeachable audit trail for compliance. Organizations of all sizes can boost service desk productivity, efficiency, and security by consolidating and standardizing help desk support with BeyondTrust.

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. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network. Learn more at

beyondtrust.com