BeyondTrust

Enable & Secure Your Remote Workforce

Keep Remote Workers Productive Without Sacrificing Security

INTRODUCTION

IT departments are under incredible pressure to maintain the business productivity for an expanded remote workforce that is exponentially larger than it was just a few weeks ago.

As many IT teams work overtime to enable remote workers, maintaining security practices and compliance may not be top of mind, but **threat actors are actively seeking opportunities** to benefit from current circumstances.

Although enabling a remote workforce is typically a common practice, some particularly **urgent and unique considerations** are being thrust upon organizations and their employees during the coronavirus crisis.

Attackers are largely opportunistic.
Hackers seek to exploit companies with large attack surfaces due to outdated security policies or reduced adherence to security best practices during this crisis.

It's not just the big guys being targeted.
Small to medium-sized businesses (SMBs) and state and local government organizations, such as schools, have been some of the hardest hit by malware outbreaks and ransomware attacks in recent years.

TABLE OF CONTENTS

THE COVID-19 IMPACT

What are the Most Pressing Challenges to Enabling a Secure Remote Workforce?

Many companies were forced to "go remote" in a very short window of time. Some have been able to provide employees with company-issued computers that are closely managed and locked down, but this is often not the case.

The following practices related to remote working create risk:

Practices Creating Risks

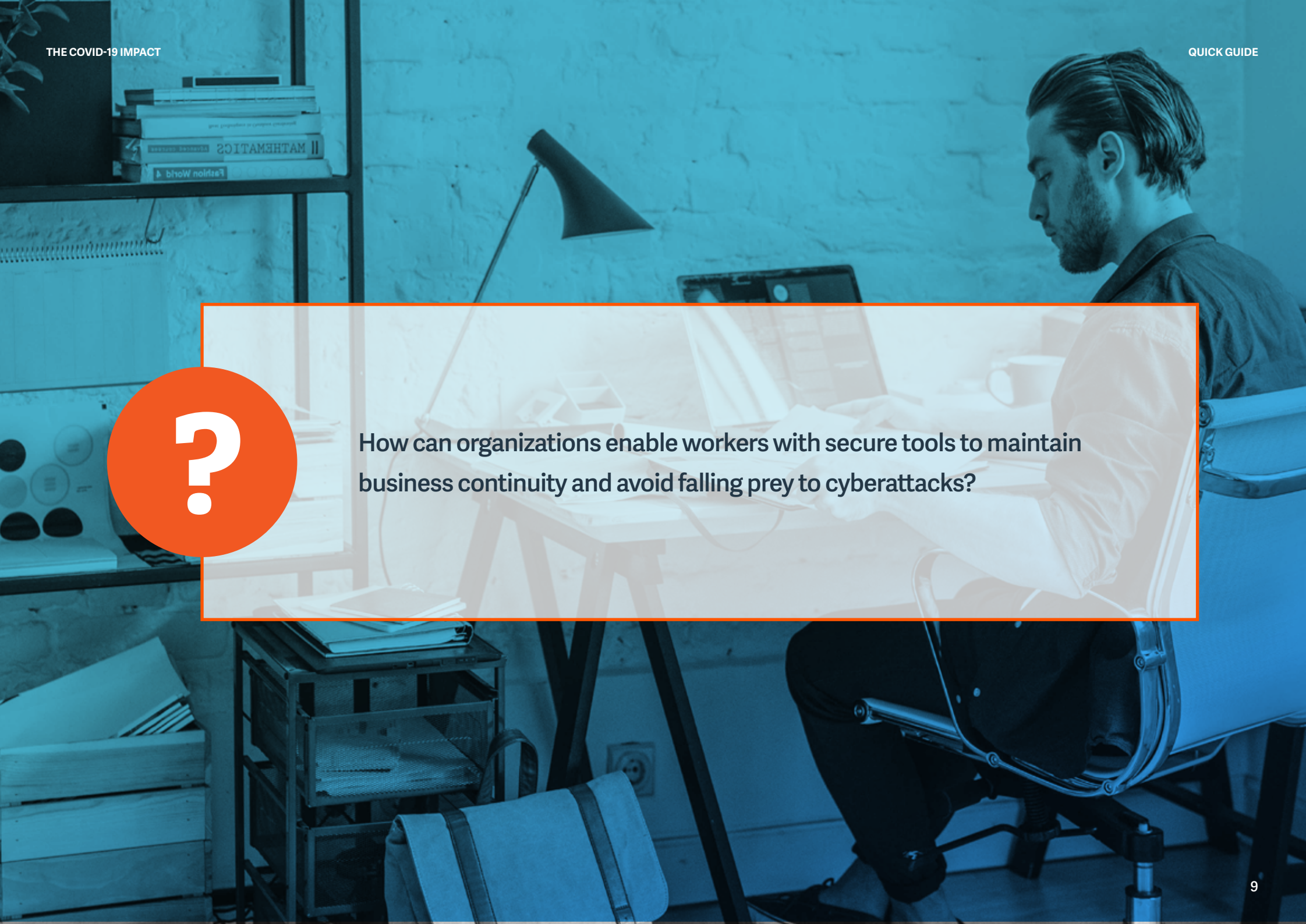
- Loosening up the BYOD (bring your own device) policy
- Conducting personal business on corporate-issued laptops, such as home schooling
- Using insecure or outdated remote access tools to connect to the network
- Utilizing "always-on VPNs" for all user connections, even when some users only need access to cloud-based applications and data
- Opening of phishing emails, which are on the rise due to the pandemic
- Downloading potentially malicious software, introducing malware into your corporate environment from home

Gartner recently conducted a study, "Solving the Challenges of Modern Remote Access,"* to offer guidance to security and risk leaders around the challenges of quickly scaling large-scale modern remote access. It concludes that **most organizations only have capacity and licenses to handle a small subset of users and are not prepared to enable all employees for remote work** during critical, longer-term events such as COVID-19. Furthermore, organizations frequently lack the required bandwidth needed to support all users working remotely simultaneously.

Gartner, "Solving the Challenges of Modern Remote Access," Rob Smith, Steve Riley, Nathan Hill, Jeremy D'Hoinne, March 25, 2020

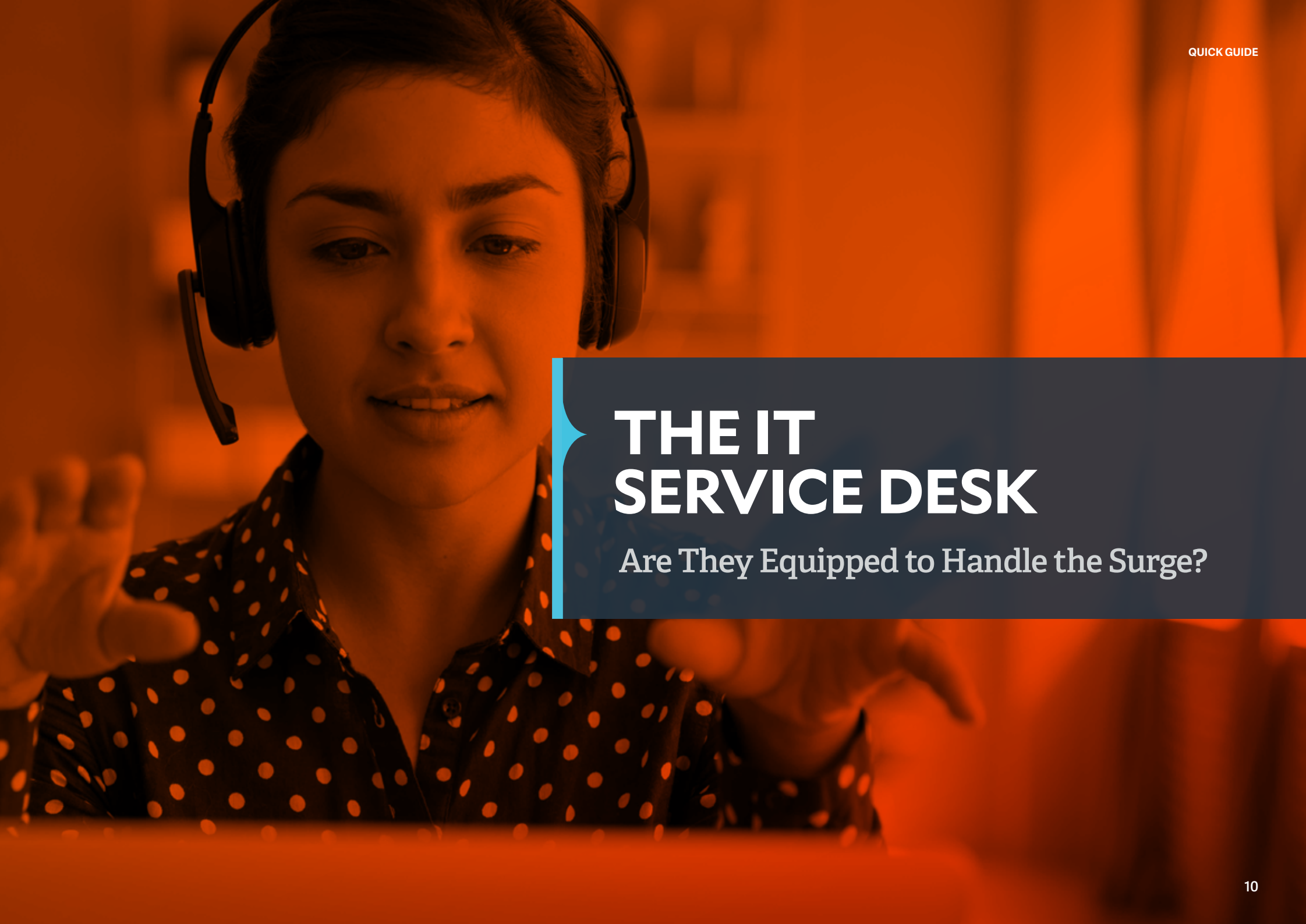
Poor cybersecurity hygiene practices, which may be better managed by employees during a more normalized business setting, can put your organization at risk, including:

- Using insecure wireless internet connections
- Reusing or sharing passwords
- Device sharing
- Opening emails that contain ransomware
- Storing passwords in unsecured locations or on sticky notes
- Downloading software that could contain malware



?

How can organizations enable workers with secure tools to maintain business continuity and avoid falling prey to cyberattacks?



THE IT SERVICE DESK

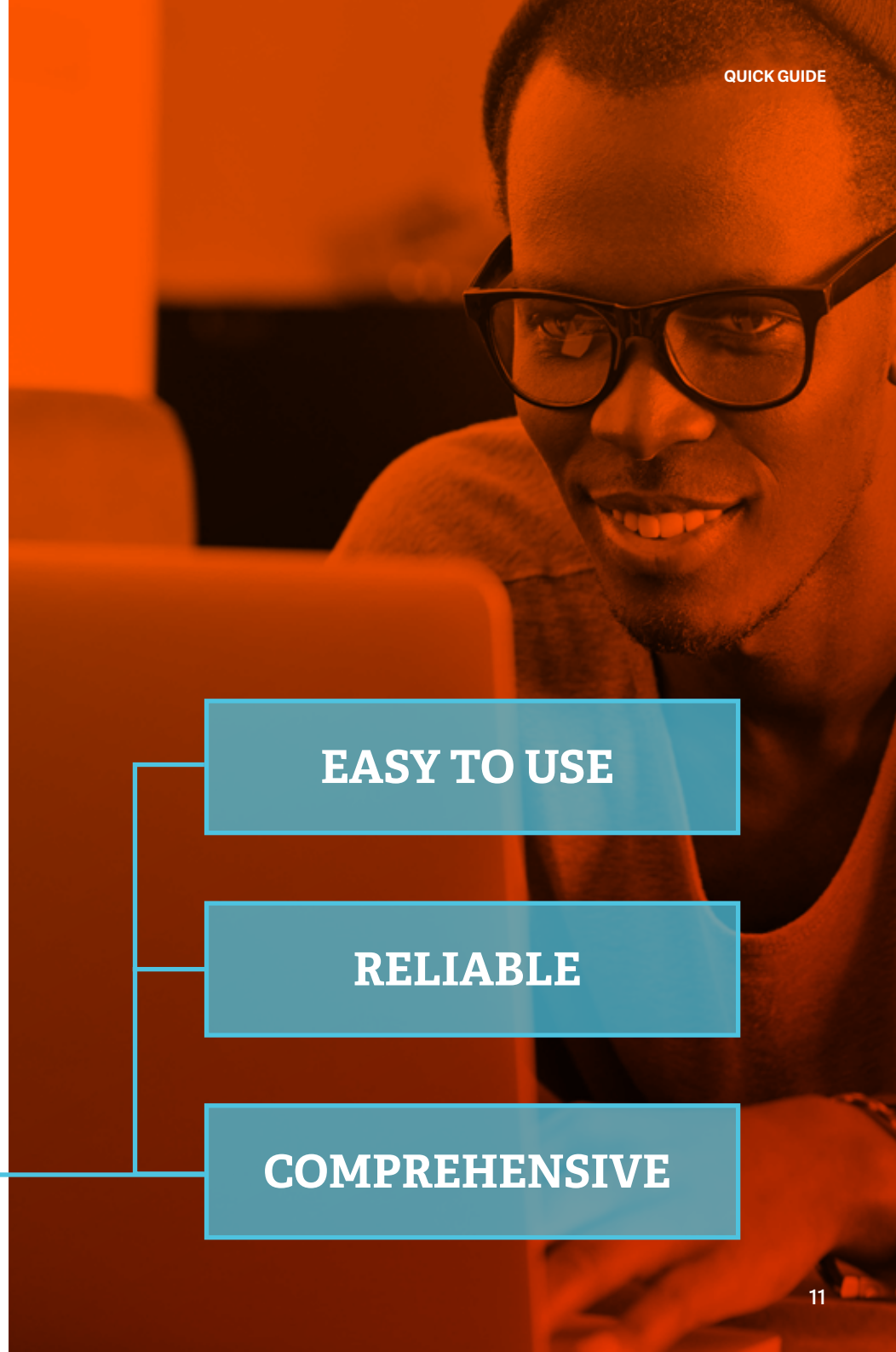
Are They Equipped to Handle the Surge?

THE MOUNTING PRESSURE ON THE IT SERVICE DESK

Mandatory work-from-home policies are placing immense demands on IT infrastructure and systems as employees turn to remote working en masse. This has a major impact on service desk employees who are trying to enable and support remote workers while working from home themselves.

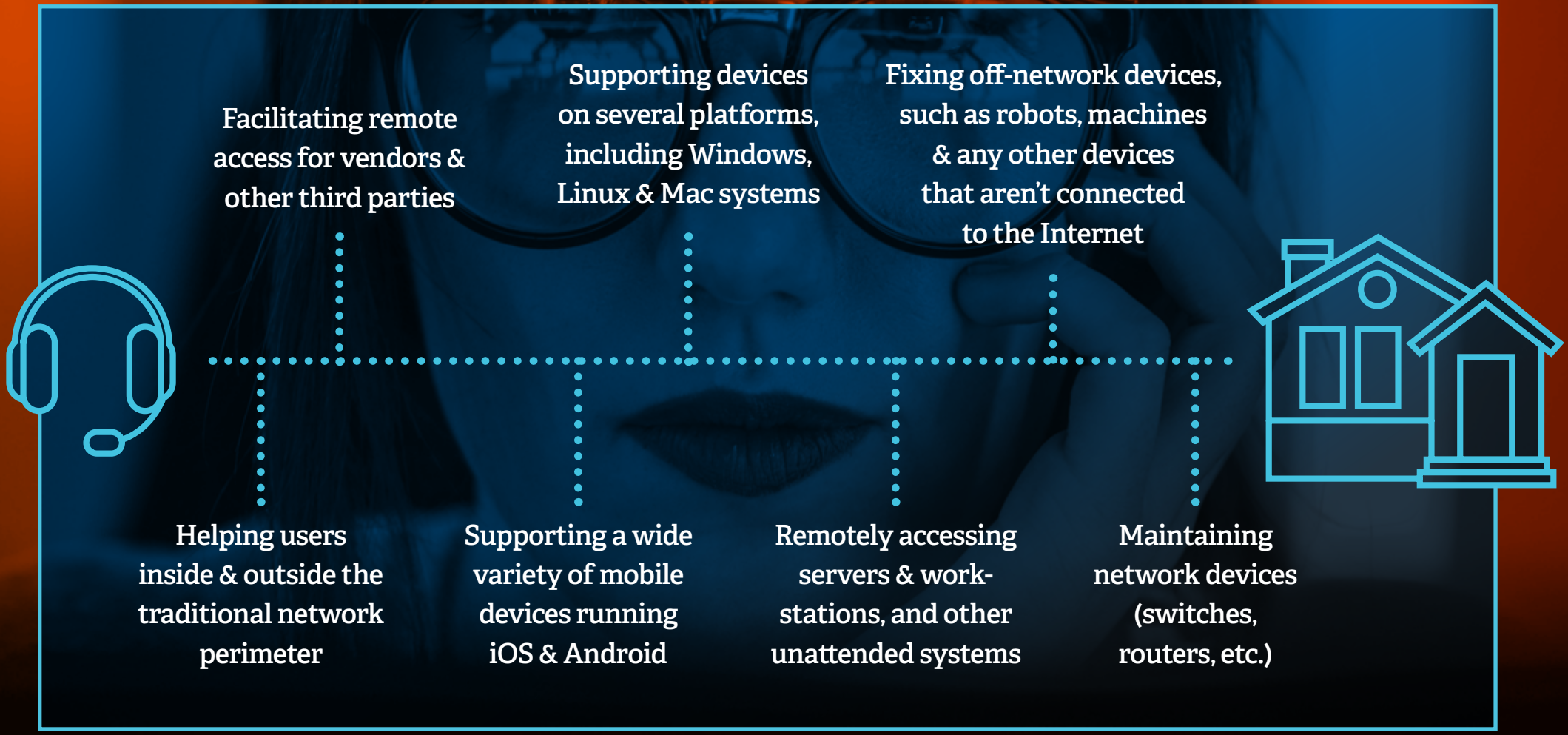
Effective remote support tools directly impact the success of remote working. These solutions must scale and adapt to meet rigorous security requirements while also driving technician productivity.

Furthermore, the solution must be:



POTENTIAL USE CASES

Organizations need a secure remote access solution that can cover an expansive list of use cases, while making the entire service desk experience more efficient and secure. Some common use cases include:



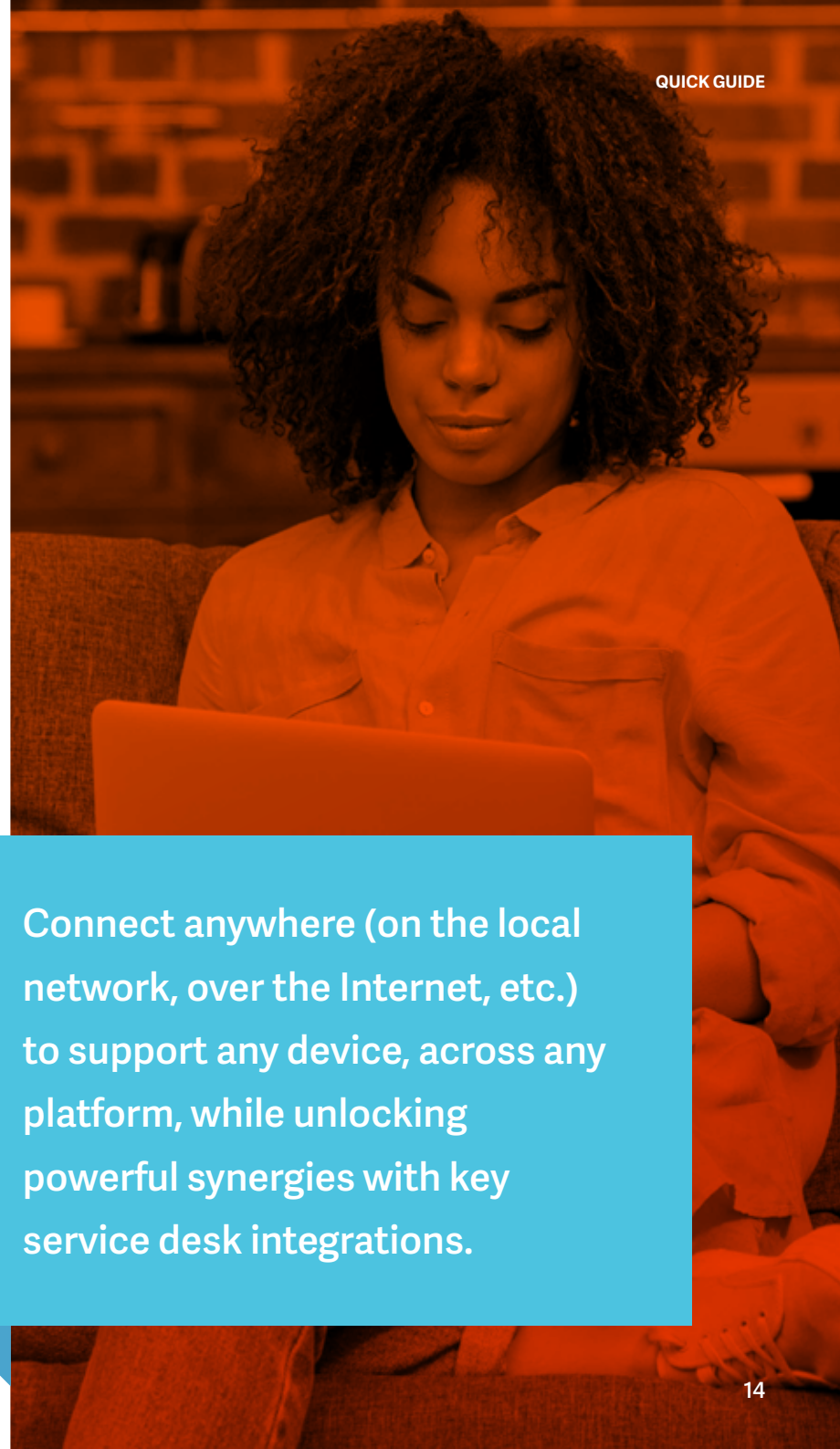
During such challenging times, choosing the right remote support software is critical to the productivity and security of your service desk.

SUPPORT ANY DEVICE OR SYSTEM, ANYWHERE

BeyondTrust Remote Support

Enable secure, reliable remote support for employees both on and off your network. See their screen, chat, elevate privileges, and access their mobile device camera to troubleshoot peripherals. Support Windows, Mac, Linux, iOS, Android, and network devices with a single solution.

BeyondTrust Remote Support is built to make your entire service desk work better. Our solution covers the broadest range of remote support use cases, while delivering the most robust remote access security available. BeyondTrust has the only Remote Support solution that meets the rigorous requirements of FIPS 140-2 Level 2.



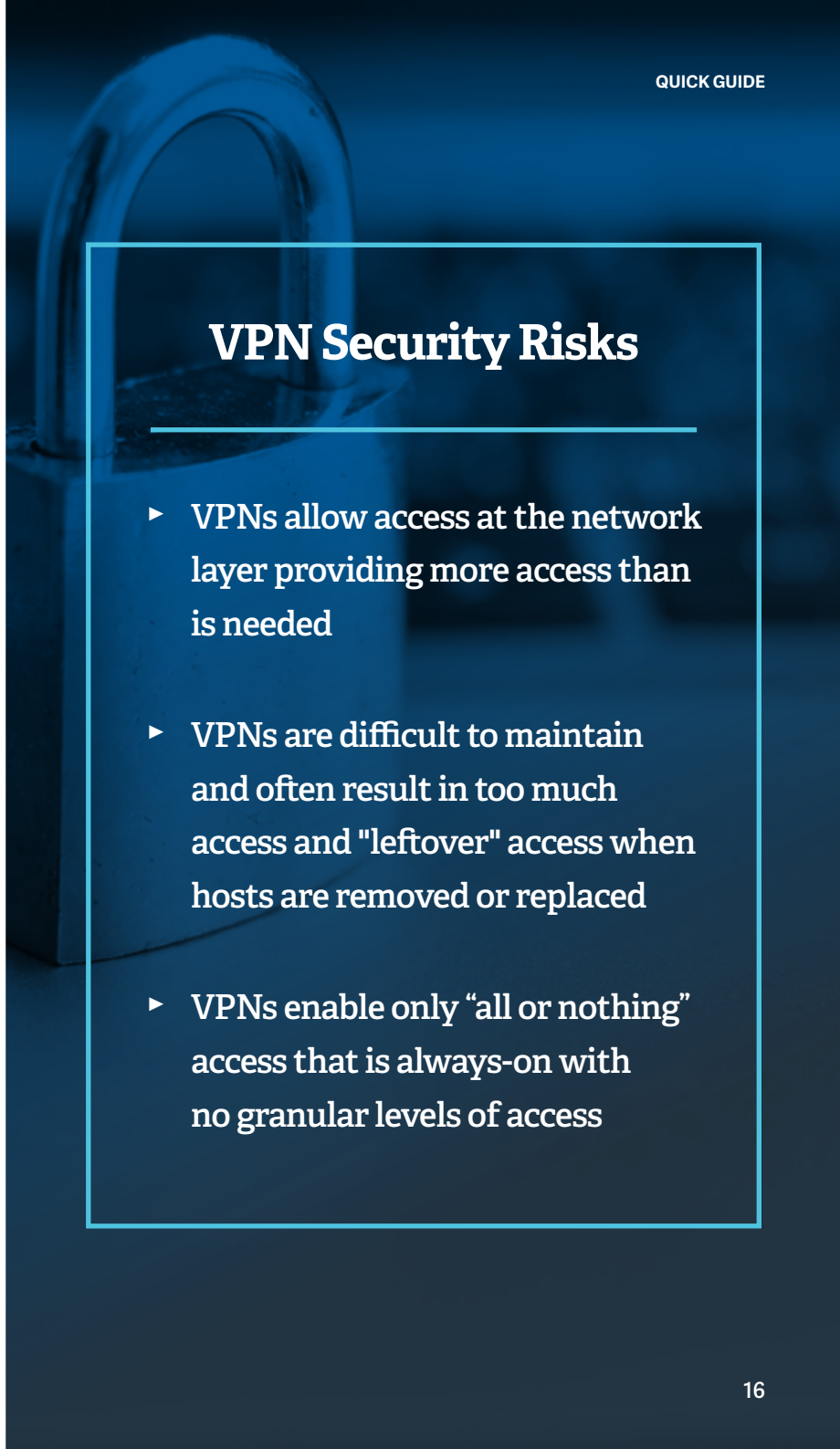
Connect anywhere (on the local network, over the Internet, etc.) to support any device, across any platform, while unlocking powerful synergies with key service desk integrations.

VPNs

Who's On Your Network & What Are They Doing?

THE SHORTCOMINGS OF VPN CONNECTIONS

Offering some sort of remote access is non-negotiable for almost every organization. Employees need to be able to access your systems from outside the firewall. However, remote access, by its very nature, creates exposure to cybersecurity risks. To establish remote connections for employees, organizations often use some form of Virtual Private Network (VPN) to allow users to interact with their systems. VPNs work well when remote employees have corporate laptops at home. But for employees who are connecting back to a corporate desktop from a personal laptop or device, or for contractors and vendors who are connecting into your systems, managing and securing VPNs presents a challenge.



VPN Security Risks

- VPNs allow access at the network layer providing more access than is needed
- VPNs are difficult to maintain and often result in too much access and "leftover" access when hosts are removed or replaced
- VPNs enable only “all or nothing” access that is always-on with no granular levels of access

MITIGATING THE VPN RISK

Hackers typically need days or weeks to find what they are after. If threat actors obtain VPN access from an exploited system to an internal network, they can often move around undetected and use pivoting techniques to find their ultimate target. Hackers will most likely target remote workers or external vendors using personal devices with VPN access knowing they may be easier to compromise.

182

Average number of third party vendors* that IT professionals report are accessing their internal network on a weekly basis.

Many of them are over privileged with more access than required for their roles.

*BeyondTrust, "Privileged Access Threat Report 2019"

BeyondTrust Privileged Remote Access

BeyondTrust Privileged Remote Access enables secure session management, with the ability to proxy access to RDP, SSH, and Windows/Unix/Linux hosts, without requiring a VPN. Dynamic assignment of just-in-time privileges via Adaptive Workflow Control allows organizations to lock down access to resources based upon the day, date, time, and location. For example, if you expect your remote workers to be logging on from particular systems, you can ensure that access is only permitted from predefined address ranges. Similarly, you can set up policies to control when the accounts are accessible, and alert when specific access policies are invoked.

Using BeyondTrust Privileged Remote Access in conjunction with your corporate VPN enables your organization to reduce the attack surface and drive productivity **in the following ways:**

1. Enforce a policy of least privilege by giving certain users just the right level of access
2. Enable individual accountability for shared accounts
3. Define what endpoints users can access and when to whitelist and blacklist applications
4. Remove the administrative burden of configuring and installing VPNs for vendors or remote workers using personal devices
5. Control and monitor sessions via a secure agent or using standard protocols for RDP, VNC, Web, and SSH connections

ADDITIONAL CONSIDERATIONS

VPN Performance

Most corporate VPN implementations, even used in conjunction with corporate-issued devices, are not architected to support the entire company working remotely. Enabling certain users, such as third-party vendors or employees on home devices, to access systems through Privileged Remote Access can help reduce the strain on your VPN and increase performance.

In addition to introducing security issues into the corporate environment, movement to VPNs en masse can result in severe network performance issues.

VPN Large-Scale Risks

- VPN technologies often lack rapid scalability, and when a significant number of employees or external workers suddenly need access, the solution may not perform at an acceptable level
- VPNs are highly dependent on the bandwidth available to the connecting user's home, and how much bandwidth the application requires
- VPNs are not typically configured to allow access to all of the resources that are available when someone is physically sitting on a trusted network within an office building

SIMPLIFIED REMOTE ACCESS

Use Any Company or Personal Device

A SIMPLE PATH FOR USERS

BeyondTrust Privileged Remote Access

Employees that left their desktops or laptops in the office can leverage BeyondTrust Privileged Remote Access to securely connect back to the very workstation they use every day. They can do this from a personal computer or tablet using only a web browser.

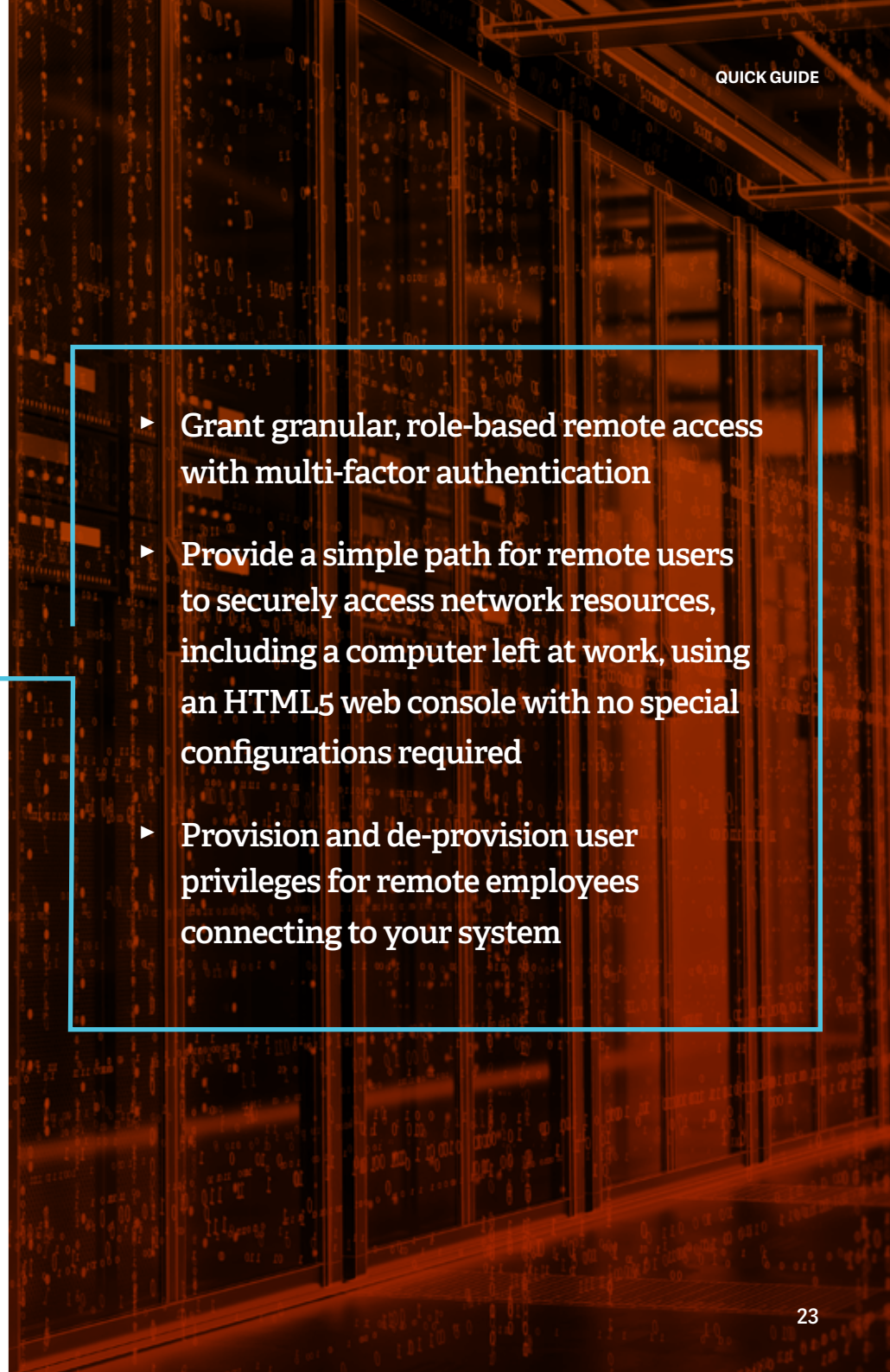
While many remote workers will use a company issued laptop, those that do not have access to one may be **using any of the following devices to connect to your network:**

BeyondTrust makes it easy for remote workers to access the resources they need to stay productive, using both company-issued and personal devices.

- Employees on personal devices
- Vendors or contractors using either company or personal laptops

While employees on company-issued devices are considered trusted, the other remote workers represent a significant security risk to your organization if connected to your VPN. These devices can be used by hackers to infiltrate your network and establish a persistent presence.

For all of these scenarios, **BeyondTrust enables IT teams to do the following:**



- Grant granular, role-based remote access with multi-factor authentication
- Provide a simple path for remote users to securely access network resources, including a computer left at work, using an HTML5 web console with no special configurations required
- Provision and de-provision user privileges for remote employees connecting to your system

CYBERHYGIENE

Passwords Are Like Germs — Don't Share Them!

THE ROLE OF PASSWORD MANAGEMENT

In addition to washing hands to avoid sharing germs with others during the coronavirus crisis, remote workers also need to stop sharing passwords. Passwords that are not properly managed or controlled represent a significant security risk for organizations. Users have too many passwords; as a result many employees often share, reuse, or store passwords insecurely. These habits create significant threats that leave your systems vulnerable to attacks.

When employees have trouble remembering passwords they often resort to:

When considering remote access solutions, an integration with a password vault is another key factor.

Bad Password Habits That Create Risk

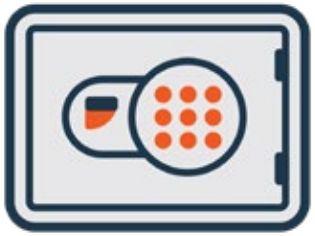
- Writing down their passwords
- Forgetting their passwords
- Choosing very simple, easily compromised passwords or reusing old passwords

PROTECT PRIVILEGED CREDENTIALS

BeyondTrust Vault

Included with Privileged Remote Access and Remote Support, the BeyondTrust Vault unifies comprehensive session management and essential credential vaulting for internal and third-party privileged users with a simple, fast cloud-based solution.

BeyondTrust Password Safe



For more advanced Password Management functionalities, BeyondTrust Password Safe combines privileged password and session management to discover, manage, and audit all privileged credential activity. Password Safe helps you protect privileged user accounts, applications, SSH keys, cloud admin accounts, RPA accounts, and more, with a searchable audit trail for compliance and forensics.

Get flexibility to protect and control the management of privileged credentials and session monitoring with models that adapt to your specific business needs.

ENDPOINT PRIVILEGE MANAGEMENT

Protect Remote Endpoints from Attacks & Malware

The abrupt, large-scale shift to remote work has not only disrupted normal end-user workflows and processes, it has also wreaked havoc on security processes and policies. Many organizations are inadequately prepared to support fully remote workforces, yet business continuity requires they find a way to make it work.

Workers who find themselves suddenly — often for the first time — forced to work remotely, may face these challenges:

- Displaced from their normal environments
- Disconnected from the secure corporate network
- Exposed to risk from external and internal threats
- Expected to suddenly use new technologies to stay connected and be productive

As a result, these employees are relying on the Service Desk to do more. If they feel they aren't getting what they need from IT, or just want to try and figure it out themselves, these workers will often self-provision the tools and applications — creating even more security risk.

Users either have **no admin rights** and can't do anything at all or have **full admin rights** and too much control.

ENSURE SECURITY & PRODUCTIVITY

With the increase of cyberattacks against remote workers, it's imperative for organizations to secure end-user machines and prevent malware and ransomware from being introduced into your corporate environment.

BeyondTrust Endpoint Privilege Management solutions enforce least privilege across all desktops and servers, enabling the exact level of privileged access end users need — while preventing malware and ransomware from being introduced into your corporate network. This empowers users to perform day-to-day activities, such as installing and updating approved applications and printers, cameras, etc., without giving them full administrative rights and without overwhelming the service desk.

*Ponemon Institute, "The Third Annual Study on the State of Endpoint Security Risk", January 2020

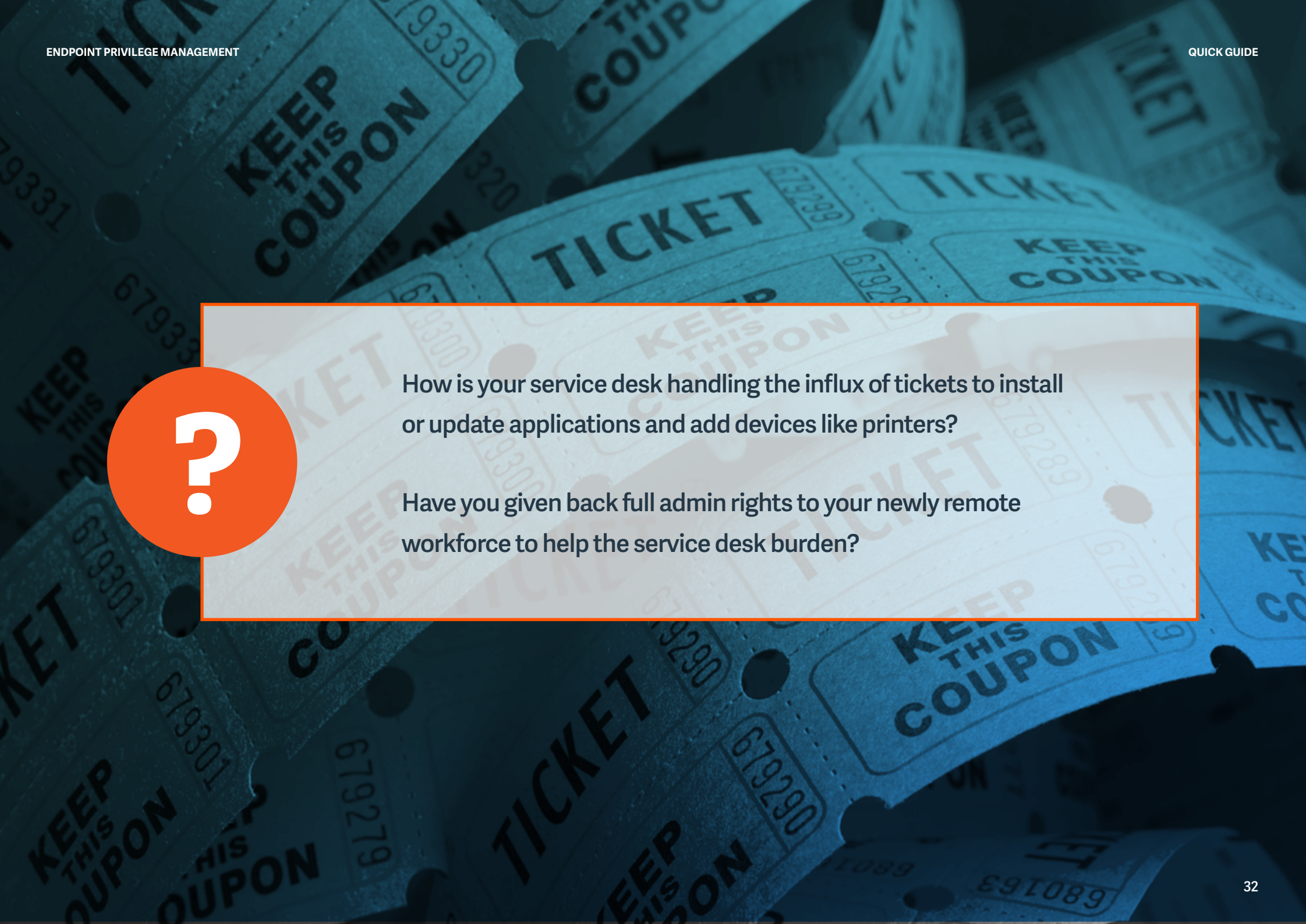
Prevent the attacks missed by antivirus software by removing admin rights, implementing least privilege, enabling privilege elevation, and securing apps with total application protection.

With Endpoint Privilege Management, organizations can quickly implement policies across all users or groups of users. Plus, our unique QuickStart policies that leverage data from thousands of deployments, allow IT administrators to rollout flexible workstyle templates and operationalize quickly.

With global deployments spanning more than 50 million endpoints and a myriad of industries, our experience has helped to create a tried and tested approach providing unmatched time-to-value across the industry.

> My bigger customers have measured a **75% reduction** in the amount of service desk tickets after removing admin rights.
>
> *- Sami Laiho, Microsoft MVP & Ethical Hacker**

**BeyondTrust, "Microsoft Vulnerabilities Report 2020"*



?

How is your service desk handling the influx of tickets to install or update applications and add devices like printers?

Have you given back full admin rights to your newly remote workforce to help the service desk burden?

REDUCES SERVICE DESK BURDEN

BeyondTrust Privilege Management for Windows & Mac

Eliminate unnecessary privileges and elevate rights for Windows and Mac users without hindering productivity. We've combined best-in-class privilege management and application control, making admin rights removal simple to ensure compliance, security, and efficiency.

Features and benefits include:

- Deflecting service desk tickets and empowering users to install and run their own pre-approved applications, with out-of-the-box policies
- Giving users ad hoc elevation rights to install only approved/safe applications
- Integrating with ServiceNow and other ITSM tools to automate the submission of a ticket to the service desk, so that they can make an informed and expedited decision on the user's request to run an application, installation, script, or task
- Quickly fixing a problem once — for all users — through broad policy updates
- Empowering users to self-install printers and other accepted hardware

?

How can you prevent users from introducing malware and ransomware into your environment?

BeyondTrust Privilege Management for Windows and Mac reduces the attack surface in the **following ways:**

1. Enforcing least privilege across the desktop environment, as well as servers — maintaining security, user productivity, and operational efficiency
2. Stopping attacks involving trusted apps, catching bad scripts and infected email attachments in real time
3. Using an automated whitelist and elegant exception handling to provide complete control over what users can install or run
4. Providing a single audit trail of all user activity to streamline forensics and simplify compliance
5. Correlating user behavior against asset vulnerability data and security intelligence to assess end-user risk with advanced threat analytics

THE TIME IS NOW

Enable Remote Workers Today

GET UP & RUNNING FAST WITH SIMPLE DEPLOYMENT

BeyondTrust solutions are available in multiple deployment options, including virtual appliances and SaaS, which can be up and running very quickly. With BeyondTrust's Secure Remote Access solutions, no desktop agent downloads are required – users can log in through a web console from any browser. For Endpoint Privilege Management (EPM), agents are quickly deployed to the endpoints, with policies enforced – without interruption to the users.

Simplified administration and streamlined or automated workflows ease the burden on your IT teams as well. The following are the benefits from using BeyondTrust's solutions:

THE BENEFITS

Consolidated Access Pathways	Tracking the Access	Mobile Apps	Audit Trail	QuickStart Policies (EPM)
Broker all connections through a single access pathway, reduce the attack surface and provide a single list of authorized endpoints available for each user	Set preferences to be alerted when a vendor/ privileged user is accessing your network/systems, or a remote access-initiated session is occurring	Administrators can use their mobile devices to approve requests and monitor access usage from anywhere	Record all sessions to satisfy compliance requirements and for use in session forensics and other reporting needs	Maintain security, user productivity, and IT operational efficiency by enforcing least privilege across the desktop environment

BeyondTrust enables organizations to apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks. Users can **quickly and securely access any remote system, running any platform, located anywhere**, and leverage an integrated password vault to discover, onboard, and manage privileged credentials.

Gain absolute visibility and control over internal and external remote access, secure connectivity to managed assets, and create a complete, unimpeachable audit trail that simplifies your path to compliance.

In addition, stop users from downloading malicious software and opening dangerous phishing attachments that could lead to overwhelming harm in your corporate environment.

All while reducing the influx of service desk tickets and continuing to meet compliance regulations.

Our approach creates a frictionless experience for users, enabling the right level of access at just the right time.

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/remote-workers