

Securing External and Remote Access

How to reduce the remote risk and achieve digital transformation



Securing External and Remote Access

How to reduce the remote risk and achieve digital transformation

TABLE OF CONTENTS

1. EXTERNAL AND REMOTE ACCESS OVERVIEW	2
2. SOLUTIONS FOR MANAGING EXTERNAL ACCESS	6
3. SECURING EXTERNAL AND REMOTE ACCESS	11
CONCLUSION	15

EXTERNAL AND REMOTE ACCESS OVERVIEW

Introduction

In the modern IT environment, organizations need to enable external access to their information systems for service providers and remote employees alike. Digital transformation, the shift towards employing new digital technologies to make existing services more effective and efficient, is a priority for many enterprises. As such, it is having a major effect on business processes and cultures, including working practices. The increasing use of external and remote access is both a by-product of the race towards digital transformation and a way to enable it.

Externalization empowers the virtual collaboration and flexibility that drive digital transformation. However, it also presents organizations with a new set of challenges, particularly around access security. IT departments may struggle to have the same level of control and visibility when IT services or resources are accessed remotely, from outside the corporate security perimeter. Issues of maintaining compliance, managing privileged access, and moving security from the perimeter to the endpoint all come into play.

Many existing solutions do not offer the visibility, granular control, and limitation of privileges needed to secure external access to critical IT assets. To leverage the opportunities that remote access offers in driving digital transformation, organizations must employ a robust access security framework that incorporates a strong PAM (Privileged Access Management) solution and an EPM (Endpoint Privilege Management) solution. By securing remote access for external providers and remote employees alike, organizations can advance towards a secure digital future.

Why Organizations Rely On External Access

In the modern IT environment, with digital transformation both a priority and an inevitability, there are many reasons why users may require external access to an organization's IT services or resources to carry out daily tasks or to work on infrastructure requiring elevated privileges. We can break the need for external access down into three common scenarios:

Enabling Contractor and Third-Party Services

Many companies turn to third-party organizations to manage some or all of their IT infrastructure. This requires them to open their IT infrastructures to an increasing number of external service providers, including:

- Vendors who intervene and maintain their own software applications or equipment
- IT operators who manage all or part of the complete infrastructure (the outsourcing of IT services is common amongst smaller organizations and those with small IT teams)
- Consultants who work with organizations for specified periods or on specific projects
- Managed Security Service Providers (MSSPs) who deliver outsourced management or monitoring of cybersecurity

The need for third-party access spans a wide variety of sectors. Healthcare organizations may

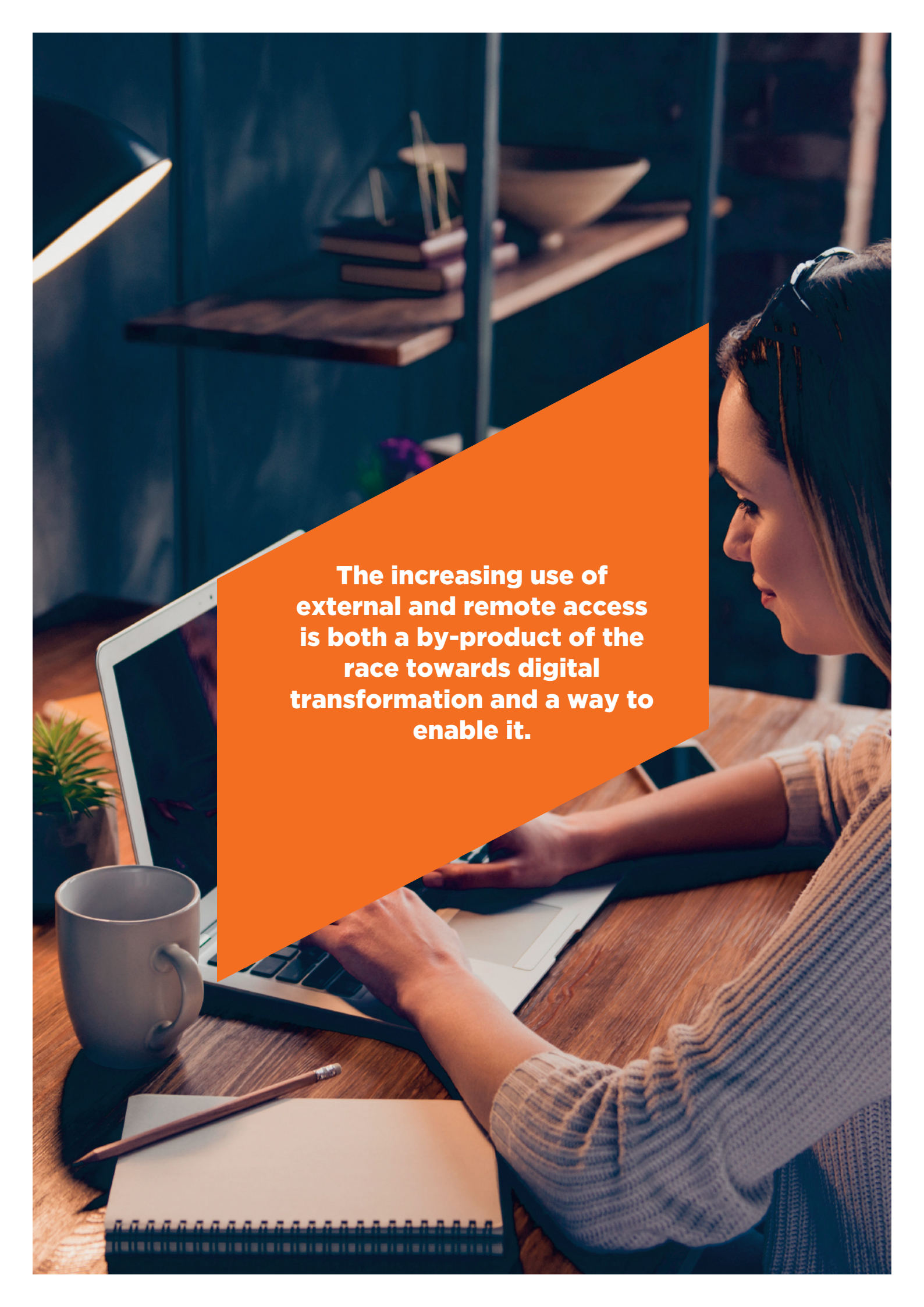
require external licensed technicians to maintain and calibrate equipment such as MRI machines. Financial institutions may enlist contractors to manage servers holding highly sensitive customer or bank data. Industrial and manufacturing organizations make have a geographically distributed workforce needing to intervene on production lines in plants across the globe.

Cloud hosting is one emergent trend that exemplifies the need for external access in the age of digital transformation. In a cloud hosting service, a third-party provider offers an organization infrastructure services for its computing and storage resources. Cloud hosting is a form of externalization that allows organizations to better manage IT budgets, access expertise that's beyond the remit of the in-house IT team, and scale up capacity with ease.

The benefits of facilitating remote access to IT resources are obvious. But, as with all forms of externalization of information services, the external provider may end up being granted traceless privileged access to sensitive and critical resources within the organization. Even if this access is given for just a short period, risks emerge.

Enabling Remote Access for Employees

External access is not only required by third-party providers. These days remote access is often needed by employees of the organization, with increasingly dispersed workforces and adoption of

A woman with long dark hair, wearing a light-colored sweater, is sitting at a wooden desk in a modern office. She is looking at a laptop screen and has her hands on the keyboard. On the desk, there is a white mug, a pencil, and a spiral notebook. In the background, there is a shelf with books and a small plant. An orange diagonal overlay covers the right side of the image, containing white text.

**The increasing use of
external and remote access
is both a by-product of the
race towards digital
transformation and a way to
enable it.**

remote work. Where this need may once have been restricted to administrators requiring occasional external access for off-hours response, the concept of employees working remotely has become the 'new normal' for many organizations.

Employees often work remotely on a part-time or occasional basis, and distributed workforces (with employees working from multiple geographical locations) are increasingly common. Organizations such as GitLab and Zapier have gone as far as to adopt a fully remote approach, where the entire workforce is spread across multiple countries and company-wide remote work policies are in effect. This is again true across sectors; no business sector is exempt from this aspect of digital transformation in an increasingly connected world.

Remote work has also been shown to have benefits on workforce productivity and wellbeing. Results from the [IWG Global Workplace Survey](#) suggest that 4 out of every 5 candidates would turn down a job offer without flexible working in favor of a similar offer that included this benefit. But in terms of security, a distributed workforce means a broader attack surface. This increased threat overlaps with:

- Remote workers' expectations that they will have the same access to data and systems that they would in the office
- Their use of shadow IT (hardware or software that is not supported by the organization's IT department) and need to access or download software despite being far from Helpdesk support

- The IT department's lack of oversight into actions carried out by remote workers
- The introduction of BYOD (Bring Your Own Device) policies that enable workers to connect to organizational networks on their personal devices

Facilitating Remote Collaboration

Central to both the external provision of key services and the rise of remote work is the issue of remote collaboration. Collaboration is as key to digital transformation as it is to work in general. In an age where workforces are increasingly distributed and external providers are needed to keep pace with competition, collaborative processes often take place through digital means – with employees, teams, and external providers working in concert across dispersed locations and time zones, and on different endpoints and devices.

Let's take the rise of DevOps as an example of where remote collaboration is paramount. DevOps is an IT model that combines software development and IT operations for more efficient and rapid advancement, an approach which can accelerate the speed at which a business releases software. In encouraging communication, integration, and automation between these two traditionally separated teams, the DevOps approach requires collaboration, with the shared goal of delivering at speed and scale.

In such a fast-paced environment, there is a tendency within DevOps teams to share privileged access credentials or even hard-code passwords

into scripts for faster automation. These practices happen for the sake of speedier workflows – but can come at the expense of business security.

Existing collaboration tools can also compromise security. Collaborative platforms enabling multiple users to share a work session are readily available, but they also offer bad actors a place where they can infiltrate the network or pose as a trusted employee to share malicious files or move laterally into resources where they can access sensitive data.

External Access and Digital Transformation: The State of the Landscape

The need for remote access is only increasing. Chasing ever-growing competition in the race to digital transformation, companies are more likely to invest in new technologies and employ external providers to implement them, with cloud adoption one major example: a Flexera report found that in 2019, 45% of enterprises prioritized a hybrid cloud solution while 31% saw public cloud as their top priority.

Rates of remote work are similarly expanding. Global Workplace Analytics estimates that regular work-at-home in the US grew 173% between 2005 and 2018, 11% faster than the rest of the workforce and nearly 47 times faster than the self-employed population.

In this context, it's clear that an organization's important assets can't be siloed by region or isolated from the world outside the corporate network. External and remote access is critical to today's businesses and to enabling productivity and digital transformation. Trends such as cloud

hosting and DevOps show the necessity of being able to secure external connections and facilitate successful remote collaborations.

Enabling remote access to IT resources brings clear benefits, but it also poses a key problem. Through the process of externalization, companies can lose control and visibility over what resources users have access privileges to, a particularly sensitive issue when concerning critical systems and data. This can lead to issues around:

- Regulatory compliance
- Access management
- Leaving organizations vulnerable to malicious actors

Let's take a closer look at these issues and explore how effective traditional solutions for enabling external access are at addressing them and delivering secure access.

SOLUTIONS FOR MANAGING EXTERNAL ACCESS

The Challenges of Securing External Access

A variety of solutions exist to enable external and remote access to corporate networks in some form or another. They include:

- **VPNs (Virtual Private Networks)**
- **IPsec (Internet Protocol Security)**
- **SSL (Secure Socket Layer)**
- **Proxy servers**

- Leased lines
- NGAV (Next-Generation Antivirus) to protect endpoints
- Internal security measures

In order to consider the effectiveness of these solutions, it's worth looking in more detail at the various challenges that remote access brings organizations.

Security Risks

For fragmented organizations and enterprises relying heavily on external contractors or remote workers, each instance of external access to the network opens up a vulnerability that puts the IT infrastructure at risk of a data or system breach. Breaches could result in:

- Information leaks
- Destruction of sensitive data
- Theft of intellectual property
- Financial loss
- Reputational damage

In diverse modern IT environments, broad, external defenses are often not enough. For example, the remote access VPN, once deemed vital to securing external access, has become one of the most common targets for cybercriminals; it exposes servers to the internet and requires users

to be placed on the organizational network through tunnels that poke holes in the firewall, creating vulnerabilities to malware and ransomware. VPNs are also untraceable, offering no way to know who is accessing the network, what resources they are accessing, or when they have access to them. Due to such vulnerabilities, Gartner predicts 60% of enterprises will phase out most of their remote access VPNs by 2023.

“Traditional access solutions like VPNs are untraceable, offering no way to know who is accessing the network, what resources they are accessing, or when they have access to them.”

Insider Threat

Even where remote workers and external service providers are deemed entirely trustworthy, every instance of legitimate access carries the risk of inadvertent breach. Any individual who has privileged access (e.g. login credentials) to sensitive servers, data, and systems can be deemed an insider threat, as each user's access

credentials create a point of vulnerability. Insider threat is a considerable risk given that it is employee error and negligence, not malicious intent, that are the leading causes of data breaches.

External access can magnify existing insider threats such as lost or stolen credentials or overprivileged access. This is due to the external location of access (meaning reduced oversight and control) and exponential numbers of remote

workers. The proliferation of endpoints that aren't covered by the organization's perimeter security, and the use of BYOD policies increase the insider threat risk and the vulnerabilities to spam, malware and ransomware.

Endpoint Access Management

When it comes to the risks of external access, endpoints such as servers and workstations are sitting targets, offering attackers ways to infiltrate a system. Endpoints are especially vulnerable when taken outside of the corporate network as they no longer benefit from any perimeter security measures. Despite this, the increased prevalence of remote workforces and BYOD policies means a proliferation of endpoints – some entirely uncontrolled by the organization – creating avenues into critical systems.

Although software vendors have developed protections such as the Next Generation Antivirus (NGAV) which relies on tools including Machine Learning and Endpoint Detection and Response (EDR), these technologies tend to take a reactive rather than proactive approach, focused on identifying existing, known threats rather than protecting the system from the inside.

Regulatory Compliance

Solutions that permit external access to critical systems must also maintain and ensure compliance with various regulatory standards, including GDPR, PCI-DSS, NIST, NIS, and ISO 27001.

Let's focus on GDPR as one of the strictest and most wide-ranging set of regulations, and a model for regulations including California's CCPA. GDPR requires all companies that collect data about European Union (E.U.) citizens to prove they have security measures in place to protect those citizens' data privacy. Risks that must be assessed include loss, alteration, and unauthorized access to or disclosure of data.

Although GDPR does not attempt to prescribe specific technical measures that must be taken for data security, it does lay out some general requirements, including:

- Controllers (those who assess what data is collected and for what purpose) and Processors (those who actually work with the data) should always maintain the confidentiality, integrity, and availability of data
- There should be ongoing assessment of data security, both technically and organizationally
- The Controller must be able to prove compliance and the Processor must ensure they can document compliance

GDPR compliance boils down to supervision and traceability. Strict control over privileged access to assets is needed – and that access must be traced, monitored, and logged for audit and proof of compliance. The introduction of GDPR-inspired initiatives in key US states, such as the SHIELD act in New York and the CCPA in California, suggests these concerns will only grow more pertinent.

Despite this, most of the traditional remote and external access solutions outlined above do not include the tools and detailed logs necessary to meet the supervision and traceability requirements expected by many cybersecurity regulations, GDPR included.

Why Traditional Solutions Are No Longer Enough

The broad issues with traditional solutions for securing external access can be narrowed into three areas:

Insufficient Traceability

A lack of clear records can make it difficult to get a complete view of what has been done by a privileged user during a session. For organizations with remote workers, this means any actions that have inadvertently caused a data breach cannot be pinpointed and so effective measures to recover and to safeguard against a repeat offense cannot be taken. For external providers, the inability to provide a clear record of actions is at odds with their need to demonstrate accountability and maintain relationships built on trust with client organizations. What's more, in order to prove compliance, it's imperative that privileged sessions be monitored and logged.

Low Granularity of Rights

Many existing solutions for granting access are simplistic, giving organizations an insufficient level of control over who is connecting into which

resources. With these tools, organizations authorize connections to a target IP address that represents a server or entire network infrastructure, but do not have the ability to narrow it down to specific targets or actions.

This setup means it is impossible to authorize a connection for one or several specific accounts without providing access to all of the accounts for a given IP address. This broadens the attack surface and leaves an organization at greater risk of a breach than if granular account permissions were in place.

A more robust solution could grant remote or internal users access to the specific resources they need to do their task without also making visible other resources on the same network. It would also offer granularity in terms of what actions could be permitted within the target resource. An effective PEDM (Privileged Elevation and Delegation Management) solution, for example, would give organizations the ability to elevate privileges as and when needed for third-party contractors and employees alike, then revoke those privileges when the need expires to maintain strict access controls and minimize insider threat. To secure endpoints, privileges could be addressed at the application and process level for more granular control. Without local admin rights, no intruder or malware could acquire the necessary privileges to run any processes and applications to inflict damage.

Password Exposure

The use of root passwords alone represents a

considerable security risk, but further risks are created when passwords to privileged accounts granted outside the organizations are shared, rarely changed, or if they're similar and easy to guess.

For external service providers, existing solutions require third-party workers to be assigned unique account access details that are specific to the target equipment ("administrator" access details for a Windows system, "root" access for Unix/Linux servers, etc.). These credentials provide extended access to a service provider that can represent a considerable security risk. Simply knowing the password in the first place is a security risk.

Remote workers can expose their employer to threats by reusing the same passwords for work and their personal devices. The practice of password reuse could allow an attacker to obtain credentials from a user's leisure-affiliated account and use it to gain access to their work account.

How to Secure External Access: Best Practices

Despite the challenges of external access and the limitations of existing solutions, establishing a relationship of mutual confidence between organization and employee or contractor while working remotely is achievable. First, organizations employing external service providers and/or remote workers must take into account some best practices that serve the united goal of making external actions tangible.

Limit Privileged Access

A privileged user is anyone who has elevated rights or administrative access to critical systems. By limiting privileges, an organization ensures that only a small number of people can access only a small number of systems — and only when needed. This Principle of Least Privilege holds that users are granted only the privileges necessary for them to carry out their job, for the duration required. This allows organizations to minimize the risk of insider threat and secure remote collaboration by removing excess, unnecessary privileges that could otherwise leave the infrastructure exposed. External providers and remote workers alike only have access to the organizational data needed to perform their job, no more and no less, even when collaborating.

Ideally, this practice should extend to enforcing privileges at the endpoint itself. When privileges are managed at the application and process level, regardless of the individual user's privilege level, the issue of local admin rights (and their attendant risks) is eliminated, without any extra pressure being placed on the IT helpdesk and without hampering the end user's productivity.

Achieve Compliance

Complying with cybersecurity regulations and standards is vital, especially if when managing critical resources or manipulating sensitive data. These policies and requirements drastically reduce system vulnerabilities even when open to external access, ensuring business continuity and

productivity and, of course, avoiding hefty fines for non-compliance. It is here that strong processes for auditing, tracing, and monitoring user actions are crucial.

Proper tools can save organizations and third-party providers significant time and stress by illustrating exactly what actions have been taken on a system, eliminating long recovery analysis, and allowing actions to be monitored and audited in case of a security breach. These include session management tools that allow compliance to be documented by providing unalterable audit trails and OCR (Optical Character Recognition) recordings that enable security teams to catch all surreptitious activity and easily search through metadata rather than spend hours watching footage.

These best practices are rooted in and can be achieved with a robust access security framework that relies on key Privileged Access Management (PAM) and Endpoint Privilege Management (EPM) concepts.

SECURING EXTERNAL AND REMOTE ACCESS

Privileged Access Management: Key Concepts

Zero Trust

A robust PAM solution for securing external access will always incorporate the concept of zero trust. The zero-trust model to security rests on the principle that no user is trusted implicitly when it

comes to accessing an organization's critical data. In this model, users are proactively required to prove that they have both the need and the authorization to access a network resource before that access is granted.

It makes sense to implement a zero-trust model when it comes to any user accessing sensitive IT assets, especially those connecting from outside the business's network. When work is carried out beyond perimeter security, on a variety of endpoints and devices, and by a combination of employees and third-party providers, insider threat is a significant risk and the attack surface is broadened. A zero-trust model combats this by clamping down on unauthorized access of any kind, from any user, from anywhere.

Principle of Least Privilege

Central to a zero-trust model is the Principle of Least Privilege, which by reducing privileges to the absolute minimum required ensures that if credentials are stolen, the impact that a hacker can make is mitigated. Applying least privilege or, similarly, Zero Standing Privileges involves the effective restriction of individual users' rights within an organization's IT infrastructure and is applicable to employees and providers whether they are remote or in-house. At its core, it means ensuring that any access to sensitive information is only granted to users who need that information to perform their work task when they need it, and revoked when the need expires.

Here is an example of the Principle of Least Privilege in action:

- Frank is a third-party specialist who has been contracted to carry out some administrative work for Anna's organization.
- Frank does not need the same levels of access and permission as Anna, who can access servers containing the company's consumer data. Nor does he need to even be aware of assets beyond the one on which he intends to work.
- By ensuring that Frank has access only to Server A and only from 9AM to 5PM on designated days, the Principle of Least Privilege eliminates the risk that Frank could bounce laterally across the network into other resources, exposing sensitive customer data.
- Anna's organization remains secure and compliant with myriad regulatory frameworks.

A robust Privileged Access Management (PAM) solution typically includes a range of powerful access control and monitoring capabilities to apply the Principle of Least Privilege and detect and defend against security threats.

- See precisely what actions remote users have taken with their access privileges. **Session Management and Monitoring** enables comprehensive oversight of privileged session activity, including visibility over keystrokes and command line and collaborative sessions. Unalterable audit logs deliver proof of compliance as well as means of training and incident recovery.

- Grant and revoke privileges from a simple, centralized console and enable remote users to connect to sensitive assets securely from any device through a web portal. Reduce the risk that an external contractor will retain access to the organization's critical systems once their task is complete with automated and streamlined privilege management.

- Implement a Zero Standing Privileges policy with **Privilege Elevation and Delegation Management (PEDM)**, streamlining users' requests for elevated privileges to accomplish their tasks for the timeframe necessary.

- Increase password security with robust credential vaulting, automated password rotation, and enforcement of complexity of criteria. A **Password Management** system prevents privileged users from knowing the actual passwords to critical systems and renders credentials ineffective even if those known are stolen.

A PAM solution helps to facilitate a strong access privilege policy even when remote and external access is required. And for the modern IT environment, an effective PAM solution can be integrated across both cloud and on-premises environments for system-wide access security.

Endpoint Privilege Management: Key Concepts

In a traditional IT environment, employees' workstations remain safely within the corporate security perimeter, benefitting from its full

protection. In today's "digital transformation" context, user endpoints may be located anywhere around the globe, exposing them to a wide variety of external threats. When each remote employee or external contractor represents a new vulnerable entry point, a powerful Endpoint Privilege Management is essential to effectively secure remote access.

Endpoint Privilege Management (EPM) protects endpoints such as user workstations and servers from malware and other malicious activities attempting to infiltrate the IT network. Rather than settling for the reactive approach of attempting to identify, then block known attacks, it proactively prevents whatever is not deemed a legitimate action from being performed.

This approach is particularly interesting for endpoints exposed to external networks, including those used by service providers and remote employees. By deploying internal protections, it ensures that the system cannot be harmed even if the infiltration occurs outside of the corporate network. EPM employs the Principle of Least Privilege by ensuring that an intruder or malware is not able to acquire the necessary privileges to run processes and applications despite being outside of perimeteric protections.

Best-in-class solutions take EPM to another level by controlling privileges at the process and application level, not the user level. Local systems are no longer only protected against known threats or against users. With the best EPM solutions, the defense is carried out at an even more granular

level for deeper, more tailored control and security.

Providing granular protection at the process level:

- Allows the user to maintain access to all the tools necessary to accomplish their tasks efficiently without calling IT for every privilege elevation need (e.g. downloading software, running a process)
- Ensures that malware, ransomware, and cryptoviruses are unable to harm the system should they find a way onto the endpoint, as they are unable to elevate their privileges to execute, regardless of the user's privilege level.

And by fusing the key concepts of Privileged Access Management and Endpoint Privilege Management together, an organization can create a robust end-to-end access security framework that secures external and remote access.

The Benefits of End-to-End Access Security

Robust access security, grounded in strong PAM and EPM solutions, offers a number of benefits to today's organization in the throes of the digital transformation.

Reduced Security Risk with More Visibility

Maintaining visibility of user actions has traditionally been the biggest challenge of securing remote access. The best access security solutions provide both traceability and supervision, allowing all privileged sessions – remote or

otherwise – to be logged, recorded, and searchable. Real-time session monitoring and management provides automatic termination of suspicious activity in addition to inalterable access and activity logs that can be reviewed for a clear picture of what was carried out by a service provider or remote user on target equipment or applications.

Minimized Business Risk with More Control

By implementing the Principle of Least Privilege, robust access security offers organizations control over the permissions granted at both the user and application levels, from streamlined and centralized systems. Control over external access is made simple with granular account permissions and blocking capabilities.

With high-level password management and control over privilege elevation, organizations remain in control over all access to sensitive IT resources. Organizations can enforce password rotation policies for remote users and eliminate hard-coded passwords forgotten in scripts by DevOps through Application-to-Application Password Management effectively accelerating productivity and improving security at once.

Seamless and Secure Collaboration

Organizations and users can work in mutual confidence with strong yet easy-to-use access security to facilitate the collaboration that drives digital transformation. The most effective Privileged Access Management solutions enable

users to securely connect from anywhere to receive remote assistance, be trained by an equipment vendor, or assist a third-party contractor during system maintenance tasks. IT team members can securely connect to existing user sessions for ongoing assistance and Managed Service Providers can securely share sessions for enhanced collaboration no matter where users are located.

Better User Experience

With a streamlined platform facilitating centralized access to any number of authorized resources, and no passwords to memorize or jot down, privileged users can work simply and without disruption. Seamless remote collaboration offers clear benefits for employees, and remote users can use their own devices for maximum efficiency while the traditional cybersecurity risks of BYOD are mitigated by a unified PAM-EPM security strategy. With both PAM and EPM in place, users can run all the applications they need, and IT retains control over authorized processes and privilege elevation for enhanced efficiency on all sides.

Achieve Regulatory Compliance

Cybersecurity regulations require strict control over who has access to which resources and data. Proper remote access security allows you to meet – and prove – audit and compliance requirements through session management and password management capabilities. Granular, tailored privilege management and detailed logs of all sessions help meet the strict supervision and traceability expectations of various regulatory

frameworks. Defining rules that allow remote access rights to be automatically authenticated and revoked for a given period means there's no risk of remote users compromising your organization's compliant status.

Conclusion

Securing remote and external access with robust security technologies like Privileged Access Management and Endpoint Privilege Management allows organizations to pursue digital transformation with renewed confidence. The benefits of digital technologies and modern business trends including cloud hosting, DevOps, and BYOD policies can be implemented within a secure framework that offers control and visibility both on-premises and in the cloud for internal and external users.

That robust level of access security can be applied regardless of the endpoints and devices that data is being accessed from. Once access is secured, the goals of seamless collaboration, flexibility, and new levels of efficiency are within reach. Organizations can leverage the full opportunities of external and remote access with added peace of mind: driving digital transformation with advanced solutions supporting a secure digital future.

about WALLIX

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

WWW.WALLIX.COM

