Delinea

Remote Access Granted

How to secure access to critical data and resources

Executive Summary

Providing users access to sensitive systems and data from outside your corporate network is a must-have, everyday requirement, not a nice-to-have or emergency-only situation. As you add remote talent, rely on more third parties, and expand through mergers and acquisitions (M&A), user demand for remote access increases.

So does the risk.

In this eBook, you'll see what can happen when remote users in each of these scenarios can't easily get the access they need.

Traditional methods of providing remote access — such as VPNs — create friction, leading to higher costs and lower productivity. They also increase your attack surface, invite malware, and make it impossible to limit and track individual privileged behavior.

To help you overcome these challenges, a new security category called Remote Privileged Access Management (RPAM) eliminates friction and lowers the likelihood of an identity-based attack. Discover how to expand a foundational Privileged Access Management (PAM) strategy to include remote employees, third parties, and acquired companies. Learn how to apply the same granular, policy-based access controls for these remote and M&A scenarios as you do for your in-office staff.

Employees have gone remote and they're not coming back the same way

It's been years since COVID radically changed how people work. Employees are trickling back to the office in fits and starts, but it's unlikely that most organizations will return to a pre-COVID state. The workforce still craves the flexibility, autonomy and work-life balance that remote work offers. If you want to attract top talent, you need to meet the demand for remote or hybrid work arrangements.

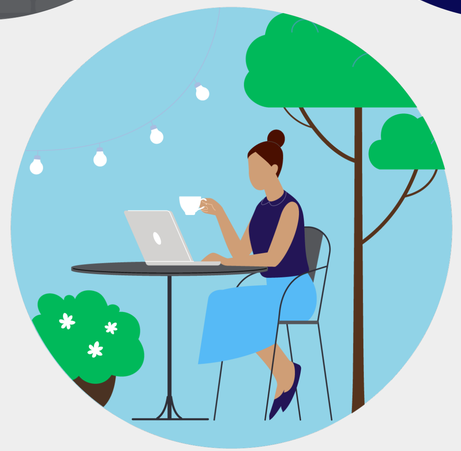
You're most likely to find remote workers in departments like IT, accounting, finance, legal, and human resources.[1] These are the very types of employees that often have privileged access to critical business systems and applications. They need to access sensitive data and execute transactions from wherever they work — whether that's a home office, coffee shop, or airport.

How can friction increase risk?

Most employees aren't technical experts. So, the traditional remote access tools that IT were already familiar and comfortable with can be a struggle for business users. When employees get frustrated and have deadlines to meet, they may find ways to skirt security policies. For example, they could share passwords or ask colleagues to send sensitive data over email so they can accomplish their goals.

1. www.forbes.com/advisor/business/remote-work-statistics

Even if employees are in the office, vendors and contractors will likely be remote



The volume and diversity of work that contractors, vendors, and other third parties handle is exploding, as companies tighten their belts, hiring slows, and employees with specialized technical skills are increasingly difficult to find. Third-party IT support handles troubleshooting, configuration, patches and upgrades, development, testing, and more — all remotely.

In these scenarios, speed of access is essential to meet service level agreements and business expectations. The longer it takes third parties to gain access, the more your business may suffer. For example, if third-party fixes take longer, users and customers can't execute transactions, which impacts your revenue. Let's say third-party developers can't get access to test and production servers. Your next product launch may be late to market.

How can friction increase risk?

While waiting for secure set-up, it's not uncommon for a well-meaning employee to share their own credentials with a third-party vendor. While the vendor can do their work using the employee's credentials, now the security team has lost visibility on what the vendor is doing

Here's a hypothetical, but realistic, situation to illustrate the point:

Imagine a vendor provides a team of people working in shifts so they can provide 24x7 coverage. What if the vendor's team shares a single privileged account? In that case, you wouldn't know which individual has access to your systems at any time. There's no way to monitor individual privileged behavior, and there's no audit log for compliance.

Here's another realistic, hypothetical example:

Oftentimes, a business unit will want to use a vendor again in the future. Unsurprisingly, they won't want to go through the pain and delay of setting up privileges all over again. So, they might leave existing privileges in place without the knowledge of IT. When that happens, standing, excessive privileges become orphaned and unmanaged. The vendor could continue to use their privileges off your radar, share them with others, or store them in a way that invites credential theft.

The speed of integration drives M&A success

Mergers and acquisitions are always a tricky time for security teams. Once the two entities come together, the pressure to get things done fast is at an all-time high. People need to plan and solve problems to demonstrate the new company's value, but they're still using different systems and can't easily collaborate.

In addition to new and unknown employees working from multiple locations, there may also be a cadre of contractors and third-party service providers who need temporary access to sensitive data and systems before a full security review can occur.

In this scenario, security measures can't be rushed. Even if a new entity has been vetted at a high level before the deal is finalized, it doesn't mean that users of the acquired company should be granted access to sensitive information automatically. When it comes to privileged access, you need to consider the acquired company's users as a high-risk third party.

How can friction increase risk?

Relying on the acquired organization's identity source (such as Active Directory) to create user groups and permissions isn't always straightforward. There may be multiple identity directories (IdPs) in place, such as AD, Azure, Okta, or Ping with duplicated identities. Because of this complexity, you can't track the full scope of an individual's privileged access to understand the risk they represent.

For example, let's say a malicious insider isn't a fan of the acquisition and wants to cause harm. Or, worried for their job, an employee starts downloading sensitive data they can take to a new job. Without accurate visibility of remote access, you won't be able to detect and respond to these actions.

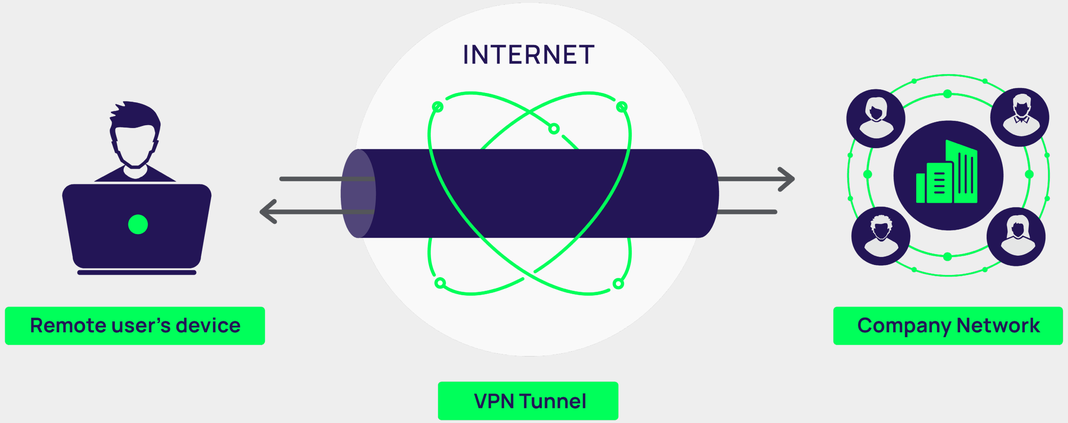
VPNs aren't the answer

If you're like most organizations, you've got a hodgepodge of inconsistent approaches to remote access for employees, contractors, and vendors. As a result, remote access can be a nightmare to use, manage, and secure. Most remote access solutions offer limited auditing with only basic event logs, increasing the chance you'll miss malicious activities.

Many companies are still relying on old-school VPNs to provide access to remote users. Unfortunately, VPNs cause operational headaches as well as security risks. They lack robust authentication, governance, and visibility.

VPNs create a tunnel that sits between the network and a remote user. This tunnel is an open access point in your attack surface. If remote users access that tunnel via untrusted endpoints, they may introduce malware into your environment.

What is a VPN Tunnel?



> 57% of people experienced a cyberattack while using a VPN in 2023"
>
> → Forbes, www.forbes.com/advisor/business/vpn-statistics

Once inside, VPN users have unrestricted access and can move laterally. You have no way of knowing which remote users are operating in your environment and what those individuals are doing once inside. You can't provide consistent reporting to demonstrate proper management of material risk, so you can't comply with compliance or cyber insurance requirements.

Many users find VPNs to be a hassle because of their complicated setup and the lag they can cause. Plus, some partners and vendors won't allow VPNs on endpoints. VPNs need downtime for updating, which causes business disruption.

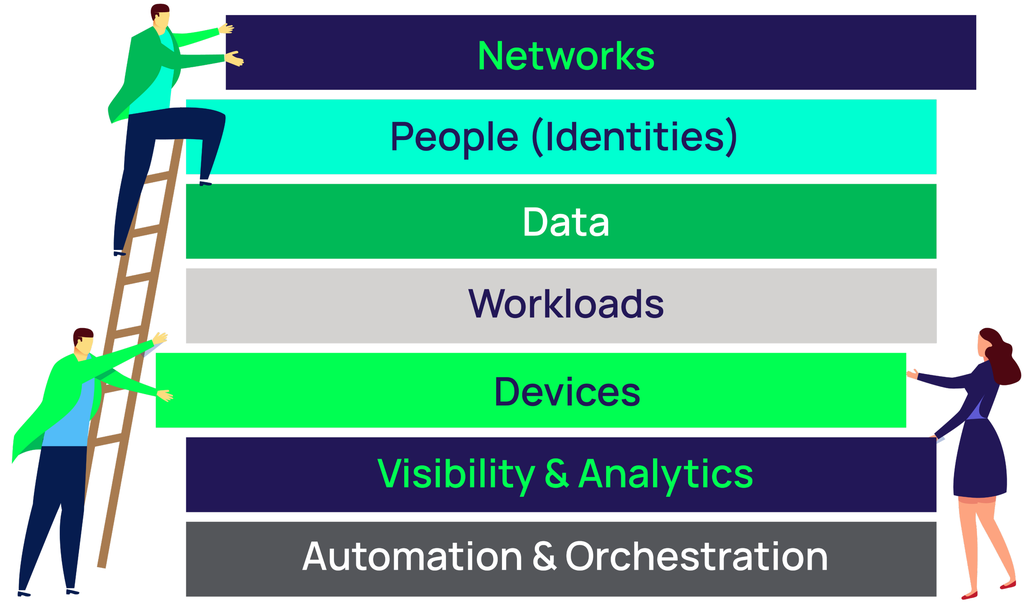
ZTNA addresses the *network* layer, not the *identity* layer

Some companies try to address the risk of remote access through network segmentation. It's a solid approach, but it has some gaps.

Network segmentation isolates segments within your network that contain high-risk resources. Zero Trust Network Access (ZTNA) solutions can be helpful in the network segmentation approach to limit lateral movement across segments.

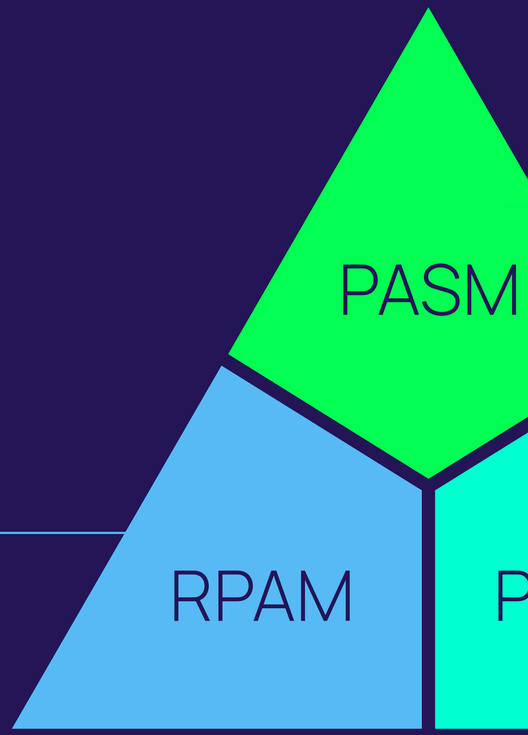
While network segmentation protects the ***network*** layer of your attack surface, it doesn't protect against ***identity-based*** attacks. Should a threat agent steal credentials and impersonate an authorized remote user, they will still be able to gain access and move laterally.

Closing the security gap requires a layered approach to remote access that specifically addresses identity-based threats.



Remote Privileged Access Management is the way forward

According to Gartner, Remote Privileged Access Management (RPAM) has become an essential part of Privileged Access Management, along with Privileged Access and Session Monitoring (PASM), and Privileged Elevation and Delegation Management (PEDM).



PASM

is based on a password vault. It provides privileged account discovery, storage, session management, and recording capabilities. It's required for users whether they are remote or inside the corporate network.

RPAM

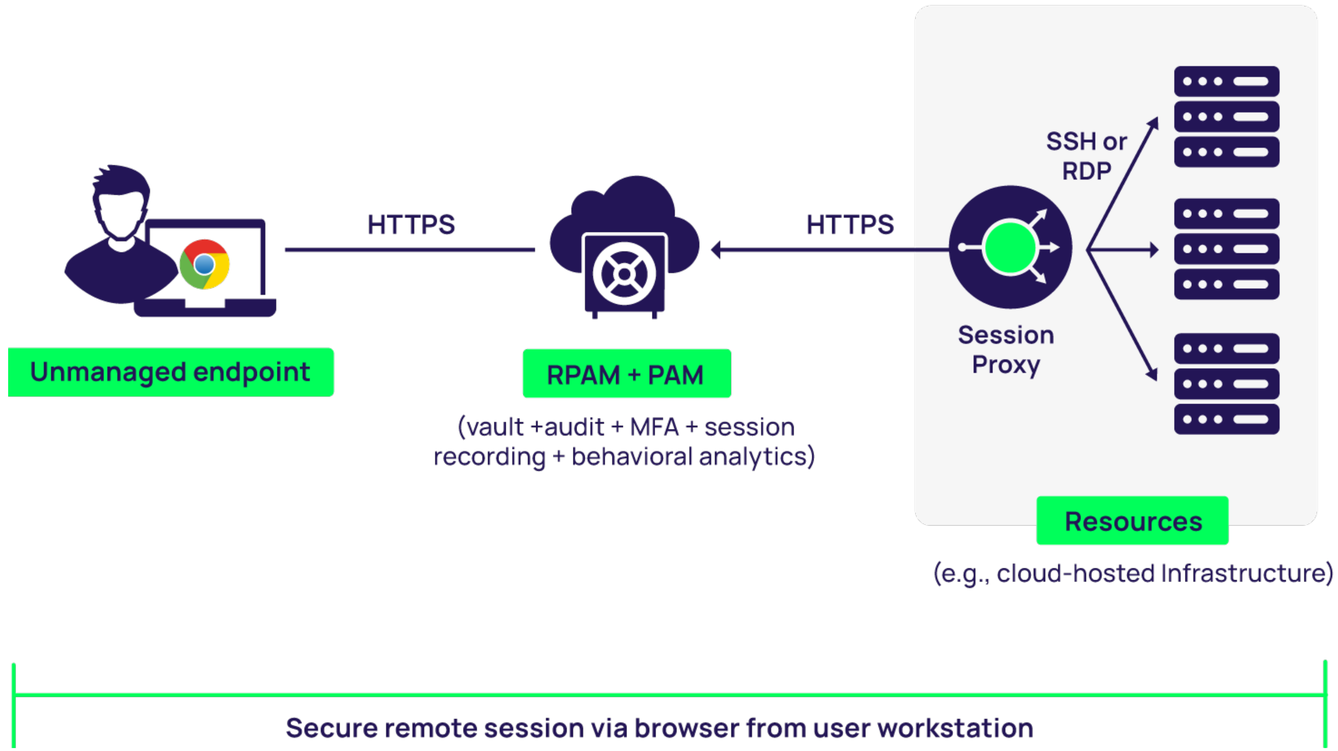
allows granular access to authorized privileged accounts by using PAM gateways that broker access. RPAM solutions register external identities outside of corporate identity stores and enable short-term and time-bound access.

PEDM

helps reduce the risks posed by overprivileged users by providing more specific controls. All users (even domain admins and system admins) operate with standard privileges until they require a higher level of access. Controls on endpoints (servers or workstations) elevate privileges for a limited time, under limited circumstances.

How RPAM works

Simplified Remote Privileged Access Management Architecture



RPAM integrates tightly with PASM for password vaulting and session monitoring.

Instead of requiring you to open ports or install clients on endpoints, RPAM solutions use a browser-based, zero-install approach. A session proxy enables connections to the vault, while providing isolation from the external world.

A remote access engine sits safely inside your network, constantly listening for a legitimate connection request coming from a vault with a trusted relationship; in fact, it's the only thing that engine will listen to.

Once the connection is made, the vault automatically injects passwords into remote sessions. That way, you eliminate the exposure of privileged credentials on the remote endpoint.

Because RPAM solutions are fully integrated into PAM vaults, they offer additional benefits:

- Fine-grained access control of authorized privileged accounts
- Password rotation on a frequent basis
- Session monitoring for continuous visibility, auditing, and reporting
- Multi-factor authentication (MFA), either provided directly by RPAM tool or by third parties

A checklist for remote privileged access

As you expand your strategy for Privileged Access Management to include remote workers and third parties, below are criteria to look for in an RPAM solution:

- Shrinks the attack surface and eliminates the open tunnel, by limiting inbound traffic.
- Easy for remote workers to connect and perform tasks remotely without support from IT teams.
- Establishes trust relationships between different identity providers (e.g., Azure and Okta) through identity federation.
- Adds layers of identity assurance through multi-factor authentication (MFA) at initial log-in and privilege elevation.
- Continuously monitors individual behavior and automatically detects anomalous behavior.
- Automatically applies least privilege principles based on policies, ensuring remote users can only access authorized privileged accounts and systems.
- Simple to demonstrate compliance and insurance requirements with auditing and reporting.
- Uses the same access security and management tools for employees as well as third parties, so you only need to learn one user interface.
- Connects into an integrated identity security solution so that you have consistent access policies, risk posture analysis, contextual alerts, and comprehensive reports.

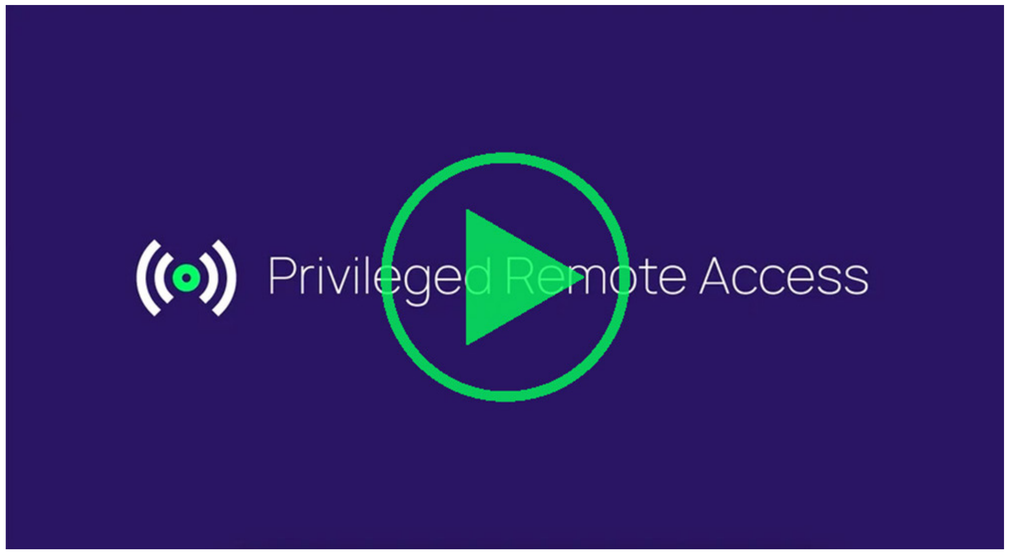
Discover Delinea Privileged Remote Access

Unlike traditional methods of remote access, Delinea's browser-based approach is easy to use and reduces your risk.

Delinea more efficiently enables time-bound access with faster provisioning and deprovisioning of remote sessions with value delivered in as little as three clicks.

By applying context and intelligence to remote access, session monitoring and AI-driven auditing helps improve governance and tracking of user activities.

See for yourself with a free trial of Delinea Privileged Remote Access.



Delinea

Securing identities at every interaction

Delinea is a pioneer in securing identities through centralized authorization, making organizations more secure by seamlessly governing their interactions across the modern enterprise. Delinea allows organizations to apply context and intelligence throughout the identity lifecycle across cloud and traditional infrastructure, data, and SaaS applications to eliminate identity-related threats. With intelligent authorization, Delinea provides the only platform that enables you to discover all identities, assign appropriate access levels, detect irregularities, and immediately respond to identity threats in real-time. Delinea accelerates your teams' adoption by deploying in weeks, not months, and makes them more productive by requiring 90% fewer resources to manage than the nearest competitor. With a guaranteed 99.99% uptime, the Delinea Platform is the most reliable identity security solution available. Learn more about Delinea on **Delinea.com**, **LinkedIn**, **X**, and **YouTube**.