ManageEngine

PAM360

An admin's guide to **secure remote access**

What is secure remote access?

Secure remote access refers to an IT security strategy that allows authorized, controlled access to an enterprise network, mission-critical systems, or any confidential data. It enables IT teams to provide varying levels of access for employees and third parties based on their roles and job duties. Secure remote access methods protect systems and applications, and ensure their continual operational efficiency.

What are the types of secure remote access strategies?

Some notable remote access methods that enable enterprises to secure access to their IT infrastructure include:

- **Virtual private network (VPN):**

VPNs are the most common form of remote access. They use authentication and encryption to establish a secure connection to a private network over the internet.

- **IPsec VPN**

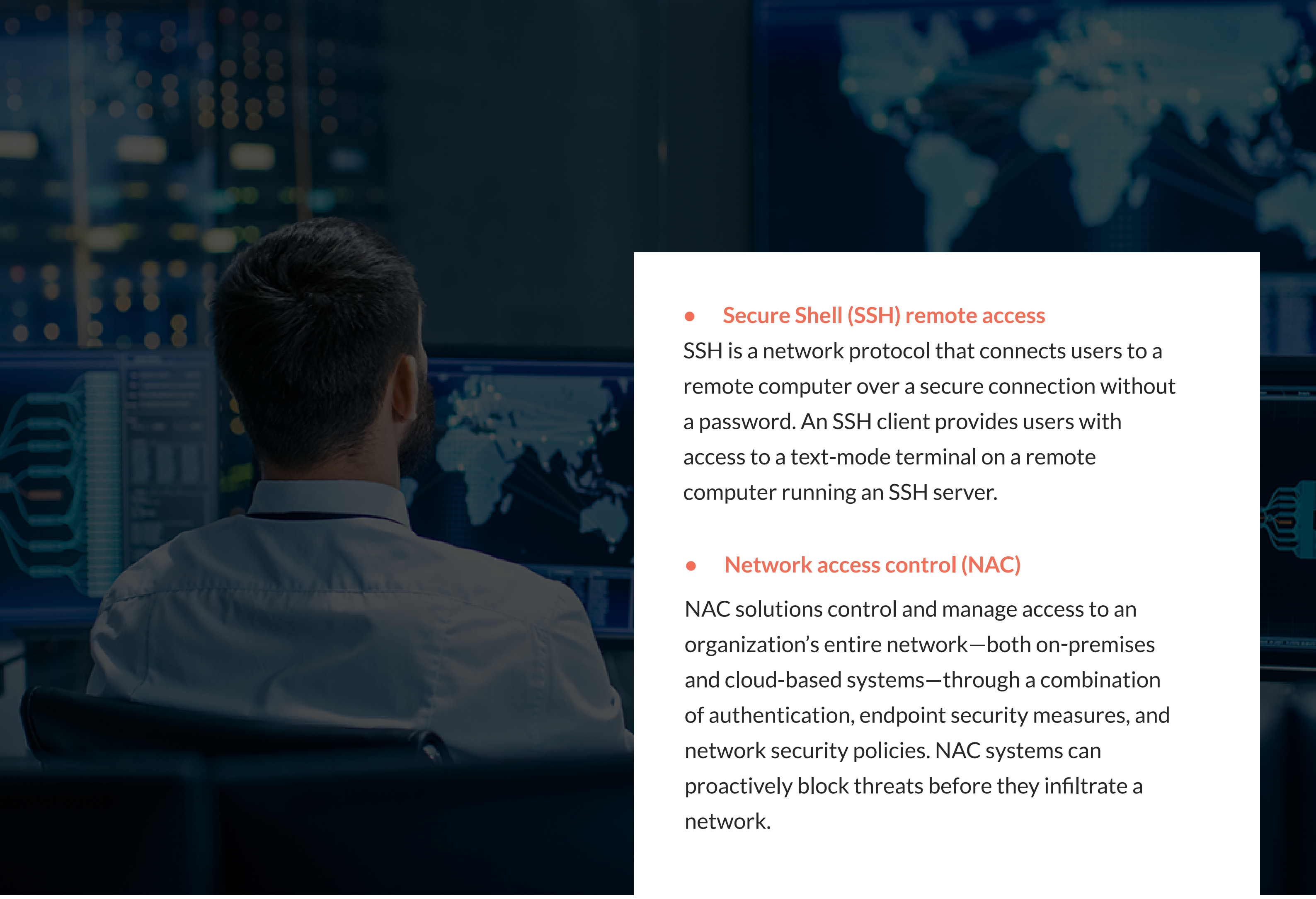
IPsec is a group of networking protocols used for establishing encrypted connections, such as VPNs, across publicly shared networks over the internet.

- **SSL VPN**

SSL VPNs use authentication and encryption technology to create a secure VPN connection with a web browser, enabling remote users to access organizational resources from outside the corporate environment.

- **Desktop sharing**

Desktop or screen sharing is a remote access and collaboration method that shares a particular desktop screen with other devices. This provides a user with complete control over real-time access to the data on another device.



- **Secure Shell (SSH) remote access**

SSH is a network protocol that connects users to a remote computer over a secure connection without a password. An SSH client provides users with access to a text-mode terminal on a remote computer running an SSH server.

- **Network access control (NAC)**

NAC solutions control and manage access to an organization's entire network—both on-premises and cloud-based systems—through a combination of authentication, endpoint security measures, and network security policies. NAC systems can proactively block threats before they infiltrate a network.

- **Single sign-on (SSO)**

SSO is a user authentication approach that authenticates users and gives them access to multiple applications and resources across the IT infrastructure with just one set of login credentials.

- **Context-based remote access**

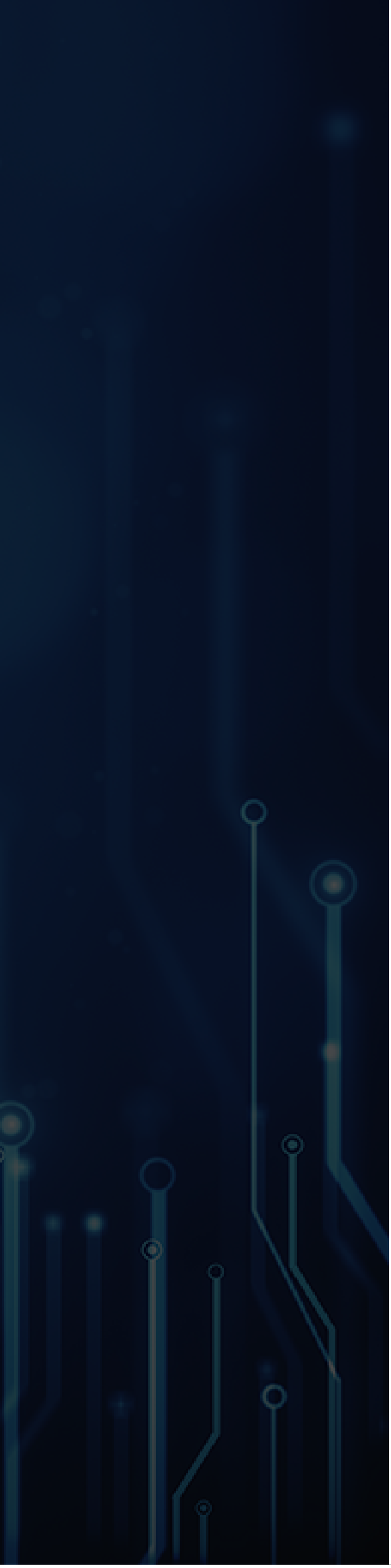
This strategy applies different security controls to different access contexts depending on the various levels of risk. Context-based access control provides great flexibility and granularity, and defines policies based on who accesses what, when, where, why, and for how long.

- **Zero Trust network access (ZTNA)**

ZTNA systems enable secure access to private applications on the network only after proper verification. It's a secure remote access model that doesn't automatically trust users, and provides them with just the right access based on roles, least privileges, and other granular security controls.

- **Privileged access management (PAM)**

PAM is a set of cybersecurity strategies that secure, manage, and monitor privileged access and permissions for users, accounts, applications, systems, and processes across an IT environment.



Why is securing remote access important?

The current remote work trend has impacted many organizations' overall security strategies, and IT admins are now managing confidential enterprise data and accessing sensitive servers from remote locations. Traditional access security methods are no longer sufficient to cater to the growing remote access needs.
Organizations must adopt safeguards to provide employees with secure remote access anytime, from any device and location.

- **Risks from an enterprise's weakest link**

Humans are the weakest link in an enterprise's cybersecurity chain, be it internal disgruntled employees or external cybercriminals masquerading as privileged insiders. Often, employees are provided more access than what's required for their roles. Common work-from-home habits like using corporate devices for personal work, using unmanaged personal devices from a home network to access corporate systems, reusing passwords, or sharing sensitive devices and data with family members put critical enterprise systems at risk.

- **Privileges are strewn across corporate networks**

With the expansion of the Internet of Things (IoT), many systems and applications require privileged access to ensure business continuity. Such non-human entities are harder to manage, and mostly remain undiscovered. Many employees are also granted surplus privileged access to accelerate operations, presenting more
opportunities for attackers to target these accounts and install malware.

- **Endpoints are one of the key targets of cyberattacks**

The rising number of endpoints (computers, laptops, servers, smartphones, etc.) requiring access to corporate networks also substantially broadens the attack surface. Attackers can exploit default admin accounts, steal more credentials, escalate privileges, and move laterally within the network, vandalizing the security chain.

- **Remote access hacks and scams**

Remote working also presents new challenges, notably employees being caught by sophisticated phishing scams and hacking attempts. Cybercriminals leverage weak and vulnerable points in insecure remote access methods and VPNs to wreak havoc.

- **Increased attack surface**

Privileged access spans the entire IT infrastructure—in endpoint devices, the cloud, applications, automation systems, and throughout the DevOps pipeline. Poor security practices and the growing threatscape help cybercriminals exploit the most critical corporate assets.

- **Trouble with VPNs**

Most organizations use VPNs to enable remote access to remote systems outside the corporate network, which allows too much lateral movement. VPNs don't provide granular controls, and using them to facilitate remote administrative access increases the vulnerability to breaches, insider threats, and compromised credential risks.

What are the benefits of adopting secure remote access methods?

Implementing a secure remote access solution as part of their cybersecurity program helps enterprises mitigate security risks, reduce operational complexity, improve visibility into privileged access, and adhere to compliance standards.

- **Provides centralized access to geographically sequestered assets**

From now on, many organizations will continue to embrace a work-from-home-culture and have most of their employees work from various remote locations. Secure remote access allows IT and security heads to have a central point of control to manage critical resources from anywhere across the globe, have granular controls on access pathways, and define how other privileged remote users connect to critical systems.

- **Enables granular access to third parties and external systems**

Secure remote access solutions help provide temporary, role-based access for third parties, like contractors, vendors, and outsourced employees, to access specific enterprise systems or applications without the need for privileged credentials. Sharing only the sufficient data with a third party depending on their roles and job duties can be very beneficial when done correctly.

- **Increases productivity and ease of administration**

Implementing a secure remote access solution facilitates centralized administration of distributed remote IT assets through a single point of control. Privileged users can update, troubleshoot, and manage remote servers centrally, facilitating quick, efficient administration. It also ensures improved quality of work and better accountability through standardized policies and efficient supervision.

- **Tightens overall access governance**

In addition to providing granular access, secure remote access solutions also provide admins with the right controls to monitor and manage geographically distributed assets. Real-time monitoring of privileged remote sessions promotes organizational transparency, and provides IT admins with the ability to proactively mitigate insider attacks.

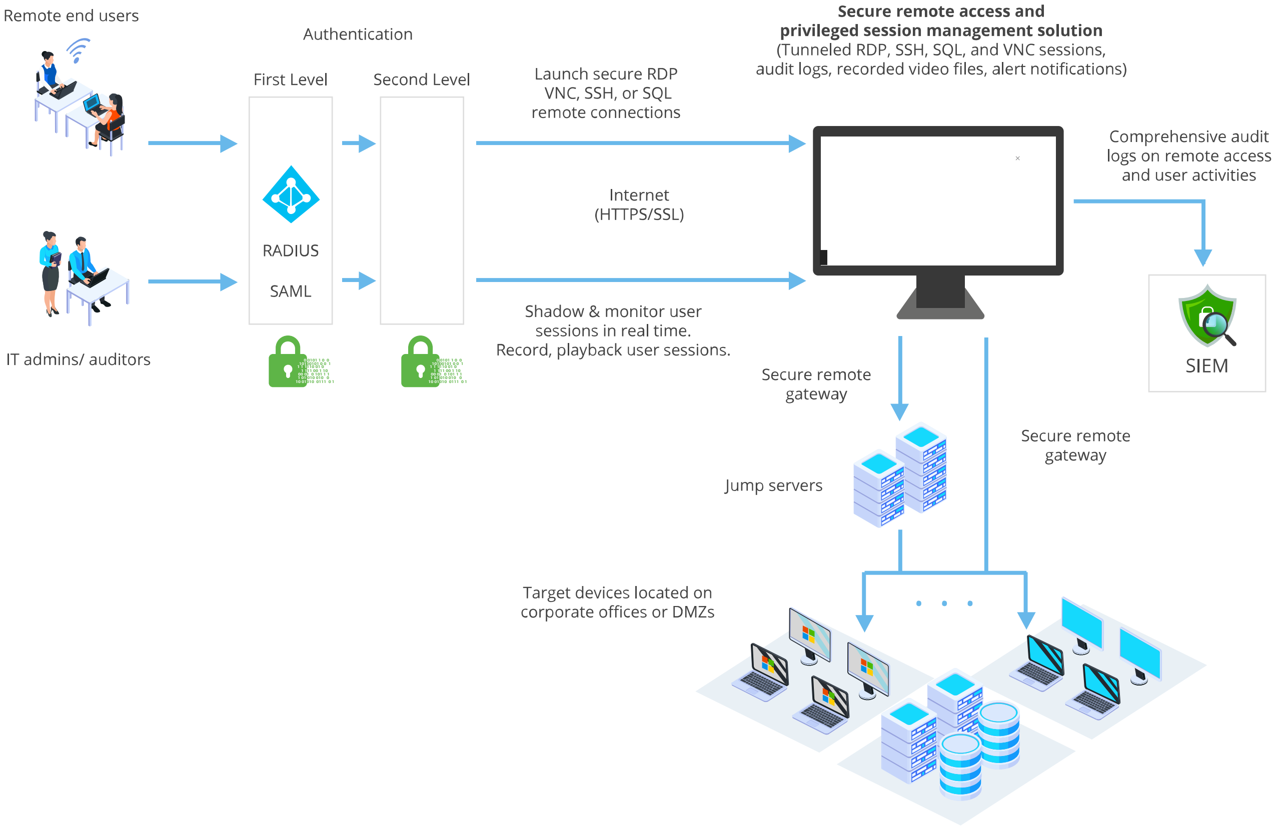
- **Helps comply with various remote access compliance standards**

A secure remote access service meets industry compliance standards, and allows organizations to convince customers who entrust them with keeping their data as secure as possible. Implementing secure remote access as part of a comprehensive cybersecurity strategy enables organizations to record all activities related to critical IT infrastructure and privileged access, helping them effortlessly adhere to audit and compliance requirements.

How does secure remote access work?

A well-designed remote access tool can enable secure connections to target systems and prevent unauthorized access. The following steps define a general secure remote access process, and are applicable for most of the enterprise remote access architectures.

- A remote access session starts with authenticating users or other entities, like systems or applications, through the organization's identity and authentication system.
- Before authorizing a remote session, it's mandatory to define who can access what system, at what time slot, from which device, and what specific actions can be performed.
- Upon successful authentication, the user is granted controlled access to the designated systems in the enterprise network,based on least privileged or role-based access control (RBAC) principles.


Remote end users
Authentication
First Level
Second Level
RADIUS
SAML
IT admins/ auditors
Launch secure RDP VNC, SSH, or SQL remote connections
Internet (HTTPS/SSL)
Shadow & monitor user sessions in real time. Record, playback user sessions.
Secure remote access and privileged session management solution
(Tunneled RDP, SSH, SQL, and VNC sessions, audit logs, recorded video files, alert notifications)
Comprehensive audit logs on remote access and user activities
SIEM
Secure remote gateway
Secure remote gateway
Jump servers
Target devices located on corporate offices or DMZs

- Remote sessions (RDP, SSH, SQL, or VNC) are tunneled through encrypted, secure pathways without the need for supplying credentials.
- All remote sessions are recorded as video files for post session review. The sessions are also monitored in real-time.
- The admin team may block or terminate a suspicious remote session, and the secure remote access tool may generate an alert on anomalous activities.
- The audit logs can also be sent to SIEM systems to achieve better insights into privileged remote sessions.

Best practices for secure remote access

Incorporating best practices and security controls for remote connections is essential, as a lack of remote access security could allow cybercriminals to gain access to privileged systems, resulting in data breaches. An effective secure remote access solution incorporates the necessary tools and best practices to ensure complete cybersecurity and remote access security. Considering the business challenges posed by a remote workforce, it's important to secure remote access by privileged users to critical enterprise systems and infrastructure.

- **Adopt SSO and password management**

Employees and third parties should use SSO access to simplify and centralize the authentication process. Enterprises must also consider a central credential vault that enables IT heads to store, manage, and track the usage of highly sensitive, privileged credentials, and also reset them after a single access instance.

- **Mandate multi-factor authentication (MFA)**

MFA is imperative to authenticate users for secure remote access. Many regulations and compliance standards require MFA for privileged remote access.

- **Implement a Zero Trust security strategy**

Enterprises must not automatically trust users or applications trying to access the internal network. It’s crucial to know who or what is requesting access, why, and from where.

- **Embrace least privilege access policies**

The least privilege policy ensures that employees and third parties are only granted minimum, just-in-time access required to perform their tasks, restricting them from having full access to the entire corporate network for extended periods of time.

- **Apply granular access controls**

Ensure that only authorized privileged users can access and manage remote resources. Establish a set of policies that allow admins to remotely control privileged sessions and mandate remote users to be confined to the authorized activity.

- **Manage endpoint assets**

The finest remote access software must also provide effective endpoint management to protect assets like employee laptops, smartphones, and other IoT devices. It must also help admins monitor remote endpoints, proactively secure all corporate devices, and secure corporate data.

- **Monitor and audit privileged sessions**

Monitor user behavior in real time to mitigate the risk of unauthorized activities. A comprehensive audit trail helps identify vulnerabilities and trace an anomalous session to the root cause. Privileged session monitoring and recording promote organizational transparency and enable IT admins to view and, if necessary, interrupt and terminate a malicious privileged session.

- **Promote employee awareness**

Train your employees and ensure they strictly follow the proposed security standards before connecting to the enterprise network. Conduct regular trainings on the importance of basic cybersecurity policies involving the integrity, confidentiality, accessibility, and availability of critical data, and explain the importance of following them.

Adopting a secure remote access strategy

In the 2020 Market Guide for Zero Trust Network Access report, Gartner states that by 2023, 60 percent of enterprises will replace their VPNs with ZTNA solutions. A robust, secure remote access solution provides centralized protection against access misuse. By fortifying privileged remote access with a Zero Trust, least privilege-based solution, organizations can make intelligent, automated decisions while granting privileged access.

Outdated and traditional remote access security solutions must be replaced with those that meet the modern remote access requirements of launching secure remote access to any system, device, or application, from any location, at any point in time. Secure remote access solutions help enterprises provide users with granular access, and gain visibility into what systems users are connecting to and what actions they perform during entire remote session.

ManageEngine PAM360 enables secure privileged access to remote endpoints and other critical IT systems. The solution's gateway server routes all remote connections through an encrypted channel, protecting enterprise networks from malware and cybercrime. Through robust authentication, granular access controls, and session management capabilities, PAM360 minimizes deliberate and unintentional access misuse risks while also letting enterprises choose and design a utilitarian remote access strategy.

Learn more about ManageEngine PAM360
and enterprise secure remote access from our experts.

Register for a free, online demo

https://www.manageengine.com/pam360

Contact us

Email: pam360-support@manageengine.com
Phone: +1-925-924-9500

ManageEngine
PAM360