Delinea

Secure Remote Privileged Access for Your Workforce

Empower people to stay productive and secure

Privileged Access Management ensures remote users can access systems and data they need while adhering to cybersecurity best practices.

1 Recognize that security now depends on the device and human using it

There is no traditional security perimeter when employees are working remotely. Security now resides with the endpoint and the user.

2 Verify and secure privileged access with MFA and PAM

Multi-Factor Authentication in conjunction with Privileged Access Management is the only way you can adopt a Zero-Trust policy enforcement.

3 Allow administrative access from anywhere

Make sure privileged credentials for your most sensitive applications, databases, root accounts and other systems are secured in a central vault and accessible to trusted administrators no matter where they work.

4 Accelerate the ability of your IT teams to use secure remote sessions

Provide IT teams with automated tools to navigate different connection protocols, such as RDP and SSH, inject credentials, and interact with privileged sessions from start to finish.

5 Maintain auditability and visibility for shared privilege access

Delegate access so users don't need to remember or share passwords. Automate generating complex passwords, rotating them periodically, and using proxies to connect systems.

6 Make sure every user's location and workspace is secure

Every user should be aware of working in an area that's secure, private. And free from any listening devices.

7 Implement a least privilege policy to prevent access

Removing local admin rights from all users workstations will limit the spread of any cyberattack. Implement approval lists, deny lists, and sandbox policies to block applications from downloading and executing.

8 Ensure accountability of remote IT staff, contractors and third parties

Session management controls such as workflow approval, dual control, keystroke logging, and session recording add an extra layer of control and audibility.

9 Know the signs of privileged account abuse from remote workers

Remote user privilege account behavior monitoring can trigger alerts and encourage additional protections, such as rotating passwords, enhanced security controls. And additional approvals for access.

10 Update your incident response and business continuity plans

Make sure your incident response and back-up plans are revised to reflect the new reality of remote workers and how they respond to incidents.