Remediant

SOLUTION BRIEF

Remediant PAM+™

The Transformation of Privilege Access Management.

Cyberattacks are successful today because attackers use compromised admin credentials to gain privileged access and can steal administrator credentials once they get a toehold on an enterprise system. With elevated privileges, attackers are free to move from system to system due to the implicit trust conferred to already verified privileged access. This enables compromise without detection of additional administrator accounts and allows the attacker unfettered access to an organizations most valuable data and IP.

Digital transformation is causing even more privilege sprawl as cloud workloads, SaaS applications, Dev Ops, and multi-cloud instances require administrative access. This results in a massive increase in the privileged identity attack surface. Ransomware and other advanced malware attacks are successful today despite large investments in network, endpoint and PAM solutions. This is mainly because organizations have overlooked privilege sprawl, or more likely, do not realize that the privilege sprawl can, in fact, be eliminated.

According to the 2022 Gartner® Magic Quadrant for Privileged Access Management, JIT PAM 'capabilities provide on-demand privileged access without the requirement of shared accounts carrying standing privileges. Typically, this involves nonprivileged accounts being granted appropriate privileges on a time-bound basis. Common methods for achieving this can be use of PEDM approaches, use of temporary and on-demand group membership, or the use of ephemeral accounts or security tokens. This capability is focused on compliance with the principle of least privilege and subsequently achieving zero standing privileges (ZSPs) for PAM access. JIT use cases include:

- *The ability to dynamically add and remove users from AD groups*
- *Dynamically provide time-limited access to privileged accounts*
- *PEDM functionality through on-demand privilege elevation*
- *The ability for on-demand creation and deletion of privileged accounts*
- *The ability to create and use ephemeral tokens*
- *The ability for on-demand access to SaaS control panels such as AWS*

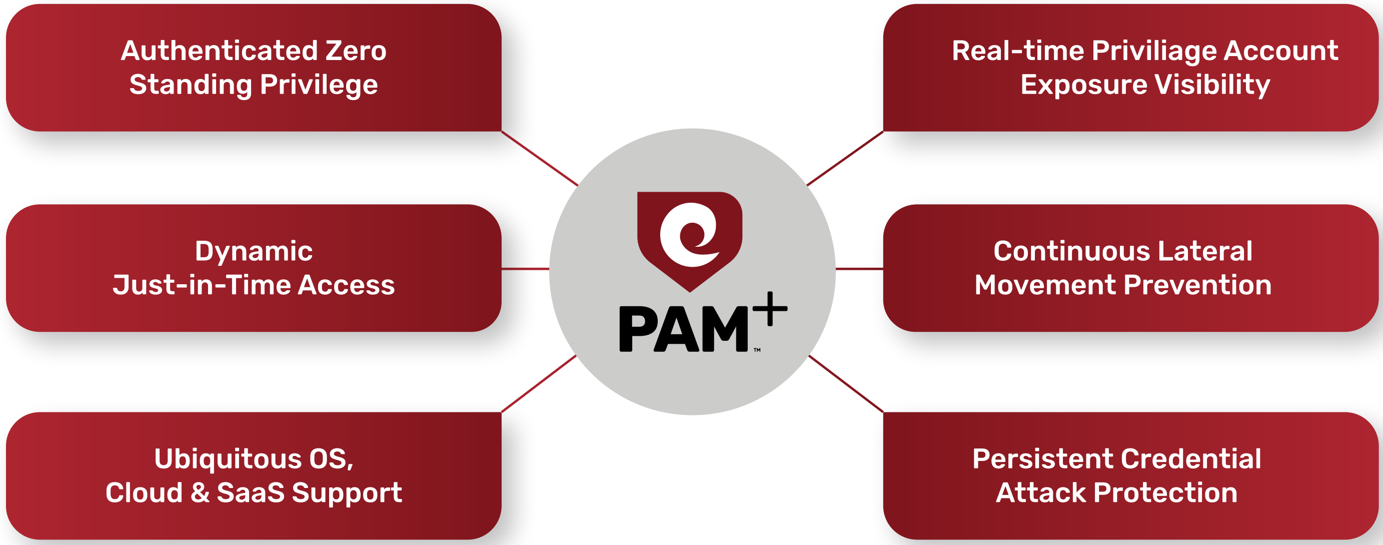
Gartner.

INTRODUCING PAM+

Remediant PAM+™ meets the needs of large and small enterprises struggling to achieve real-time privilege account exposure visibility, prevent lateral movement attacks, and establish persistent protection against attacks utilizing stolen credentials.

PAM+ delivers immediate value above and beyond legacy PAM toolsets including:

- Reduce Privilege Identity Attack Surface
- Eliminate Admin Credential Compromise
- Render Password Stealing Malware Ineffective
- Stop Lateral Movement
- Enable and enforce Just-in-Time Access
- Bolster access with MFA
- Reduce 90% of Admin Processes


Authenticated Zero Standing Privilege
Real-time Priviliage Account Exposure Visibility
Dynamic Just-in-Time Access
PAM+™
Continuous Lateral Movement Prevention
Ubiquitous OS, Cloud & SaaS Support
Persistent Credential Attack Protection

HOW PAM+ WORKS

Remediant PAM+™ gives IT administrators and security analysts dynamic and continuous visibility into their organizations permanently provisioned privileged accounts and the ability to them with a single click. Users then self-administer privilege access, getting access to only the right resource, at the right moment and for the length of time they need to complete their job. This approach eliminates standing privileges, effectively preventing lateral movement attacks and significantly reducing an organization's attack surface.

Remediant's PAM+ is defined by five unique and differentiated capabilities including:

1. Zero Standing Privilege (ZSP) for all Endpoints: This capability removes administrative accounts from all endpoints, effectively eliminating privilege sprawl by removing 24x7 admin access and reducing privileged identity attack surface to zero. By virtue of ZSP, implicit trust to privileged users between endpoints is also eliminated thus preventing lateral movement.

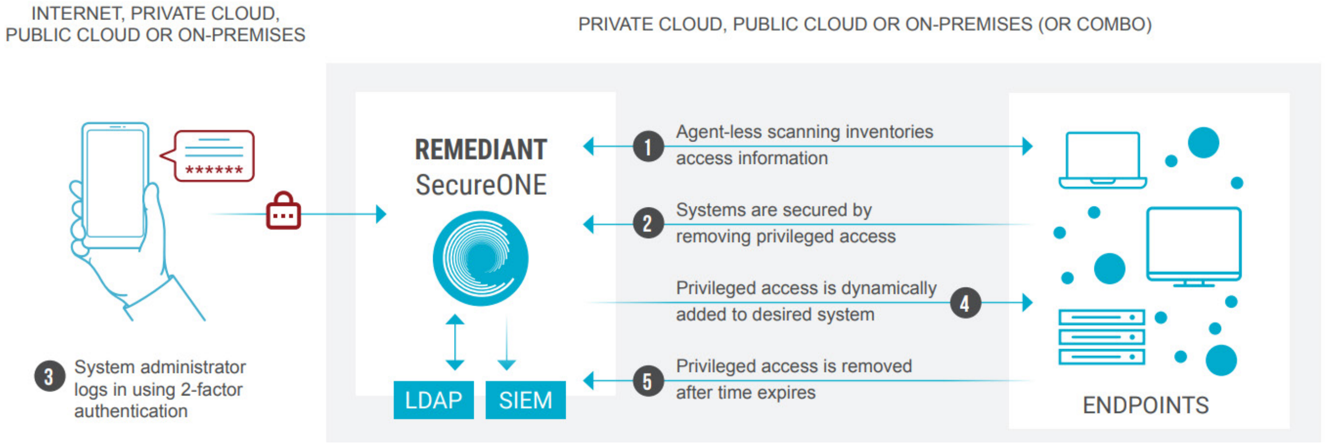
2. Just-in-Time Access (JITA): Privileged users are granted Just-in-Time Access to specific endpoints that require administration in real-time, for only the amount of time needed to complete their task, after which access is de-commissioned or the administrator indicates access can be terminated.

3. No New Credentials: PAM+ does not require the creation of new credentials or a change in how credentials are managed. The administrator can use his/her standard network credentials for just-in-time access which is validated by the directory service. Credentials can be checked out of a password vault.

4. Multi-factor Authorization: PAM+ is a single control point for all JITA, making it simple and straightforward to power the adoption of JITA with MFA to ensure every administrator access is processed via additional authentication factors prior to access being granted.

5. Ubiquitous Endpoint Coverage: Only PAM+ includes coverage of privilege accounts of all types including Windows, Linux and Mac administrative accounts as well as privileged service accounts, network devices, cloud workloads, SaaS applications, and remote endpoints (WFH coverage).

6. Rapid Time-to-Value: A key tenet of PAM+ is to deliver value quickly and effectively: rapid deployment, seamless integration into existing IT and DevOps workflows, ease of adoption and low TCO are the critical success factors of PAM+.


INTERNET, PRIVATE CLOUD, PUBLIC CLOUD OR ON-PREMISES
PRIVATE CLOUD, PUBLIC CLOUD OR ON-PREMISES (OR COMBO)
******
REMEDIANT SecureONE
LDAP
SIEM
1 Agent-less scanning inventories access information
2 Systems are secured by removing privileged access
3 System administrator logs in using 2-factor authentication
4 Privileged access is dynamically added to desired system
5 Privileged access is removed after time expires
ENDPOINTS

Visit **remediant.com** to learn more or click the REQUEST A DEMO button and try SecureONE today!

Remediant, Inc.
Two Embarcadero Center, 8th Floor
San Francisco, CA, 94111

info@remediant.com
www.remediant.com
(888) 418-3911

Remediant