Remediant

REMEDIANT SECUREONE

STOP LATERAL MOVEMENT ATTACKS BY PROVIDING THE RIGHT JUST-IN-TIME (JIT) ADMIN ACCESS WITH MFA

With rapid innovation comes the rapid scaling and adoption of infrastructure. To fuel this innovation, the number of privileged users (on-call developers, admins, SREs) is growing and evolving constantly. With this growth in new technologies, and privileged users to support them, comes new threats. It is, therefore, no surprise that 74% of breached organizations admitted the breach involved access to a privileged account*.

THE PROBLEM: PREVALENCE OF UNDETECTED 24X7 PRIVILEGED ACCESS SPRAWL

Undiscovered, always changing privileges: Today, there is no automated way for organizations to discover and inventory all the privileged access across the enterprise. Traditional privileged access management (PAM) vendors with vaults only protect known privilege, and have no visibility into the sprawl of 24x7x365 administrator privilege across an enterprise.

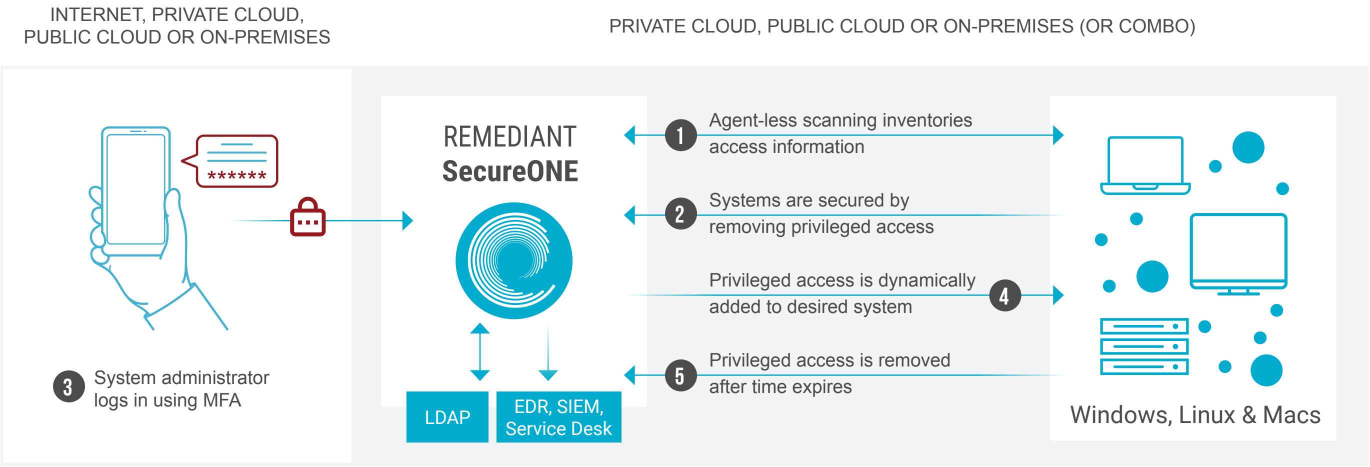
Unnecessary standing access = Larger attack surface: Standing privileged user access without business justification allows hackers to move laterally and spread identity-based threats such as ransomware across a network. It is imperative to remove these standing privileged accounts across Windows, Linux and Mac systems and replace them with appropriate access directly to user accounts just for the time needed.

High friction user experience for administrators: Administrators managed through a password vault have to checkout a generic or shared ID and get approval every time there is an incident. This approach slows down their ability to respond quickly, thereby increasing Mean Time To Respond (MTTR) and impacting uptime.

Incomplete, inaccurate view of risk posture: The number of privileged accounts across the enterprise is a key indicator of an organization's overall risk posture. Today, there is no way to comprehensively report on this risk across an enterprise, nor there is a way to report on how the risk posture has evolved over time.

REMEDIANT SECUREONE: STOP LATERAL MOVEMENT ATTACKS BY PROVIDING THE RIGHT JUST-IN-TIME (JIT) ADMIN ACCESS WITH MFA

Remediant SecureONE was purpose built to address this problem and be a force multiplier to Identity and Access Management (IAM) and traditional PAM programs worldwide. Specifically, SecureONE was developed to (1) Rapidly deploy, scan and inventory Windows, Linux and Mac privileged access with no agent, (2) Continuously monitor, (3) Remove standing access enterprise-wide with a single action, and (4) Administer privileges Just-In-Time (JIT) and MFA to enable Zero Standing Privilege (ZSP) and implement Zero Trust security..



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

* 2020 Verizon Data Breach Investigations Report

HOW IT WORKS: THE ENTERPRISE-READY ZERO-STANDING PRIVILEGE MODEL

The SecureONE platform leverages the power of Remediant's patented enterprise-wide Zero-Standing Privilege (ZSP) model to deliver the following key capabilities:

Agent-less, single virtual appliance deployment: Deployment requires no agents on endpoints. The SecureONE management console can be set up as a single virtual or physical appliance.

Dynamic Visibility: SecureONE constantly scans for and discovers privileged access across the infrastructure, acting as a single source of truth for reporting the distribution of privileged access (150,000 endpoints in approximately 2-3 hours).

Single-action Access Reduction: Users may be removed from administrator groups across all endpoints with a single click. Enabling this takes milliseconds per endpoint with no additional software.

Just-In-Time Administration and MFA and no shared accounts: Privileged access is elevated instantly upon request using the user's own credentials. MFA is used to authenticate the request and access is removed after a pre-determined amount of time.

Privileged Access Risk dashboards: Executives and security practitioners can graphically review the current state of privileged access risk and decide how to reduce this risk or attack surface over a period of time using three dashboards:

1. Privileged Users Access dashboard: Provides a graph of instances of privileged users based on group access and direct access over a period of time. This enables organizations to view and start reducing privileged access at the riskiest groups.
2. Segregation Access dashboard: Enables executives to view privileged access across tiers by domain, servers and workstations . This enables organizations to view the riskiest groups and start reducing the attack surface and stop lateral movement attacks.
3. Cumulative Access dashboard: provides total instances of privileged users based on the combination of workstations and servers at any point in time. Organizations can also obtain the average privileged access/per system.

Technology Ecosystem Integrations: SecureONE integrates with technology partners such as SIEMs (Splunk), EDRs (SentinelOne, CrowdStrike and VMware Carbon Black), Service Desk (ServiceNow), Asset Management (Axonius), and PAM policy monitoring and enforcement (SailPoint) to provide real-time context into all privilege escalations.

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

KEY BENEFITS

1. Prevent lateral movement of compromised privileged accounts early to stop attackers from spreading identity-based threats such as ransomware and phishing
2. Reduce the attack surface by removing 24X7 admin access sprawl and replacing with JIT administration to ensure Zero Standing Privilege (ZSP)
3. Simplify deployment and management. Remediant SecureONE is agentless. This architectural approach dramatically reduces the complexity of employing yet another agent and simplifies support and management
4. Enable Zero Trust security with MFA to provide the right access to the right resources for just the right amount of time
5. Enhance the value of our technology partners and improve the security risk posture of organizations by providing PAM context
6. Complement and secure traditional PAM implementations by removing undetected 24x7 admin access sprawl that exist outside the vault

> *"It's rare to find a simple solution that simultaneously improves compliance, operations, and security. Granting full administrator rights, Just-In-Time, to individual systems, improves administrator support coverage while drastically limiting lateral movement risk."*
>
> **CHAD ANDERSON** | CYBER MITIGATIONS ARCHITECT, LOCKHEED MARTIN

Remediant
Two Embarcadero Center, 8th Floor
San Francisco, CA 94111
(415) 854-8771

Remediant leads with innovation, delivering enterprise-class cybersecurity solutions that enable real-time monitoring, zero trust protection of privileged accounts and Just-In-Time Administration (JITA) across IT/Security ecosystems. We protect organizations from stolen credentials being used to take their data, which is the #1 attack vector across all breaches.