Remediant

REMEDIANT SECURE**ONE** FOR GOVERNMENT

MISSION READY ZERO-STANDING PRIVILEGE: THE RIGHT ACCESS AT THE RIGHT TIME, ACROSS EVERY WORKLOAD

THE PROBLEM: PREVALENCE OF UNDETECTED & STANDING PRIVILEGED ACCESS

Privileged access is still the "weak underbelly" for nation state adversaries and malicious insiders

74% of breached organizations admit involvement of a privileged account

480 Average number of admins with 24x7 access to each workstation[1]

$3.92M the average cost of a data breach in 2019

[1] For organizations with 15,000+ endpoints

Strategic Imperative: "Agencies shall implement processes to manage access control, including the ability to revoke access privileges, when no longer authorized" - OMB Memorandum 19-17

WHY IT HAPPENS

Undiscovered, always changing privileges
Unclear where admin access exists; groups / GPOs change; vaults easy to circumvent

Unnecessary standing privilege = larger attack surface
Admins and Helpdesk have 24x7x365 access

Focus on credentials, not access
Legacy PAM solutions focused exclusively on credentials, but once stolen, rendered useless

High friction user experience for admins
Have to check out a generic ID and get approval slowing down their ability to respond

Agent-based deployment
An agent on each endpoint

REMEDIANT SECUREONE — HOW IT WORKS

Remediant SecureONE was purpose built to address this problem and be a force multiplier to Identity & Access Management programs worldwide. The founding team especially had in mind those looking to secure and enable access to global, distributed and always scaling infrastructure. Specifically, SecureONE was developed to (1) Rapidly deploy and inventory with no agent, (2) Continuously monitor, (3) Remove standing access enterprise-wide with a single action, and (4) Administer privileges Just-In-Time with no shared accounts.

KEY BENEFITS

Integrate – *Faster time to value*

- Agentless, vaultless deployment
- 150K+ endpoints rolled-out in days
- Enterprise-wide coverage
- Force multiplier to other IAM, PAM investments
- Integrates into existing workflows (e.g., ServiceNow)

Protect – *Better coverage, faster remediation*

- One-click attack surface reduction
- Instant discovery of privileged access
- Always-on monitoring

Use – *Frictionless privileged user experience*

- 1 FTE to manage 150K endpoints
- Admins use their own accounts

Report – *Comprehensive, continuous*

- CMMC, NIST aligned
- Always updating, historical trend view

KEY FEATURES

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

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

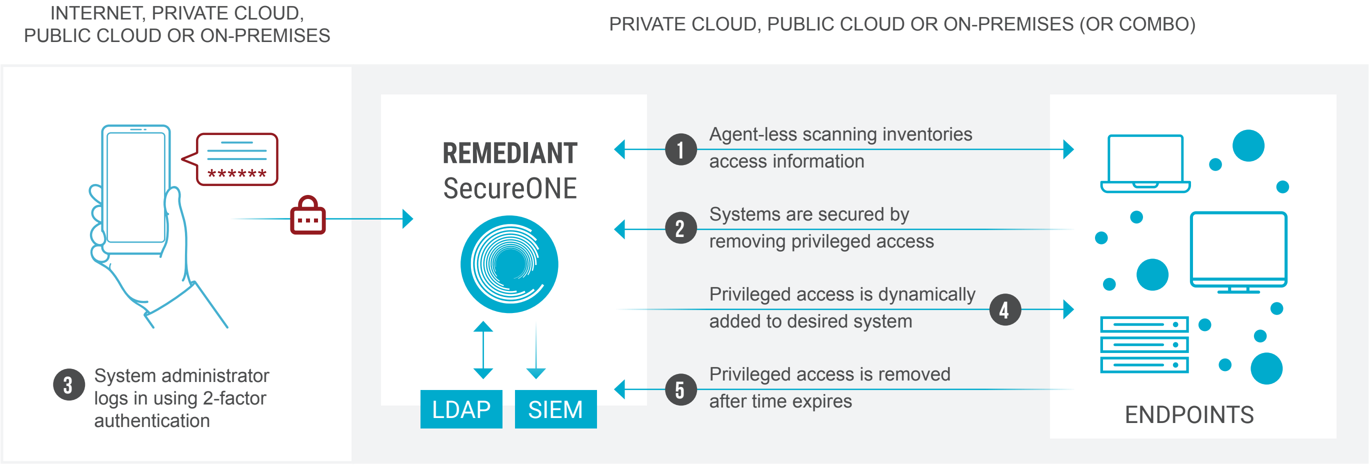
Continuous Inventory & Visibility: SecureONE constantly scans for and discovers privileged access across the ecosystem, acting as a single source of truth for reporting the distribution of privileged access (150,000 endpoints in approximately 2-3 hours).

Just-In-Time Administration with 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.

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

Real-time SOC Insights: SecureONE integrates with Splunk and other SIEMs to ensure real-time visibility into all privilege escalations.

HOW IT WORKS



INTERNET, PRIVATE CLOUD, PUBLIC CLOUD OR ON-PREMISES

PRIVATE CLOUD, PUBLIC CLOUD OR ON-PREMISES (OR COMBO)

REMEDIANT SecureONE

LDAP

SIEM

ENDPOINTS

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

USE CASES

Privileged Access Discovery & Control
Mitigate the risk associated with contractors, inside threats

Adversary Containment
Quick lock-down of endpoints to stop ransomware spread

Cloud & DevOps Privileged Access
Enforce privileged access controls on public, private, hybrid cloud and integrate into DevOps

Regulatory / Policy Compliance
Align with CMMC, SP 800-53 revision 5, 800-171, DFARs supplement

HOW TO GET STARTED

Visit ***remediant.com*** to learn more or click the ***REQUEST A DEMO*** button and try SecureONE today. How to work with us: NAICS Codes: 511210, 541511, 541512, 541519, ; Programs: SBIR Phase 1 (AFWERX)

Security & Compliance: NIST SP 800-171 compliant today. Assessed for NIST 800-171 and 800-53 product applicability by TAG Cyber

CASE STUDY: LOCKHEED MARTIN

Challenge: Cyber DFARS Program Office sought a highly-scalable solution that coupled multi-factor authentication (MFA) and dynamic privileged access, and could meet compliance requirements (NIST SP 800-171) while minimizing impact to operations.

Solution with Remediant: Meets NIST SP 800-171 with significantly enhanced operational security

1 FTE to manage **150,000 endpoints** and **4 hours** to deploy & scan.

"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

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.