Remediant

Success Story

Security Without Compromise

Remediant Helps Lockheed Martin Achieve Instrumented Compliance for Privileged Access

LOCKHEED MARTIN

BACKGROUND

In response to an ever-increasing number of data breaches involving government data, the Department of Defense (DoD) mandated, effective December 31, 2017, the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, which levies far-reaching security requirements on all defense contractors and their subcontractors who store, process or transmit "covered defense information" (CDI) on a DoD contract.

The clause requires, among other components, compliance to 110 security controls defined in NIST Special Publication 800-171, with emphasis on network access and administrator privileges. In late 2016 industry giant Lockheed Martin established a Cyber DFARS Program Office to instrument enterprise-wide solutions.

CHALLENGE

Lockheed Martin needed a highly-scalable solution that coupled multi-factor authentication (MFA) and dynamic privileged access, and could meet compliance requirements while also minimizing impact to ongoing operations. The team started by evaluating a broad selection of legacy password vault solutions, as this mature technology was already in use across parts of the company.

It was determined that legacy password vault solutions could not meet the requirement for dynamic privileged access, and that the Remediant solution would be easier to deploy, more secure and able to continuously inventory the distribution of privileged access across Lockheed Martin's systems. Lockheed Martin considered in-house resources to design and develop a Privileged Access Management (PAM) solution. However, internal development would be an expensive and time-consuming process that would distract from other security priorities in the near-term and build in an ongoing cost to the department.

"When seeking a PAM solution that could meet our requirements, ease of integration, reliability and scale were all critical, and we couldn't afford to compromise in any of those areas," said Mike Gordon, Deputy Chief Information Security Officer, Lockheed Martin. "We needed a solution that the information security marketplace simply didn't offer at the time."

While the option of in-house development remained on the table, Lockheed Martin's Corporate Information Security team continued to look for an innovative partner that approached the problem from a new angle.

> ***"When seeking a PAM solution that could meet our requirements, ease of integration, reliability and scale were all critical, and we couldn't afford to compromise in any of those areas. We needed a solution that the information security marketplace simply didn't offer at the time."***
>
> **Mike Gordon**
> **Deputy Chief Information Security Officer**
> **Lockheed Martin**

> *“In the defense industry, compliance is necessary but, alone, is far from sufficient — we also sought to increase the security around our privileged access. SecureONE brings tight control of privileged access throughout our ecosystem. One of the key steps in the Lockheed Martin Cyber Kill Chain® is to exploit weaknesses in the privileged access protections on endpoints. SecureONE eliminates the potential for lateral movement by attackers seeking to obtain sensitive information.”*
>
> Chad Anderson, Cyber Mitigations Architect, Lockheed Martin

SOLUTION

Working in various information security-related roles in biotech and security consulting led Remediant’s founders to the same conclusion: it was time to forge a new path in the world of privileged access.

SecureONE is based upon three main principles:

1. Utilize the user’s own account for privileged access - not a generic or shared account which creates audit/traceability and compliance challenges.
2. Make the tool extremely easy to use, including a responsively-designed web interface and API-first architecture that is easy for administrators, DevSecOps, operations and information security teams to manage.
3. Continuously scan for changes in privileged access across the enterprise, bringing a new level of insight and control over privileged access.

Stopping lateral movement calls for being careful about how privileged access is allocated. SecureONE takes a fully dynamic approach, assigning privileged access solely to the endpoints the administrator needs, and only for a specific time period. Even if administrator usernames or passwords are stolen, the zero-privilege baseline for protected endpoints ensures that compromised accounts cannot be used to access systems, nor move laterally through the network.

During a security conference in Las Vegas, Lockheed Martin had their first glimpse of SecureONE, Remediant’s solution for managing privileged access. Impressed with what they saw, Lockheed Martin immediately requested a Proof of Concept deployment to test the solution’s features and scalability.

“In the defense industry, compliance is necessary but, alone, is far from sufficient — we also sought to increase the security around our privileged access” said Chad Anderson, Cyber Mitigations Architect, Lockheed Martin. “SecureONE brings tight control of privileged access throughout our ecosystem. One of the key steps in the Lockheed Martin Cyber Kill Chain® is to exploit weaknesses in the privileged access protections on endpoints. SecureONE eliminates the potential for lateral movement by attackers seeking to obtain sensitive information.”

Administrators need privileged access to perform, which makes them prime targets for attackers. To combat this, SecureONE offers security while enhancing workflow. Capabilities include:

Unauthorized access is blocked

- Blocks lateral movement even if administrator usernames and passwords are compromised.

Legitimate access is easy

- MFA-authenticated user-friendly and secure access for users of privileged access.

Insight Dashboard

- Continuous inventorying of privileged access changes brings real-time visibility.

Tool Integration

- Integrates with existing investments in SIEM, IGA, IDM and Active Directory tools.

Remediant

www.remediant.com

> *“Remediant worked an aggressive timeline and a full-lifecycle implementation across the global enterprise to provide added security for our desktop administrators. We call it ‘Instrumented Compliance’, which means not only being compliant but, more importantly, being able to continue to assure our customers and employees that we are protecting their critical data.”*
>
> Joel Johnson, Cyber DFARS Program Manager, Lockheed Martin

RESULT

Compliance does not equal security, but solutions that clearly demonstrate improved security and compliance are surprisingly difficult to find. By making it easy to protect privileged access with MFA and continuously detecting any unauthorized privileged access, SecureONE accomplishes both.

In a matter of weeks, Remediant provided a dynamic, scalable PAM solution with minimal disruptions to Lockheed Martin’s 150,000+ endpoints. Today, Lockheed Martin meets its NIST SP 800-171 requirements while significantly enhancing operational security.

“Remediant worked an aggressive timeline and a full-lifecycle implementation across the global enterprise to provide added security for our desktop administrators. We call it ‘Instrumented Compliance’, which means not only being compliant but, more importantly, being able to continue to assure our customers and employees that we are protecting their critical data,” said Joel Johnson, Cyber DFARS Program Manager, Lockheed Martin.

Today, SecureONE provides just-in-time administrator rights across the Lockheed Martin ecosystem, in countries around the world.

Contact (415) 745-9237 or email success@remediant.com to find out how Remediant can protect your ecosystem.

Click here to request a secureone demo.

About Remediant

Founded in the heart of San Francisco, meets complex security challenges that require a complete understanding of regulatory and government standards. We deliver unparalleled, innovative solutions that holistically balance policy, technology, and usability. Our motivation is to provide next-generation technology and services to secure data for corporations and government entities who must meet regulatory compliance and stop lateral movement in their ecosystems.

Remediant

www.remediant.com