tenable network security

SAI Global

Implements Tenable SecurityCenter™ to Continuously Assesses Vulnerabilities and Contains Security Risks

SAI GLOBAL

Overview

SAI Global Limited (ASX: SAI) is an Australian information services company that helps organizations worldwide manage risk, achieve compliance and drive business improvement through its information services, compliance and assurance divisions. Based on market capitalization, SAI Global is the 10th largest business-services company listed on the Australian Stock Exchange.

Key Business Needs: IT operations for all three SAI Global business units are run by a centralized team and delivered through a shared-services model. The organization places a significant emphasis on security, and facing rising threats from global cyber-crime and risks associated with handling critical information, determined it needed to implement a process of continuous risk and compliance management.

Tenable Products Selected: With the expertise of Tenable partner Content Security, SAI Global implemented SecurityCenter Continuous View, Tenable's enterprise platform that combines the Nessus® Vulnerability Scanner, PVS (Passive Vulnerability Scanner), and SecurityCenter management console.

Top Benefits: Overall risk reduction has been achieved, with faster incident response times and greater levels of productivity from the security team.

Business Needs

Continuously Assess Vulnerabilities and Contain Security Risks

Evaluating opportunities for enhancing the organization's overall security posture, SAI Global's GM for IT, Peter Macarthur-King, noted significant limitations stemming from patch management. Specifically, there was no way of determining whether stats received from the patch management system were accurate and risks associated with vulnerabilities were actually being mitigated. To address these shortcomings, Macarthur-King's team established a series of requirements, including the need for:

- **Continuous view of vulnerabilities** – with the ability to discover network vulnerabilities and security issues on the fly without running active vulnerability scans.
- **Proactive auditing and configuration tracking for compliance failure**s – to help identify critical risks and build secure configuration baselines continuously.
- **Patch management system audits** – to identify reporting discrepancies and mitigate risk.
- **Centralized management and reporting** – for all vulnerabilities, configuration and compliance failures and systems logs in a single dashboard to improve team understanding of vulnerability-related risk and response.
- **Passive discovery of new and rogue devices on the network** – with the ability to group devices based on their properties (e.g., OS, services, physical location etc.), and provide customized scans for each group of devices.

The Tenable Solution

To fulfill its requirements, SAI Global engaged Content Security, a Tenable authorized partner in ANZ, with expertise implementing and integrating Tenable's complete platform for vulnerability management, attack detection and mitigation, compliance monitoring, and IT risk management

For SAI Global, Content Security deployed Tenable SecurityCenter Continuous View. An enterprise-class security solution, SecurityCenter Continuous View combines the award-winning active scanning capabilities of the Nessus® vulnerability scanner with Tenable's unique Passive Vulnerability Scanner, advanced analytics, reporting and dashboards.

The tools and data provided by SecurityCenter Continuous View are transforming SAI Global's security posture by providing:

- Centralized management of distributed vulnerability management scanners
- Insight into the criticality of risk and remediation of false positives
- Ongoing compliance and vulnerability scanning and reporting
- Identification of rogue devices and sensitive data traversing its network
- Detection of vulnerabilities associated with mobile devices
- Dashboards and reports that enable actionable insight and risk reduction

Results

Commenting on the impact SecurityCenter Continuous View has had on SAI Global's security oppertations, Macarthur-King stated, "The results have been eye-opening. We discovered that there were a few vulnerabilities within our network that impose critical risks to our environment. Remediating these vulnerabilities on a real-time basis has improved the security of our environment."

Through its use of SecurityCenter Continuous View, SAI Global has achieved a number of benefits including:

Improved compliance – enhanced reporting has created a better understanding network configuration and compliance failures, making it easier for the security team to plan for and address compliance issues.

Enhanced productivity – by grouping systems according to their function and/or properties the team can more effectively distribute responsibilities for fixing certain vulnerabilities. In addition to improving productivity, this helps ensure vulnerabilities are remediated in a timely manner.

Risk reduction – By aggregating passively found vulnerabilities, actively found vulnerabilities, configuration failures, compliance failures and system logs, SecurityCenter Continuous View boosts overall visibility of security risks impacting the entire SAI Global network.

All told, with SecurityCenter Continuous View, SAI Global is realizing significantly greater levels of insight into network security risk. This, coupled with improvements in incident response and the effectiveness of individual team members has strengthened SAI Global's overall security posture, while reducing ongoing operational risk.

> "The results have been eye-opening. We discovered that there were a few vulnerabilities within our network that impose critical risks to our environment. Remediating these vulnerabilities on a real-time basis has improved the security of our environment."

Peter Macarthur-King
GM IT,
SAI Global

For More Information

Questions, purchasing, or evaluation:

Content Security
Securing Networks