secpod

Leading Commercial Interior Design Firm Enhances Cyber Security with Automated Vulnerability Management

Profile

Claremont is a leading provider of Workplace Consultancy, Interior Design, Fit-Out, Furniture, and Workplace Technology. They focus on creating workspaces that support the basic needs of your people and create an inspirational experience, which they call the Destination Office.

For more information, visit their **What We Do** page at **https://www.claremontgi.com**

Challenge

Navigating the Complexities of manual Vulnerability Management and Cyber Security Compliance Tracking

Claremont has traditionally employed a manual approach with limited tools for vulnerability management, resulting in slower remediation times and an outdated perspective on vulnerabilities across their assets.

Periodic scans led to a lack of real-time coverage of the attack surface, making the vulnerability management process non-continuous and causing delays in risk identification. Additionally, they faced challenges such as tracking security deviations, detecting obsolete software versions, and prioritising vulnerabilities based on risk severity, exploitability, and business context.

This manual approach prevented them from achieving the comprehensive vulnerability management required for sustainable risk containment. Furthermore, Claremont undergoes annual cyber security audits as part of the UK government-backed Cyber Essentials Plus scheme. Failure to meet certification requirements imposed a strict 30-day remediation window for vulnerabilities before re-evaluation.

This manual process proved laborious and complex, escalating the need for urgent reform in Claremont's vulnerability management practices to establish a proactive security posture capable of mitigating vulnerabilities effectively, especially given their expanding business.

Solution

Saner CVEM

To automate the vulnerability management process & seamlessly meet compliance

The IT team realized the importance of a continuous, fully automated, integrated platform for vulnerability management, as this was the only way to overcome the fiascos of the manual approach.
For them, earning auditor confidence was paramount.

SanerNow, with its automated Continuous Vulnerability & Exposure Management (CVEM) capabilities, helped them to accurately identify assets, deploy software, detect any security gaps, discover & prioritize vulnerabilities, and patch them in a timely manner. It brought in greater accuracy and speed, helping them get a better understanding of the attack surface.

Their security apparatus got strengthened. They could now track vulnerability trends across assets, gain clarity on how risk changed over time, and reduce attack surface to meet compliance needs.

The IT team could now detect vulnerabilities in minutes instead of weeks, offering them an entire seven modules for vulnerability management and the world's largest vulnerability management database from SecPod, which is continuously updated every day to enable accurate detection.

Saner CVEM pruned the end-to-end vulnerability management process by enabling the IT team to detect undiscovered flaws, remediate security weaknesses, and reduce the risk of compromise.

Asset protection & compliance risk management with reassurance from Saner CVEM

Saner CVEM, with its integrated platform comprising seven modules, offered comprehensive coverage and remediation of risks to advance and accelerate their vulnerability management program.

Asset inventory management

Ensured continuous visibility and control over IT infrastructure, enabling better control over IT assets. They were able to discover rarely used and outdated applications, track software licenses, and continuously evaluate the use of assets.

Module features

- Cloud-based console for IT asset management to ensure comprehensive visibility,monitoring, and access to assets.
- Automated, real-time, live asset scans of every endpoint and server to give a comprehensive, transparent view of software and hardware inventory.
- Light-weight agents to enable continuous or on-demand scans to detect any deviations.
- Automatically track asset movement in the network
- Insightful dashboards to gather asset data and enable data-driven decisions.
- Track software licenses, allow or block applications based on use.
- Detect the availability and entry of any malicious or vulnerable assets across devices.
- Track and manage licenses of OS, third-party applications, and hardware.

Risk Prioritisation

Ensured rapid detection and combat of burgeoning vulnerabilities, including huge backlogs, to reduce risks and attack surface. Powered by the world's first SSVC-based vulnerability prioritisation framework, IT teams were able to get an exhaustive visibility of the attack surface.

Module features

- Understand, evaluate, and handle millions of vulnerabilities with ease.
- Pinpoints vulnerabilities that make up the exploitable attack surface
- Contextualize vulnerabilities based on exploitability levels, automat-
- ability, and business impact.
- Automate prioritisation of vulnerability risks in real-time
- Configure and prioritize risk based on organization's structure.

Posture anomaly management

Gained total clarity by holistically assessing IT infrastructure for any unusual processes & services, abnormal events, unusually executed commands, and other hidden risks, along with intelligent insights on how to act on these security risks.

Module features

- Identify any changes in IT infrastructure.
- Identify devices that are different from others.
- Provides remediation measures to fix anomalies instantly.
- Discover attack vectors in the network & reduce risk exposures.
- Analyse every security control and spot any changes.
- Get insightful reports to uncover any posture facts.
- Whitelist devices & configurations.
- Continuously examine security posture with insightful dashboards

Vulnerability Management

Comprehensive, proactive, continuous scans across every endpoint and server, assessed the status of vulnerabilities, the level of risk tolerance, the level of threat represented by each exposure, and vulnerabilities that need immediate fixes.

Module features

- Lightweight agent to run highly accurate scans across the breadth and depth of the enterprise IT infrastructure.
- Single unified dashboard to get a clear picture of every vulnerability.
- Scans driven by the world's largest vulnerability database owned by
- SecPod with over 175,000 vulnerability checks ensuring near zero false positives.
- Intelligent scanning algorithm to perform the industry's fastest scan to detect vulnerabilities in just 5 minutes.
- Detailed insights such as vulnerability exploitability levels, along with CVSS information

Patch Management

Automated end-to-end patch management from scanning, prioritisation, download, and testing to scheduled deployment ensured faster deployment cycles across every deployed device, eliminating manual interventions.

Module features

- Cloud-based console for role-based access control of patch tasks
- Latest vendor patches, pre-tested, ready for deployment in under 24 hours
- Effortless rollback of erroneous patches
- Assess and prioritize patches based on vulnerability severity levels
- Firmware patches to tighten security
- uto-generated reports to assess the patching status in the network

Compliance Management

Proactive, continuous compliance checks to regulate devices with UK Cyber Essentials benchmarks. The module ensured tremendous gains in speed and time to improve cyber hygiene, recover from cyber exposure gaps, and deliver better audit results.

Module features

- Continuous scans to detect non-compliant endpoints by identifying system misconfigurations.
- Assess device risks and remediate them immediately to restore compliance.
- Fast compliance scans to align with security compliance regulations.
- Customization of policies to enforce regional security compliance policies.
- Cloud-based console to simplify compliance reporting.
- Auto-generated, audit-ready reports

Endpoint Management

Secured endpoints by identifying configuration errors or any dangerous vulnerabilities that might lead to security breaches. Ensured complete control and seamlessly troubleshoot endpoint issues continuously and quickly.

Module features

- End-to-end visibility with live monitoring of endpoint health of more than 100+ metrics
- Integration of endpoint security and management to implement cyber hygiene practices.
- Automation of endpoint management across heterogeneous OS networks
- Strong security controls to harden endpoint security posture.
- Reduced attack surface by blocking/disabling malicious apps and rogue devices.
- Improved system performance through remote execution of scripts to update or troubleshoot systems.
- Regulation of endpoint use by automating reporting and audits

Saner CVEM's value proposition that enabled UK cyber-essentials compliance certification

No false sense of security

24x7 automated scanning and remediation features ensure IT assets are proactively scanned to fix vulnerability risks accurately. The platform also made security more manageable by reducing scan times and offering fewer false positives.

Overarching IT infrastructure visibility

By automating the discovery and inventory of IT assets, the security team got better control over IT infrastructure and environment. A comprehensive inventory of asset ecosystems helped them to visualise and discover devices by monitoring the network and dynamically predicting risks susceptible to breach.

Automation of vulnerability management

Automation ensures scans are not episodic, where the scanning process restarts at periodic intervals. Rather, it became continuous and seamless, covering the entire attack surface of the organisation. With its real-time automated and continuous assessment capabilities, built-in security intelligence, risk prioritisation, and insights, the platform helped in understanding vulnerabilities and proactively remediating them deeply.

Detect provisioned resources that are out of compliance

Asset inventory visibility provided continuous monitoring and evaluation of IT assets, and continuous compliance scans helped detect non-compliant devices with defective system configurations. Faster compliance assessments & immediate remediation by automating the installation of verified patches to address compliance risk.

Gather information about IT estate to prepare for audit

Evaluate the security status of systems, applications, and networks through customised reports on risk remediation. Heightened audit readiness is due to an in-depth understanding of vulnerabilities and risks, including inefficiencies or flaws in IT systems and the need to fix them immediately.

Maximise returns on compliance investments

Evaluate the security status of systems, applications, and networks through customised reports on risk remediation. Heightened audit readiness is due to an in-depth understanding of vulnerabilities and risks, including inefficiencies or flaws in IT systems and the need to fix them immediately.

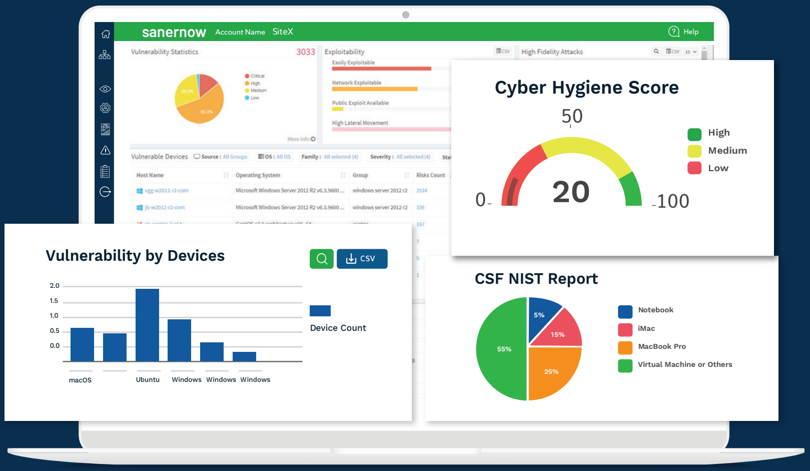
The Saner CVEM Experience: Client’s View

“Saner CVEM has revolutionised the way we deal with vulnerabilities. It not only shows you the risk, but it also does a deep dive analysis of these risks and tells us how to remediate them. Saner CVEM is easy, intuitive, and simple to use. This has helped us to neutralise any threats due to vulnerabilities and keep track of our devices.”

- IT Team

Outcomes

- Radical reduction in the number of vulnerabilities (from 20,000 to 3,000) in a month
- Drop in posture anomalies (from 50,000 to 3000) in a month.
- Lowered missing patches in devices (from 10,000 to 300) in a month.



About SecPod

SecPod is a cyber security technology company. We prevent cyberattacks. We do everything to prevent attacks on the computing environment. Our product helps implement cyber hygiene measures, so attackers have a tough time piercing through. Our SanerNow Cyber Hygiene platform provides continuous visibility to the computing environment, identifies vulnerabilities and misconfigurations, mitigates loopholes to eliminate attack surface, and helps automate these routines. Our product philosophy is offering simplicity and automation to make the job of security administrators slightly better.

Email: info@secpod.com

Website: www.secpod.com