secpod

CASE STUDY

Digital Banking Services Provider Achieves Instant Visibility of Risk Posture across Enterprise IT Estate, Rapidly Remediating Risks, and Ensuring Continuous Compliance

www.secpod.com

PROFILE

The Fintech Service Provider offers end-to-end mobile financial services, enabling people to safely send and receive money through mobile devices, catering to their daily financial transactional needs. With over 800,000 agents and merchants and a customer base of more than 70 million, the company focuses on integrating banks and financial institutions to enable faster, secure, cashless transactions.

INDUSTRY

Banking & Finance

REGION

Asia Pacific

CHALLENGE

Inability to understand Vulnerability Risks due to Traditional Approaches

The company embarked on digital transformation initiatives to enable agility and adapt to market changes. This led to increased use of heterogeneous applications running on various endpoints and Windows, Linux, and MacOS servers. They saw a year-round increase in the number of vulnerabilities with different levels of severity.

The ever-expanding complex digital footprint, multiple platforms, and diverse, distributed technology environments led to an increase in attack surface and security risks. They could not get comprehensive visibility of their IT infrastructure to understand the full context of vulnerabilities and the criticality of affected assets. The pandemic increased this concern further.

Moreover, they used traditional vulnerability management tools having these limitations:

- ✓ Offered limited IT asset visibility & no clarity of risk posture
- ✓ Multiple tools that couldn't scale
- ✓ Siloed interfaces gave a misleading sense of security
- ✓ Complex, time-consuming patching process for software and endpoints
- ✓ Lacked transparency due to the inability to provide software and hardware inventory status
- ✓ Inability to remediate risks & had cumbersome reporting process
- ✓ Manual interventions making them non-consumable for daily operations

Continuous security & compliance were a distant dream. They decided to move out of this legacy, manual approach to address the rising number of vulnerabilities & stay ahead of the curve.

SOLUTION

SanerNow–
The Chosen One

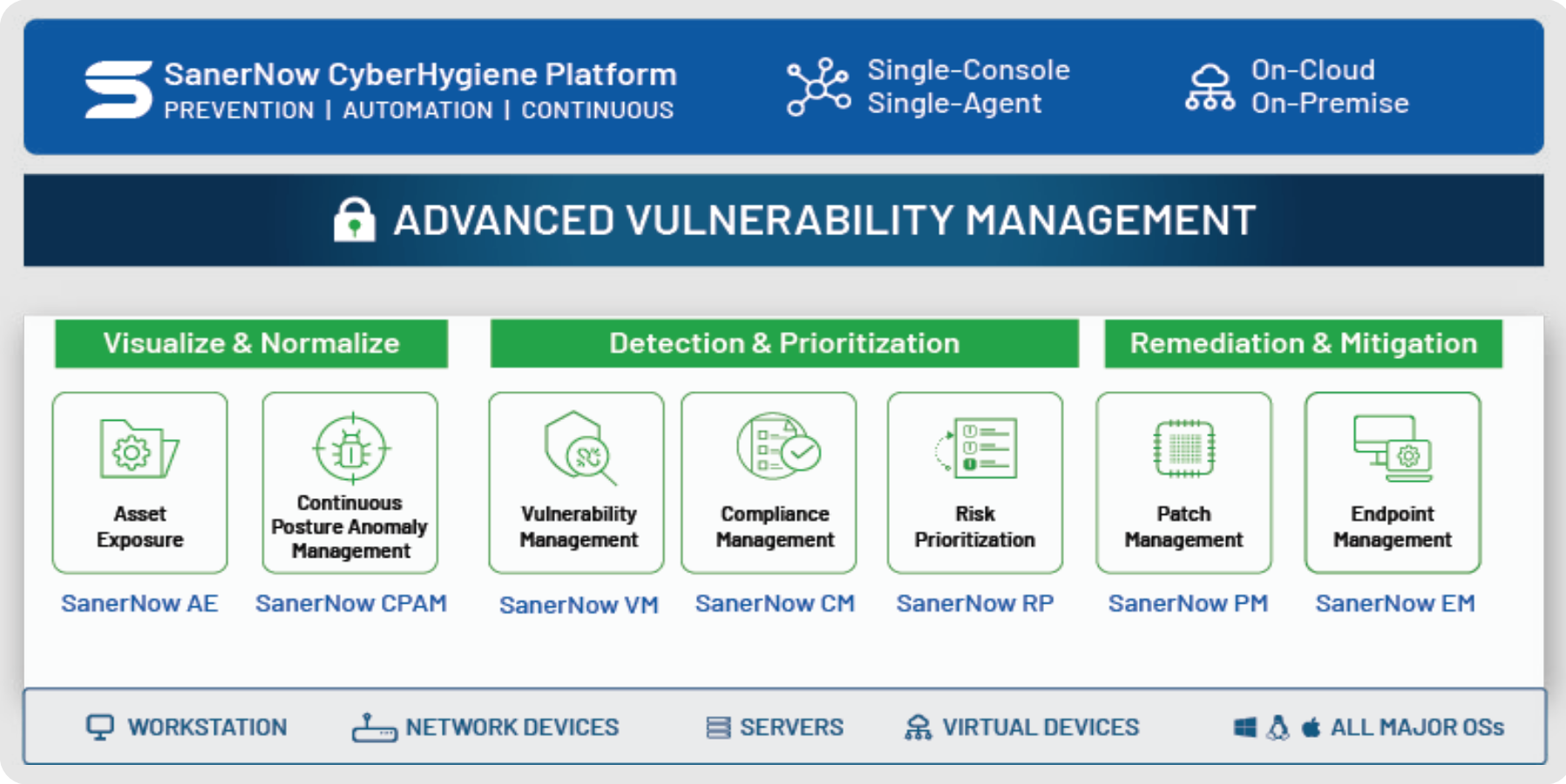
To remain agile.
To move fast.
To stay secure.

The client's security practitioners on the front lines needed a fast, easy way to gain end-to-end visibility of their IT infrastructure and proactively find and remediate vulnerabilities.

Choosing SanerNow was a game-changing move. It gave them a risk-based single pane of glass view of their attack surface and helped them to proactively identify, detect, prioritize, and remediate critical vulnerabilities. Its cloud-based centralized console helped them unify the end-to-end vulnerability management program under one suite.

With its manageability and what was built-in, as opposed to the siloed tools they were using before, SanerNow was unique.

Actioning SanerNow Features to take on Vulnerabilities



Automated Asset Inventory Management for Better Control over Assets

By leveraging the Asset Management feature, they achieved real-time visibility and control over IT assets. They were able to continuously evaluate the use of assets and right size the infrastructure. This helped faster remediation of vulnerabilities, reduced downtime, and improved productivity.

FEATURE FACTS

- ✓ 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

Automated Vulnerability and Patch Management to Remediate Risks Faster

The vulnerability and patch management feature ensured maximal non-stop security coverage at scale and prevented the occurrences of potential compromise in their endpoints and servers.

FEATURE FACTS

- ✓ Fastest, on-demand, automated vulnerability scans in less than 5 minutes

- Comprehensive scans by using the world's largest built-in vulnerability database with 175,000+ software vulnerability checks
- One smart, lightweight, multi-functional agent for all tasks with no interruption to users
- Prioritize vulnerabilities based on exploitability levels and assess high-risk ones
- Single unified dashboard for 360-degree visibility
- Automated remote patch management from the cloud for large-scale vulnerability remediation
- Patching of all operating systems, including Windows, Mac, and Linux
- Continuous patch scans to identify missing patches
- Rollback of any error-prone patches to the last stable version
- Firmware patching for total risk mitigation
- Auto-generated reports to assess patching status

Automated Compliance Management to Regulate Devices

SanerNow's automated compliance management capabilities provided a strong foundation to meet multiple global compliance and regional regulatory standards. The proactive, continuous compliance checks gave them tremendous gains in speed and time to improve cyber hygiene, recover from cyber exposure gaps, and deliver better audit results.

FEATURE FACTS

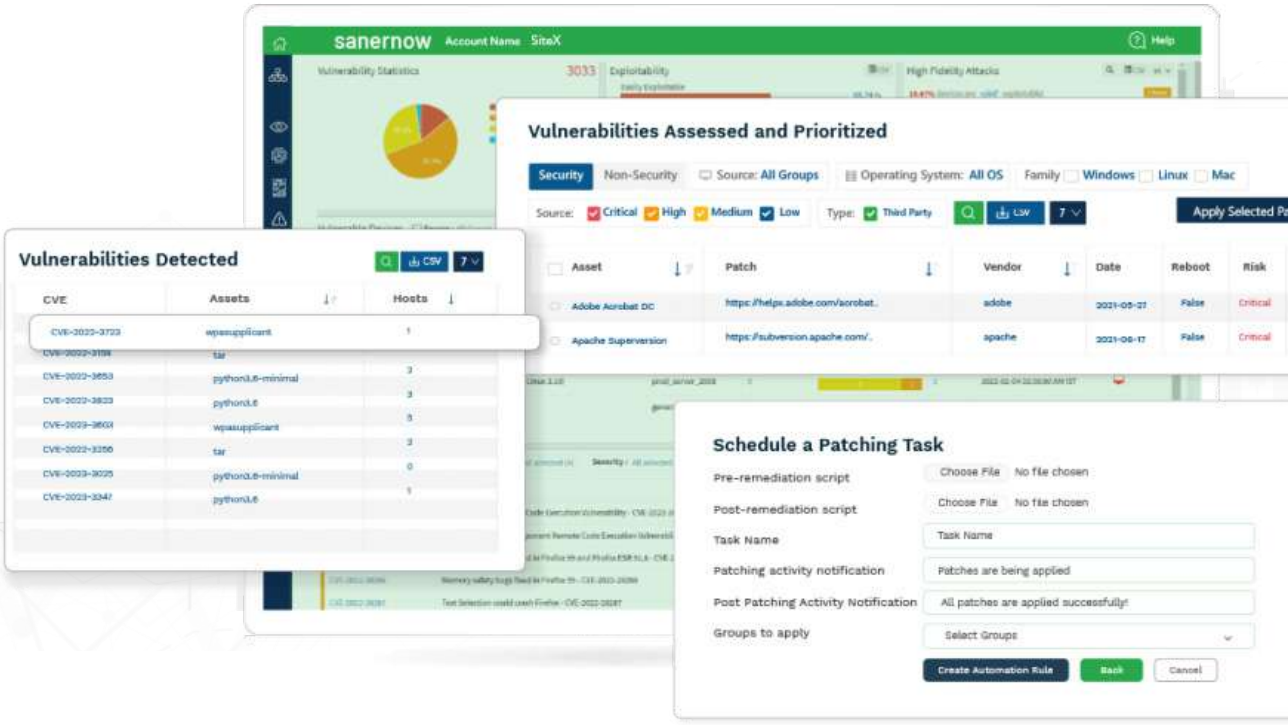
- Continuous scans to detect non-compliant endpoints by identifying system misconfigurations
- Assess device risks and remediate them immediately to restore compliance
- Fast compliance scans to align with security compliance regulations
- Customization of policies to enforce regional security compliance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

Automated Endpoint Management to Monitor and Fix System Risks

Automated endpoint management feature protect endpoints by identifying configuration errors or any dangerous vulnerabilities that might lead to security breaches. By automating every endpoint management activity, they could gain complete control and seamlessly troubleshoot endpoint issues continuously and quickly.

FEATURE FACTS

- ✓ Monitor and Assess 100+ Endpoint Health Controls in Real-time
- ✓ Integration of endpoint security and management to implement cyber hygiene practices
- ✓ Automation of endpoint management across heterogeneous OS networks
- ✓ Reduced attack surface by blocking/disabling malicious apps and rogue devices
- ✓ Improved system performance through remote execution of scripts to update or troubleshoot
- ✓ Regulation of endpoint use by automating reporting and audit systems



Here is how the Client's Security Leadership Team echoed their sentiments about SanerNow

SanerNow ensures cyber hygenie. It helps us detect and remediate vulnerabilities how we want and secures the whole environment. This platform will solve the problems the financial industry has been facing for a long time. I don't see any other platform that matches SanerNow's capability or performance. I always tell my peers that if they want a peaceful sleep, they should use SanerNow!

EVP & HoD, IT Governance, Product & Technology

SanerNow is a new product for us. We used Tenable and Microsoft solutions for vulnerability management, which were cumbersome as the patch had to be developed and deployed. SanerNow does it automatically. Patching is easy and readily available in SanerNow, making our life easier. Earlier, we also visualized the number of vulnerabilities in the server and fixed them manually. SanerNow now automates this. This saved a lot of time while deploying the patches, checking the vulnerabilities, and correlating to each other. Reporting is very easy. The dashboard provides excellent visibility of all our IT assets, how many servers are there, how many are active, how many have agents, how many are in a healthy state, etc. My peers are surprised how I am able to patch our IT assets in such a short span of time. I proudly tell them I use SanerNow.

VP, Windows Infrastructure Operations, IT Governance, Product & Technology

How SanerNow proved to be the Industry's Most Advanced, Scalable, and Extensible Platform

No False Sense of Security

24x7 automated scanning and remediation features ensured 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 visualize and discover devices by monitoring the network and dynamically predicting risks susceptible to breach.

End-to-End 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 organization. With its real-time automated and continuous assessment capabilities, built-in security intelligence, risk prioritization, and insights, the platform helped in understanding vulnerabilities and proactively remediating them deeply.

Continuous Compliance

Achieved regional banking regulatory needs to identify faulty system configurations and fix them to ensure optimal cyber hygiene. Detected and fixed non-compliant devices and eased compliance reporting to reduce time and effort.

Tighter Alignment of IT & Security Teams

The centralized, single console approach helped identify and remediate vulnerabilities and ensured IT & security teams worked in tandem to ensure no overlap or oversight. This resulted in a cultural shift in how these teams worked. Vulnerabilities and their respective patches were applied automatically with no manual dependencies and IT service disruptions, providing a forward momentum to business.

QUICK FACTS ABOUT SANERNOW PLATFORM

Why it's the next curve in Continuous Vulnerability Management

- ✓ The only platform you need to prevent cyber attacks
- ✓ Capable of detection & remediation of vulnerabilities with one lightweight, multi-functional agent
- ✓ Agent resides in systems even when they are running or aren't connected to the network
- ✓ Agent is reliable, fast, and accurate when compared to agentless scanners
- ✓ Automates the entire process of vulnerability management with no manual interventions

OUTCOMES

Proving SanerNow is ahead of the rest

- Clarity on the types of endpoint & server vulnerabilities & device compliance status
- Visibility to the number of vulnerabilities in each device and the severity level of each vulnerability (low, medium, high)
- Awareness of the exploits available for each vulnerability
- Drastic reduction in the number of vulnerabilities (from 20,000 to 4,000) in a month
- Lowered time required to fix vulnerabilities from 1 month to 5 minutes
- Reduced total cost of ownership as traditional tools were 5 times costlier than SanerNow

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.

Visit us- www.secpod.com
Write to us- info@secpod.com

Connect with us