SanerNow Solution Brief for Healthcare

Yuma Regional Medical Center in Arizona, United States, suffered a ransomware attack in April 2022. The attack exposed the Social Security Numbers and other personal information of over 700,000 patients. YRMC discovered ransomware files in their external systems and revealed that an unauthorized person had gained access to YRMC systems and invaded their network.

This incident is an infamous attack that has occurred due to loopholes in both data security and IT infrastructure security. While the healthcare sector has adopted data security widely in recent years, IT infrastructure security still has a great deal to do. InfoSec Leaders in Healthcare should be concerned about IT infrastructure security and not ignore it, believing healthcare businesses do not rely entirely on IT assets.

Cyberattacks on healthcare and public health institutions can occur in many forms.

Apart from the theft of patient records, healthcare organizations can face disruption due to both sophisticated and uncoordinated attacks. Modern healthcare organizations rely on an extensive network of medical devices, each acting as an entry point for an attack. Attackers can easily gain unauthorized access to medical devices, causing wide-scale disruption across healthcare facilities.

For instance, network systems monitor and manage power generation and transmission, heating of ventilators and airconditioning units, water and oxygen supply utilities, and multiple critical controls like this. An attack on these systems will affect the healthcare facility to a large extent, causing huge inconvenience to the patients. An attack like this is worse than a data security breach and goes beyond data privacy. This will put patients' lives at risk and the healthcare organization's reputation at stake.

Impact of Cyberattacks due to Inadequate IT Security in Healthcare

Loss of Trust and Reputation

Patients and practitioners could lose trust in healthcare providers, tarnishing their reputations.

Threat of Facility Disruption

Cyberattacks in network systems can take facilities offline, disrupting patient care and operations continuity.

Hefty Regulatory Fines

HIPAA mandates a wide array of security controls for healthcare and public health institutions. Violation of HIPAA will cause hefty fines to the healthcare organization.

Physical Damage to Systems

Cyberattacks can damage systems performing crucial healthcare functions, impair patient care, impede emergency response, and even lead to the loss of patients' life.

SanerNow AVM (Advanced Vulnerability Management) to Secure IT Infrastructure and Implement Cybersecurity For Healthcare Organizations

SecPod SanerNow provides a continuous, automated, advanced Vulnerability Management solution to prevent cyberattacks and achieve continuous security risk and compliance posture. We enable IT security teams to go beyond traditional vulnerability management practices and get complete visibility and control over the healthcare organization's attack surface. With SanerNow, you can automatically detect and manage vulnerabilities and other security risks from a single centralized cloud-based console and a light-weight, multifunctional agent.

The New Age, Continuous, and Automated Vulnerability Management Solution Built to Prevent Cyberattacks

Harden Systems and Achieve Conformance with HIPAA Compliance

SanerNow provides the necessary security controls to identify the non-compliant devices and harden them to comply with HIPAA. You can run real-time compliance scans, fix deviations and misconfigurations, generate audit-ready reports, achieve continuous HIPAA compliance, and safeguard your network.

Real-time Detection of Vulnerabilities and Security Risks

Run the industry's fastest vulnerability scans in 5 minutes, powered by the world's largest security intelligence library with 160,000+ security checks. Continuously detect vulnerabilities and security risks in real-time and assess them thoroughly.

Timely Remediation with Integrated Patching

Remediate vulnerabilities on time with integrated patching without leaving any security gaps. SanerNow supports automated patching for all major operating systems like Windows, Mac, Linux, and 300+ third-party applications.

Gain Continuous Visibility into IT Asset Exposure

Perform continuous IT asset scans and gain complete visibility over your computing environment. Monitor your IT infrastructure continuously, gain control over hardware and software inventory, and detect malicious IT assets.

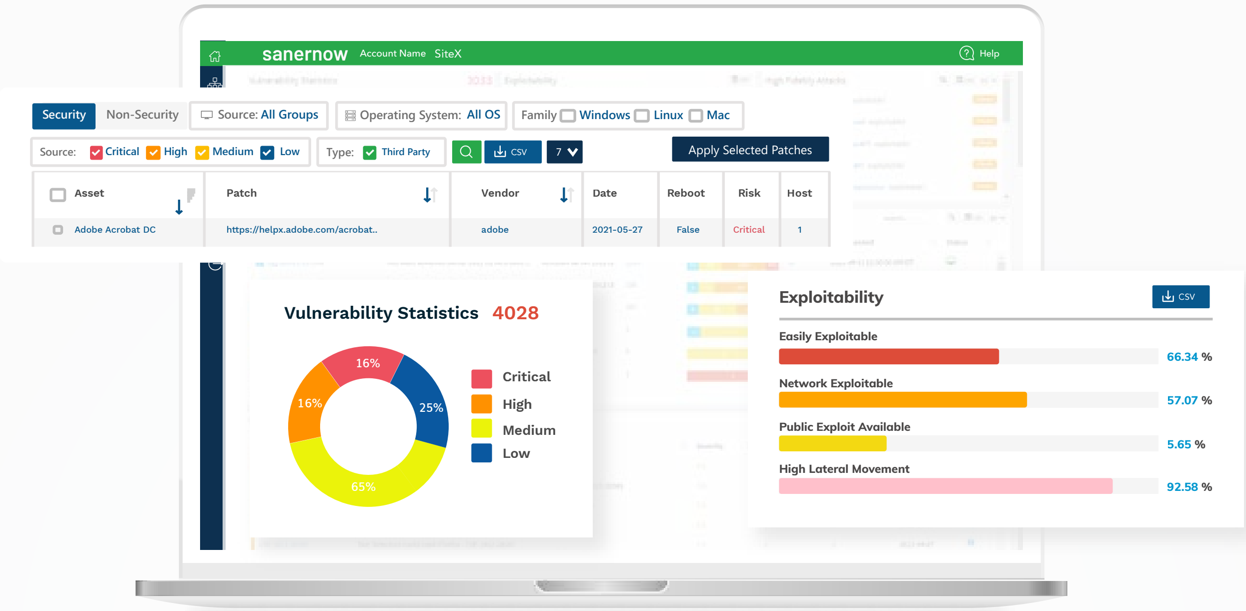
Remediation Controls Beyond Patching to Eliminate Attack Surface

Go beyond patching and leverage various remediation controls to mitigate numerous security risks. Monitor 100+ endpoint security metrics, manage system health, fix posture anomalies, apply security controls, block malicious applications and devices, and more.

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 CyberHygiene 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.



Source: All Groups | Operating System: All OS | Family □ Windows □ Linux □ Mac

Source: ☑ Critical ☑ High ☑ Medium ☑ Low | Type: ☑ Third Party

□ Asset	Patch	Vendor	Date	Reboot	Risk	Host
□ Adobe Acrobat DC	https://helpx.adobe.com/acrobat..	adobe	2021-05-27	False	Critical	1

Vulnerability Statistics 4028

Exploitability

Easily Exploitable	66.34 %
Network Exploitable	57.07 %
Public Exploit Available	5.65 %
High Lateral Movement	92.58 %

Schedule a SanerNow AVM demo here, and let us show what we tell

Schedule a Demo

CONTACT US

India - (+91) 80 4121 4020 / USA - (+1) 918 625 3023

info@secpod.com / www.secpod.com