SECURITY OPERATING PLATFORM FOR HEALTHCARE PROVIDERS

Palo Alto Networks® is uniquely qualified to protect patient data and safety as well as support regulatory compliance for thousands of hospitals, clinics and healthcare networks around the world through the advanced security prevention capabilities of the Security Operating Platform.

What We Do

- Provide next-generation cybersecurity for healthcare organizations with consolidated capabilities:
  - Sandboxing
  - IDS/IPS
  - Firewall
  - URL filtering
  - Anti-malware
  - Anti-exploit protection
  - Credential theft prevention
  - Dynamic authentication policies
- Protect all points in your healthcare IT environment:
  - Network perimeter
  - Data center
  - Endpoints, including medical devices
  - Mobile devices
  - Cloud
- Support and comply with regulations healthcare organizations must meet, such as HIPAA, PCI and GDPR.
- Detect, analyze and remediate threats, known and unknown, including advanced persistent threats, or APTs.
- Offer the same protection on both physical appliances and virtual machines.

How We Are Different

- Automatically identify more than 2,600 applications, such as HL7, Epic, DICOM and Cerner®, and integrate with your enterprise directory.
- Create true "Zero Trust" network segments, and allow access for approved applications and users, rather than only ports and protocols.
- Detect malware, viruses and APTs at excellent rates, powered by the integrated and community-driven nature of the platform.
- Efficiently process your traffic across all security functions in a single pass at speeds up to 200 Gbps with a purpose-built, parallel processing architecture.
- Seamlessly integrate with some of the best technology providers in the industry, such as Proofpoint™, Splunk®, Tanium® and VMware®, to deliver more holistic security.

Cybercriminals are increasingly targeting healthcare data. At the same time, healthcare providers' security and network staff must:

- Support new medical technology innovations, such as telehealth, wearable health devices and network-connected medical equipment, as well as broad IT trends, such as the virtualization of the data center, cloud migration and mobile devices.
- Detect and block threats as well as investigate cyber incidents.
- Enable safe access to patient data from myriad entry points, including hospitals, clinics, insurers, doctors' home offices, affiliate facilities, mobile devices and more.
- Ensure compliance with HIPAA, PCI DSS and other regulations on patient data, medical equipment and credit card transactions.

Palo Alto Networks helps you deploy a comprehensive cybersecurity strategy throughout your organization regardless of access point location, usage profile, type of traffic or other factors. Our Security Operating Platform protects complex IT environments for hospitals and clinics by providing:

- Full visibility and granular control over applications, users and content on your network.
- The ability to apply role-based access to any asset on your network.
- Detection and prevention of known and unknown threats to your networks, endpoints, data centers and clouds.

- Effective segmentation of network zones based on security requirements, access profiles and information exchanged to reduce risk and simplify compliance.
- Identification and elimination of unauthorized traffic and applications with high bandwidth consumption, such as Netflix®.
- Safe patient access to the internet with isolated guest-Wi-Fi at your various facilities.

A Foundation for Better Security

An effective security architecture requires consistent security rules from the edge of your network to the core of your data center. The Palo Alto Networks Security Operating Platform is a suite of natively integrated components that automate the prevention of cyberattacks.

Figure 1: Palo Alto Networks Security Operating Platform

The Security Operating Platform comprises multiple sensors and enforcement points, including next-generation firewalls at the network layer in physical or virtualized form, GlobalProtect™ network security for endpoints, Traps™ advanced endpoint protection, Aperture™ SaaS security service and Evident cloud security. These components work in concert with cloud-delivered security services, such as WildFire® malware prevention, AutoFocus™ contextual threat intelligence and Magnifier™ behavioral analytics services.

The Application Framework enables third parties and customers to make use of the sensors, enforcement points and rich data the platform collects over time to build their own security applications. This open, extensible approach accelerates adoption of security innovations from any provider by enabling customers to evaluate, deploy and operationalize new technologies that employ the Security Operating Platform components already on their networks.

Together, the platform components provide healthcare providers with visibility and enforcement capabilities as well as layered defenses to prevent cyberattacks throughout the attack lifecycle, taking advantage of automated response and enforcement.

The following table summarizes the most common use cases for healthcare providers:

Use Case	Answer
Edge Protection	Block high-risk traffic to the internet using advanced security technologies
Network Segmentation	Isolate data into zones to protect patient data and reduce the scope of compliance
HIPAA Compliance	Support HIPAA compliance by restricting access to PHI, providing audit controls and enforcing transmission security
PCI Compliance	Decrease the scope of PCI compliance audits by isolating PCI devices
Endpoint Protection	Prevent malware and exploits on endpoints – even unpatchable ones, such as medical devices based on Windows XP
Data Center Protection	Provide high-speed threat prevention for physical, virtual and public cloud-based servers
Mobile Device Protection	Enforce the same security policies on mobile devices wherever they go
Remote Clinics	Securely and safely connect remote clinics and offices

Read on for more details on these use cases.

Use Case No. 1: Prevent Cyberattacks at the Network Perimeter

Deploy Palo Alto Networks Next-Generation Firewall at the edge to gain control over what's on your network at all times. A core differentiator of our platform is the ability to automatically detect more than 2,600 applications, including HL7 and DICOM traffic, as well as integrate with enterprise directories to identify users. User identification at the firewall makes it easier to track down the location of malware-infected PCs. In addition, our credential theft prevention minimizes the effectiveness of phishing and subsequent account takeover attacks.

The next-generation firewall's native IPS, anti-malware, anti-exploit and URL filtering capabilities protect healthcare providers from sophisticated cyberattacks, including ransomware and advanced malware, such as Locky, SAMSA, Derusbi, Sakula and CryptoWall.

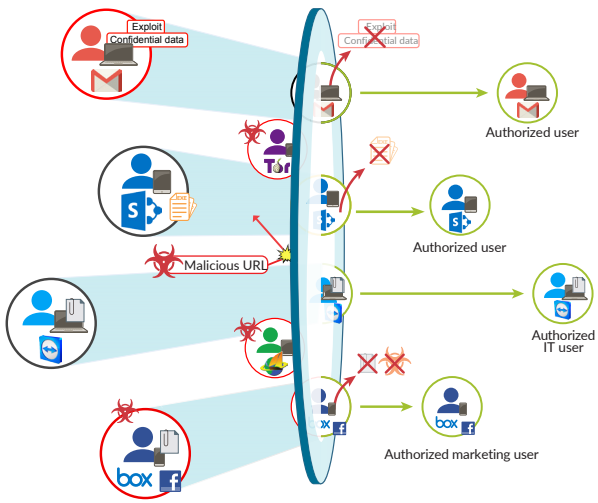

Figure 2: Safe enablement of applications, users and content through Palo Alto Networks NGFW

Use Case No. 2: Configure Network Segmentation

Network segmentation helps healthcare providers effectively:

- Limit the exposure from a compromised workstation or server endpoint by restricting lateral movement.
- Increase the difficulty for attackers to successfully exfiltrate data from hospital networks.
- Reduce the scope of PCI DSS compliance.
- Help meet HIPAA requirements related to controlling access to protected health information, or PHI.
- Implement true Zero Trust segmentation, based on the principle "never trust, always verify" – a cross-industry best practice.
- Increase visibility of internal network traffic to apply security inspections and desired policies.

With the Security Operating System, healthcare providers can achieve these benefits by isolating common types of devices into zones and allowing traffic between the zones based on approved applications or user directory groups. See Figure 3 for an example of the minimum recommended zones for network segmentation in hospitals.

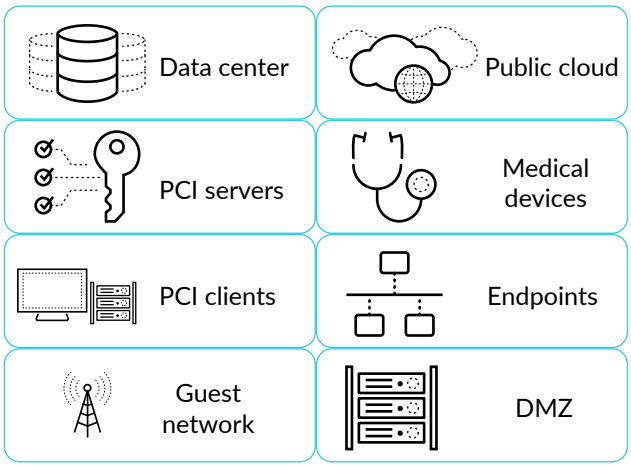

Figure 3: Example zones for segmentation in hospitals

Use Case No. 3: Support HIPAA Compliance

Healthcare providers manage highly sensitive patient data protected under regulations that differ by country. In the U.S., HIPAA outlines the minimum security requirements for managing PHI at covered entities. Some of the ways the Security Operating Platform supports numerous HIPAA Security Rule requirements include:

- **Access control:** User identification at the firewall restricts user access to applications or zones.
- **Integrity controls:** Advanced threat prevention features maintain the integrity of PHI by preventing malware and exploits.
- **Audit controls:** Audit logging with native user identification provides access reports for systems with poor reporting capabilities that contain PHI.
- **Transmission encryption:** Application detection at the firewall directs security teams to systems using unsecure protocols, such as FTP and HTTP, to transfer PHI.

See the Appendix for the full list of HIPAA requirements supported by the Security Operating Platform.

Use Case No. 4: Decrease the Scope of PCI Compliance Audits

Network segmentation helps decrease the scope of PCI DSS audits. For instance, isolating devices that process or store credit cards into a "PCI" zone with proper controls in place lets you limit the scope of PCI DSS compliance to only that zone, rather than the entire network. The next-generation firewall identifies applications and users through App-ID™ and User-ID™ technology, helping you create traffic rules between zones that are easier to understand and manage than legacy port and protocol rules.

For example, you could use the following rules to define connectivity between an Endpoint zone, a PCI Endpoint zone and a PCI Server zone:

- Block and log all inbound and outbound zone traffic (Zero Trust).
- Allow only finance users to access the PCI Server zone (User-ID).
- Flag PaymentCollect as the only allowed application (App-ID).

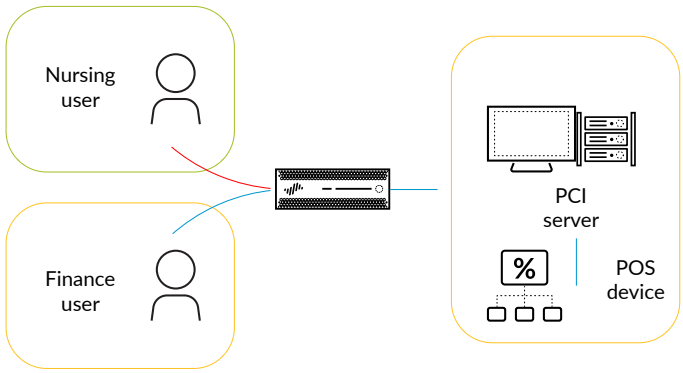

Figure 4: Defining connectivity between an Endpoint zone, PCI Endpoint zone and PCI Server zone

With these rules in action, Nursing users would not be able to access the PCI zone, but Finance users would (see Figure 4).

This gives you an idea of the dynamic rules you can define to isolate certain zones within your network to ensure only specific users or applications can pass through the zone boundaries.

Use Case No. 5: Protect Endpoints That Are Difficult to Patch

Due to the complex nature of hospital IT environments, many IT departments struggle to patch all devices across the hospital network. In addition, most vendor-provided computers that control medical devices are extremely difficult to patch – often, IT does not even have the access or visibility required to patch them – leaving these systems vulnerable.

Vendor-provided PCs are usually not patched, and IT is not made aware, so there is no clear patching owner and no local antivirus/anti-malware protection.

Many of our healthcare customers use Traps™ advanced endpoint protection to prevent malware and exploits on their endpoints. The lightweight Traps agent uses signature-less threat detection to decrease the risk to workstations, servers and PC-based medical devices that are difficult to patch.

Additionally, the multi-method prevention capabilities of Traps against known and unknown threats have earned it recognition as a suitable replacement for antivirus, meeting or exceeding the requirements of both PCI DSS and HIPAA.

Use Case No. 6: Protect Mobile Devices

Doctors and nurses extensively use mobile devices, such as smartphones and tablets, for clinical services at the bedside. You can extend the protection of the Palo Alto Networks Security Operating Platform to your deployed mobile devices with GlobalProtect™ network security for endpoints, which is natively integrated with WildFire malware prevention service for the detection of unknown threats, and with mobile device management providers, such as AirWatch®, for easier deployment.

Deploy GlobalProtect to managed endpoints with GlobalProtect cloud service to achieve the same network-level threat protection whether your laptops access the internet from inside or outside the hospital network.

You can also enable GlobalProtect Clientless VPN on unmanaged devices to access corporate web applications through the GlobalProtect portal.

Centrally Manage the Platform

Hospital IT security and network management teams can collaborate on a single security platform with defined administrative roles to enforce the separation of duties. Panorama™ network security management makes firewall management and intelligence gathering easy. You can use the native log viewer or integrate with third-party log management tools, such as Splunk, LogRhythm® and ArcSight®, to create traffic reports for network management and regulatory compliance.

Take the Next Step and Regain Control Over Your Network

Discover more about the comprehensive visibility and granular control our prevention-oriented approach provides as well as how you can use the Security Operating Platform to automatically stop cyberattacks in your healthcare environment.

Choose your next step:

- Schedule an online product demonstration we can tailor to your organization's unique needs.
- Take an Ultimate Test Drive, in which your teams can get hands-on experience with our technology.
- Conduct a free, on-site proof of concept, where we will help deploy our Security Operating Platform in your environment without impacting hospital operations. You will receive a detailed Security Lifecycle Review summarizing the findings.

Appendix: How Palo Alto Networks Security Operating Platform Supports HIPAA Security Rule Compliance

HIPAA Standard	Requirement	How Palo Alto Networks Security Operating Platform Supports the Requirement
§ 164.312(a)(1)	**Access control:** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4) [Information Access Management].	Palo Alto Networks Next-Generation Firewall integrates with your enterprise directory to identify users and enforce policies based on user types, job titles or security group. Access to entire zones or certain applications containing PHI within zones can be limited based on user attributes.
§ 164.312(a)(2)(i)	**Unique user identification:** Assign a unique name and/or number for identifying and tracking user identity.	Palo Alto Networks Next-Generation Firewall provides audit logging, which stores the unique user name so compliance reporting can associate network activity with a user identity.
§ 164.312(a)(2)(iv)	**Encryption and decryption:** Implement a mechanism to encrypt and decrypt electronic protected health information.	Palo Alto Networks Next-Generation Firewall identifies data transmitted without encryption via insecure protocols, such as FTP and Telnet. Reports enable security teams to identify systems transmitting data in the clear and remediate with strong encryption.
§ 164.312(b)	**Audit controls:** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	The Palo Alto Networks Security Operating Platform provides robust audit logging at the user level.
§ 164.312(d)	**Person or entity authentication:** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	GlobalProtect provides two-factor authentication capabilities for remote users who need to access internal systems that contain PHI. Furthermore, GlobalProtect provides end-to-end data encryption during transit.
§ 164.312(e)(1)	**Transmission security:** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Palo Alto Networks Next-Generation Firewall identifies data transmitted without encryption via insecure protocols, such as FTP and Telnet. Reports enable security teams to identify systems transmitting data in the clear and remediate with strong encryption.
§ 164.312(e)(2)(ii)	**Encryption:** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	
§ 164.312(c)(1)	**Integrity:** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Palo Alto Networks Security Operating Platform provides anti-malware, anti-exploit and threat intelligence capabilities that prevent threats on the network, such as CryptoWall and other malware, from altering PHI. Traps protects the integrity of running processes and critical files on endpoints.
§ 164.312(c)(1)	**Integrity controls:** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	
164.308(a)(5)(ii)(B)	**Protection from malicious software:** Implement procedures for guarding against, detecting, and reporting malicious software.	

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

security-operating-platform-for-healthcare-providers-b-091418