SECURITY PLATFORM FOR HEALTHCARE PROVIDERS

Our next-generation security platform prevents successful cyberattacks for hundreds of hospitals, clinics and healthcare networks across the globe.

Palo Alto Networks is uniquely qualified to protect patient data and safety and support regulatory compliance by providing advanced security prevention capabilities in ONE security platform.

Healthcare data has become increasingly targeted by cybercriminals while at the same time security and network staff at healthcare providers are required to:

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

With Palo Alto Networks®, you can deploy a comprehensive cybersecurity strategy throughout the organization, regardless of access point location, usage profile, type of traffic, and more. Our next-generation security platform protects complex IT environments for hospitals and clinics by providing:

What We Do

- Next-generation cybersecurity for healthcare organizations with consolidated capabilities:
  - Sandboxing
  - IDS/IPS
  - Firewall
  - URL filtering
  - Anti-malware
  - Anti-exploit protection
- Protection at all points in your healthcare IT environment:
  - Network perimeter
  - Data center
  - Endpoints (including medical devices)
  - Mobile devices
  - Cloud
- Support and demonstrate compliance with regulations that healthcare organizations must meet, such as HIPAA, PCI, and DPD
- Mitigate threats: detect, analyze and prevent threats – both known and unknown – including APTs
- Offer the same cybersecurity protection on both physical appliances and virtual machines

How We Are Different

- Application and user visibility at the firewall: automatically identify over 2000 applications, (i.e., HL7 and DICOM) and integrate with your enterprise directory
- Create true "Zero Trust" network segments, and allow access for approved applications and users rather than only IP/ports
- Excellent detection rates of malware, viruses and APTs, powered by the integrated and community-driven nature of the platform
- Efficiently process your traffic once across all security functions in a single pass, thanks to a purpose-built single-pass parallel processing architecture at speeds of up to 120 Gbps
- Seamless integration with some of the best technology providers in the industry to deliver a more holistic security approach

- Full visibility and granular control over applications, users, and content on your network.
- Ability to apply role-based access to any asset on your network.
- Detection and prevention of known and unknown threats on the network, endpoint, data center, and in the cloud.
- Effective segmentation of network zones based on asset sensitivity, access profiles and information exchanged to reduce risk and simplify compliance.
- Elimination of unauthorized traffic and applications that consume a lot of bandwidth (example: 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. Palo Alto Networks Next-Generation Security Platform is a set of natively integrated components that automate the prevention of cyberattacks.

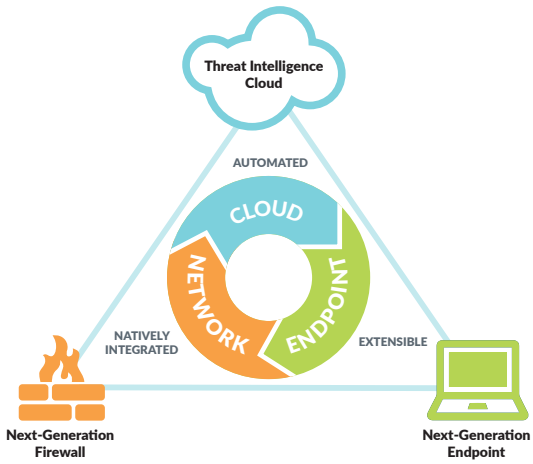

Figure 1: Palo Alto Networks Next-Generation Security Platform

There are three types of components in the platform. The network component is the next-generation firewall that inspects all traffic, detects, and safely enables applications and users. It blocks known threats and sends any unknown file or URL to the cloud (WildFire™) for inspection.

The endpoint component is called Traps™ and is a lightweight agent installed on endpoints. Only 25MB in memory, it inspects files and processes on the endpoint for both known and unknown exploits and malware. It is highly effective at protecting Windows® systems that are difficult to patch, like medical devices.

The cloud component gathers potential threats from the next-generation firewall and endpoints, analyzes and correlates threat intelligence, and distributes the threat intel back to the next-generation firewall and endpoints for enforcement.

Together, the security platform components provide healthcare providers with the visibility and enforcement capabilities to prevent cyberattacks throughout the attack lifecycle. The most common use cases for healthcare providers include:

Use Cases	Solution
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 by isolating PCI devices
Endpoint Protection	Prevent malware and exploits on unpatchable endpoints like medical devices
Data Center Protection	Provide high-speed threat protection for both physical and virtual servers
Mobile Device Protection	Enforce the same security policies on mobile devices wherever they go

Read on for more details about the most common use cases for healthcare providers.

Use Case 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 security platform is the ability to automatically detect over 2000 applications, including HL7 and DICOM traffic, and integrate with enterprise directories to identify users. User identification at the firewall makes it a lot easier to track down the location of malware-infected PCs.

The native IPS, anti-malware, anti-exploit and URL filtering capabilities in the next-generation firewall prevent sophisticated cyberattacks targeted at healthcare providers, such as APTs and advanced malware used in recent healthcare attacks like Derusbi, Sakula and CryptoWall.

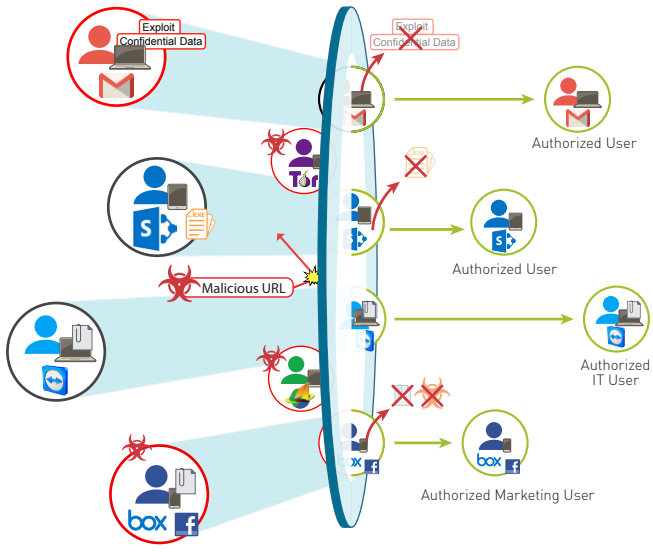

Figure 2: The Next-Generation Firewall safely enables applications, users and content

Use Case 2: Network Segmentation

Network segmentation is a highly effective strategy for healthcare providers to:

- Increase the difficulty for attackers to exfiltrate data from hospital networks.
- Reduce the scope of PCI compliance.
- Help meet HIPAA requirements related to controlling access to protected health information (PHI).
- Implement true "Zero Trust" segmentation – a cross-industry best practice.

With Palo Alto Networks, 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.

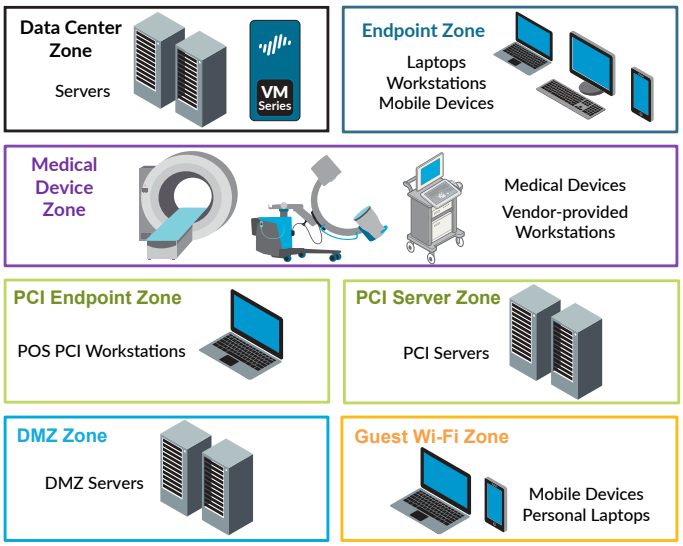

Figure 3: Example zones for segmentation in hospitals

Use Case 3: Support HIPAA Compliance

Healthcare providers manage highly sensitive patient data that is protected under regulations which differ by country. In the U.S., HIPAA outlines the minimum security requirements for managing protected health information (PHI) at covered entities. Our next-generation security platform supports numerous HIPAA Security Rule requirements at healthcare providers. For example:

1. Access Control: User identification at the firewall restricts user access to applications or zones.
2. Integrity Controls: Advanced threat prevention features maintain the integrity of PHI by preventing malware and exploits.
3. Audit Controls: Audit logging with native user identification provides access reports for systems with poor reporting capabilities that contain PHI .
4. Transmission Encryption: Application detection at the firewall directs security teams to systems using insecure protocols to transfer PHI (i.e., ftp and http).

See Appendix 1 for the full list of HIPAA requirements that are supported by Palo Alto Networks Next-Generation Security Platform.

EXAMPLE: PCI Server Zone Rules based on App-ID, User-ID

- Block and log all inbound and outbound zone traffic (Zero Trust)
- Allow only finance users in active directory (User-ID) can access PCI server zone (security group name = 'finance')
- Allow PaymentCollect (App-ID) as the only application allowed (whitelisted)
- Log high block on outbound cardholder data transfer attempts (App-ID)

Use Case 4: Decrease the Scope of PCI Compliance

Network segmentation decreases the scope of PCI DSS compliance. This means that, if you isolate your devices that process or store credit cards into a "PCI" zone, you can limit the scope of PCI DSS compliance to only that single zone, rather than the entire hospital network. The next-generation firewall identifies applications (App-ID™) and users (User-ID™), which makes it easier to create traffic rules between zones that are easy to understand and manage, compared to legacy IP/port rules.

For example, the rules listed above could be used to define connectivity between an Endpoint Zone, a PCI Endpoint zone and a PCI Server zone. Then, when you put these rules into action, the Nursing user can't access the PCI zone, but the Finance user can.

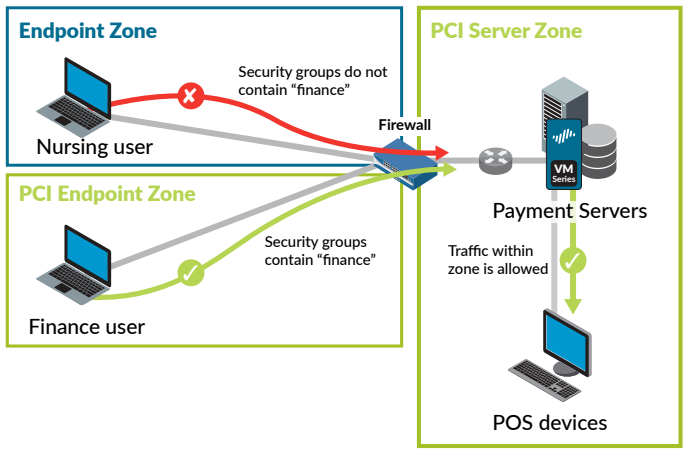

Figure 4: Defining connectivity between an Endpoint Zone, a PCI Endpoint zone and a PCI Server zone

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

Use Case 5: Protect Windows PCs that Are Difficult to Patch

Due to the highly complex nature of hospital IT environments, many IT departments struggle to patch all Windows devices across the hospital network. In addition, many medical devices are delivered to hospitals by a vendor along with a Windows-based PC. 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 at the endpoint. The

lightweight nature of the signature-less Traps agent decreases the risk to Windows workstations and servers that are difficult to patch (including Windows-based medical devices).

Figure 5: Traps protects Windows-based PCs with signature-less anti-malware and anti-exploit capabilities

Use Case 6: Mobile Device Protection

Mobile devices, such as smartphones and iPads, are extensively used by doctors and nurses for clinical services at the bedside. You can extend the same protection that Palo Alto Networks Next-Generation Security Platform provides to your deployed mobile devices with GlobalProtect™, which is natively integrated with WildFire for the detection of unknown threats, and with MDM providers like Airwatch® for easier deployment.

Deploy GlobalProtect to managed Windows laptops and deploy our VM-Series next-generation firewall to the cloud (i.e., Amazon Web Services) to achieve the same network-level threat protection whether your laptops access the Internet from inside or outside the hospital network.

Manage the Security Platform Centrally

Finally, hospital IT security and network management teams can collaborate on a single security platform with defined administrative roles to enforce the separation of duties. Our central management solution, Panorama™, makes firewall management and intelligence gathering easy. Use the native log viewer or integrate with third-party log management tools like 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 visibility and control that our prevention-oriented approach provides and how you can use our security platform to automatically stop cyberattacks in your healthcare environment.

Choose your next step:

- **Online Product Demonstration** – that we can tailor to the unique needs of your organization.
- **Ultimate Test Drive** – in which your teams can get hands-on experience with our technology.
- **Free On-site Proof of Concept** – we will help deploy our security platform in your environment without impacting hospital operations. You will receive a detailed Security Lifecycle Report summarizing the findings.

Appendix 1: How the Next-Generation Security Platform Supports HIPAA Security Rule Compliance

HIPAA Standard	Requirement	How Palo Alto Networks Next-Gen Security 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].	The Next-generation firewall integrates with your Enterprise Directory to identify users and enforce policies based on user types, job titles or security groups. 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 Name:** Assign a unique name and/or number for identifying and tracking user identity.	The 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(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 next-generation Security Platform provides robust audit logging at the user level.
§ 164.312(a)(2)(iv)	**Encryption:** Implement a mechanism to encrypt and decrypt electronic protected health information.	The next-generation firewall identifies data that is transmitted without encryption via insecure protocols (e.g., ftp, telnet). Reports enable security teams to identify systems transmitting data in the clear and remediate with strong encryption.
§ 164.312(d)	**User 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 to internal systems that contain PHI.
§ 164.312(e)(1)	**Transmission Encryption:** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	The next-generation firewall identifies data that is transmitted without encryption via insecure protocols (e.g., ftp, 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(e)(2)(i)	**Integrity Controls:** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	The next-generation security platform provides anti-malware, anti-exploit and threat intelligence capabilities that prevent threats on the network from improperly altering PHI (e.g., malware like CryptoWall).
§ 164.312(c)(1)	**Data Integrity:** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	
164.308(a)(5)(ii)(B)	**Protection from Malicious Software:** The Covered Entity must implement procedures for guarding against, detecting, and reporting malicious software.	

4401 Great America Parkway
Santa Clara, CA 95054

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

www.paloaltonetworks.com