Healthcare Cyber Defense: Protect Data and Devices, Ensure Compliance and Maintain Complete Visibility into Security Risk

From a cyber-security perspective, perhaps the most vulnerable industry is the healthcare industry, which not only treats vulnerable people but is itself extremely vulnerable.

As part of an industry that the public relies upon to literally save their lives, healthcare providers are easy targets for extortion. Having sensitive information leaked or operations shut down is not an option.

> “MANY OF THE DEVASTATING SECURITY BREACHES THAT OCCURRED IN 2017 WERE PREVENTABLE, HAD THE RIGHT TECHNOLOGY AND SOLUTIONS BEEN IN PLACE.”

THE PROBLEM

The healthcare industry is often denied hardware updates due to manufacturer regulations, and in any case has a great need for maximum medical device uptime.

Sadly, this means it was one of the hardest hit by the WannaCry attack that took down a large part of the UK’s National Health System (NHS) in May last year. In this case, computers essential for various functions, including MRI scanners, laboratory testing facilities and pharmacy needs were taken off-line leading to the cancellation of thousands of appointments and operations.

A second trend is the hacker exploiting vulnerabilities in smart devices in the hospital to enable the attack. The healthcare sector has embraced the Internet of Things (IoT) enthusiastically, with one estimate valuing the global IoT healthcare industry at over $100 billion by 2020. [1]

There are wearable medical devices, both external equipment such as insulin pumps, and implanted devices like pacemakers. Then there are stationary devices within hospitals, such as intelligent pharmacy dispensers or chemotherapy stations. In addition we find smart TVs in hospital rooms and mobile devices like tablets used by hospital staff. Too often security is an after-thought in the design of these devices in the rush to get them to market, making them easy targets. Hackers need only infect one device to then move laterally within the hospital’s networks.

Additional attack vectors include:

- Exploit the user using malicious email attachments from a “trusted” source
- Hack the USB by acting as a keyboard or other device considered “valid”
- Poison Wi-Fi networks and use man-in-the-middle attacks
- Phish vulnerable SMS (Short Message Service) apps

To sum up: there are a lot of ways to infect the patient.

THE CURE

In 2000 Bruce Schneier wrote “Security is a process, not a product. … Security processes are not a replacement for products. Rather, they're a way of using security products effectively. They're a way to mitigate the risks.” [2] Fast forward to 2010 when we see Forrester rethinking the traditional perimeter-based defense model towards a Zero-Trust model [3] where data is classified and its flow is mapped. From this “micro-perimeters” are built to only allow access to those who are authorized and from devices deemed safe. Finally improve security detection and response using security analytics and automation. Apply the model across the ecosystem to include mobile devices, apps, cloud services, social media use and third-party dependencies. [4] Then iterate.

All very high level. In practical terms how do you implement this? In Forrester’s words “What is the specific feature of the technology that enables a capability to meet the Zero Trust strategy? This is the crux of this final and most granular point of this focused framework. Any vendor who claims to offer a Zero Trust-related solution must describe how the specific feature that they offer aligns with the other levels of the framework. For example, a DLP solution may have the ability to discover and classify data. Or a NFGW vendor may have a feature that allows an administrator to manage all firewalls on all networks from a single user interface (UI).” [5]

Let’s dive into the technology. Conceptually Check Point enforcement technologies can be categorized by where they reside; on-network or on-host. On-network protections offer consolidation of security controls that can be broadly enforced at micro-perimeters or segmented network boundaries while on-host technologies provide very granular protections to the hosts or devices and the data that resides upon these devices.

On-network Protections

To ensure patients receive the emergency services they need, organizations need a solution that will not just detect advanced threats to its network, but ultimately prevent them from entering at all. This means having a solution that includes access control technologies like firewall, user identity, VPN, application control, URL filtering and Data Loss Prevention and threat prevention technologies like IPS, antivirus, anti-bot, anti-spam and sandboxing. Each has a specific capability that enables achieving the goal of Zero-Trust (see Action Plan for Healthcare Cyber Defense below).

A discussion of specific features within the technology that enables the capability to achieve Zero-Trust is beyond the scope of this document. That said, to prevent Zero-day and advanced threats healthcare providers should certainly ensure they have sandboxing technology that has CPU-level exploit detection capabilities. This will enable them to extract active content from documents, delivering a cleansed document while the file gets checked in the background, at no cost to the organization’s smooth operations. In this way, they can block malware designed to bypass regular sandboxing technologies, and maintain their security against advanced threats such as WannaCry.

In addition, healthcare providers should try to minimize the complexity of their networks, and attempt to keep the distinct software versions used to a minimum, and monitored from a single user interface. At enforcement points implement IPS as a virtual patching technology. This will make it easier to keep their systems up to date and monitor the threat landscape as well as implement security patches in a timely manner.

Finally, to protect IoT devices, thorough discovery and awareness of what is connected within the healthcare environment needs to be known. Only then can proper segmentation of these devices, and proper access policies, be carried out. This will enable prevention of potential attacks to maintain the integrity of the data that these devices hold and the operations that they perform.

On-host Protections

On-host protections can be further broken down into two device types; endpoints running Windows and macOS and smart devices running iOS or Android.

ENDPOINTS RUNNING WINDOWS OR MACOS

The weakest link in most organizations are endpoints and the users who use them. This is not an indictment of the user, but is simply the nature of today’s threat landscape where targeted spear phishing and waterhole attacks are very difficult for the end user to detect. Mobile laptops either containing or having access to sensitive PII or PHI information are especially vulnerable when used

off-site. HIPAA finds that 2017 was a banner year for data breaches of 500 or more records, "the main causes of healthcare data breaches is now hacking/IT incidents, with unauthorized access/disclosures also commonplace". [6]

To mitigate these risks, businesses implement endpoint security, but this can challenge security administrators in multiple ways. Different risks and groups require different tools to manage and enforce endpoint and corporate policies. Managing all these aspects requires more of your admin's time, effort, and thinking to execute well. Having one console enables security administrators to easily manage multiple enforcement capabilities. The solution must also integrate well with existing antivirus and security analytics tools to decrease remediation times.

In its Endpoint Security Suites evaluation Forrester positions Check Point as a leader. "Check Point offers a fully featured, traditional suite with modern updates. With its roots in network security, Check Point has expanded into other areas such as endpoint and mobile security over the years and today delivers an endpoint security suite that includes threat prevention, detection, data security, endpoint management, and mobile security. The product ships with multiple signatureless detection capabilities for malicious file/behavior, with tight integration to share policy and threat intel between the company's endpoint, network, and cloud offerings." [7]

Endpoints are protected with Threat Emulation and Threat Extraction. Anti-Ransomware technology stops ransomware in its tracks and reverses the damage automatically. Anti-Bot technology identifies and blocks command & control activities and forensics enables complete attack remediation and delivers automated incident analysis, uncovering the entire attack scope and business impact. This works in conjunction with antivirus from other vendors to enhance the detection capabilities of existing antivirus products.

In addition most corporate laptops and PCs store proprietary data on their drives, and many users regularly work outside of a secure corporate environment. A data breach from a lost, stolen or compromised laptop can result in costly fines, lawsuits and lost revenue. Full Disk Encryption secures the entire drive while Media Encryption and Port Protection secure removable media on these devices.

SMART DEVICES RUNNING IOS OR ANDROID

Verizon found that 35 percent of healthcare orgs reported data loss or downtime from a mobile device security incident in the past year. Eighty-seven percent of healthcare respondents said mobile devices were a risk, while 29 percent said the devices were a significant one. Even with those concerns, 41 percent of healthcare organizations stated they have knowingly sacrificed security for expediency or business performance. "Healthcare has the unenviable task of guarding large amounts of highly sensitive and personal data, while also providing quick access for medical practitioners," report authors wrote. "These risks need to be weighed against speed and accessibility. Complicated or unwieldy access systems could do more harm than good, especially in emergency situations." [8]

Check Point SandBlast Mobile addresses these concerns while protecting mobile devices from advanced attacks. End-user privacy is critical, so SandBlast Mobile never analyzes files, browser histories, or application data. SandBlast Mobile determines if a device is compromised by analyzing the behavior of the operating system, apps, and connected networks. App analysis is performed in the cloud to avoid impacting device performance. Since device protection runs automatically in the background, SandBlast Mobile delivers a user experience that is both elegant and unobtrusive.

Here's how our solution works: An agent called SandBlast Protect is installed on a user's Android or iOS device. The solution captures apps as they are downloaded to devices, and runs each in a virtual, cloud-based environment to analyze its behavior before being approved or flagged as malicious. SandBlast Mobile detects malicious network behavior and conditions, blocking man-in-the-middle attacks over Wi-Fi and cellular networks, phishing attacks, communications with command and control servers, and assures that only safe sites are browsed to. The solution also identifies vulnerabilities in operating systems and apps that may be exploited. Finally, mobile device policy is set and monitored in a web-based management dashboard, allowing an organization to constantly evaluate the security posture of its mobile fleet.

When SandBlast Mobile is paired with market-leading UEM solutions like Airwatch, Blackberry, MaaS360, MobileIron, Microsoft Intune and Citrix XenMobile, then users get an added critical security layer that can be used to dynamically change access privileges to reflect risk levels and transform static management policies into dynamic mobile threat defense.

Security Management

An integrated solution is needed to protect against advanced persistent threats and zero-day attacks, and at the same time, help the organization uphold HIPAA and PCI DSS 3.2 compliance while maintaining complete visibility into operations. Check Point central security and event management and open APIs control across all networks and cloud environments, increasing operational efficiency and lowering the complexity of managing your security.

Our SmartEvent consolidates monitoring, logging, reporting and event analysis functions within the same console. This means you can easily move from tracking trends to investigating and mitigating events with just a few clicks. If you are worried about a new malware that is making the rounds, our free-text search lets you quickly see if any instance of it was discovered on your network. Need to send reports to your manager or auditor? It's very simple to set up custom reports in SmartEvent. Already have a security analytics tool? We also integrate the major SIEM vendors such as Splunk, IBM, LogRhythm, McAfee, ArcSight and RSA.

With too much work and too little staff, security teams need to work smarter. Automation and granular delegation are key to helping alleviate operational overhead. With our open APIs, security teams can automate any task or create web portals for security self-service. Other efficiency elements include features built into the management interface to anticipate the daily needs of an administrator, providing security intelligence to make better policy decisions. Concurrent administration allows multiple administrators to work simultaneously on the same policy without conflict.

Healthcare is a highly regulated industry. Our built-in Compliance monitors management and security gateways to constantly validate that your Check Point environment is configured in the best way possible, providing 24/7 security monitoring, security alerts on policy violations, and out-of-the-box audit reports. Audit and compliance reporting with simple HIPAA based reports can be sent directly to managers and auditors, enabling organizations to reduce the time and costs associated with proving that each specific configuration setting is defined correctly. In addition we integrate with the major firewall auditing and change control solutions such as AlgoSec, Firemon and Tufin.

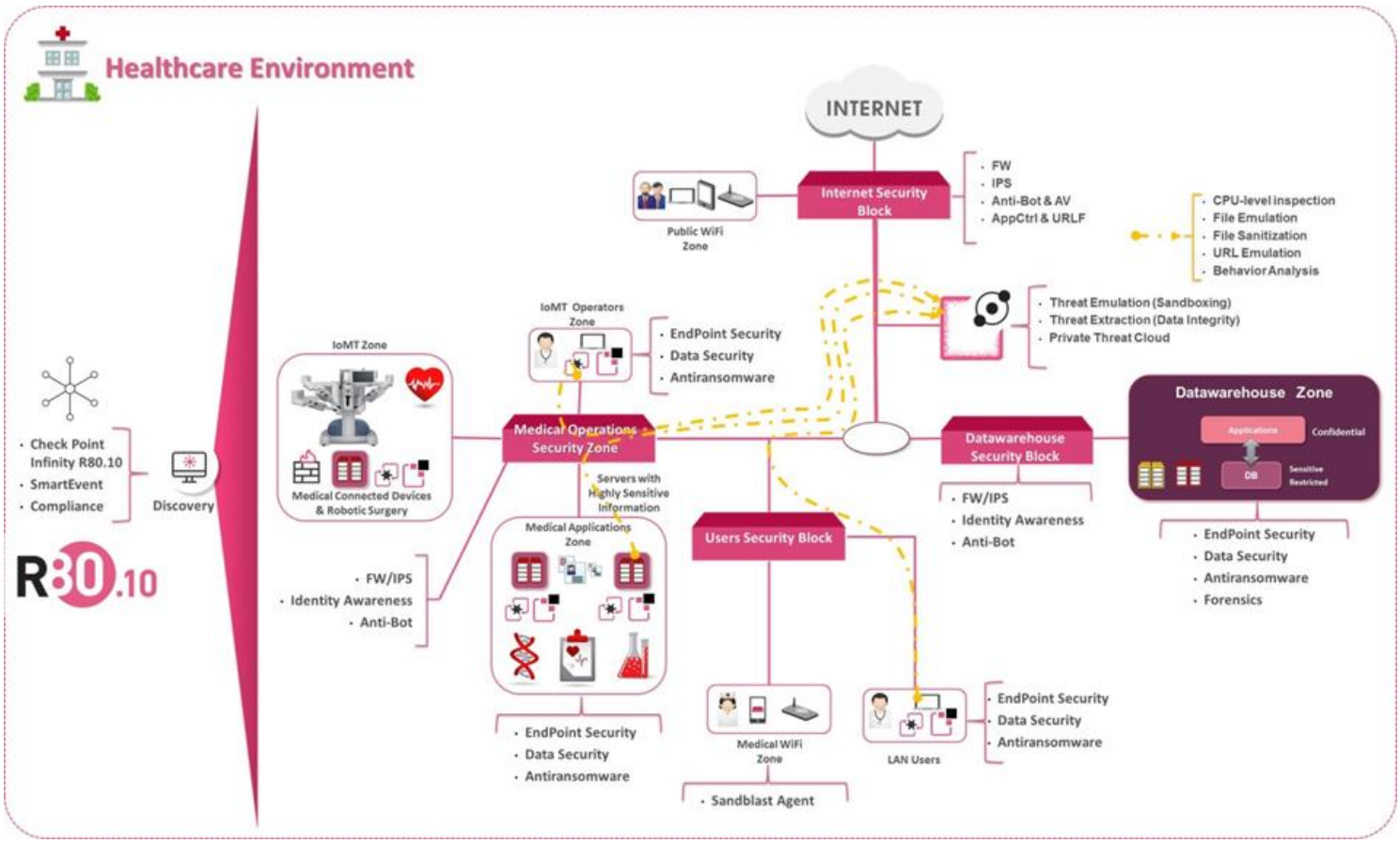
THE PROGNOSIS

We know these threats are real. Perhaps one of the biggest lessons we can learn is that many of the devastating security breaches that occurred in 2017 and so far in 2018 were preventable, had the right processes, technology and solutions been in place.

Thinking of security as a process for using security technology effectively can mitigate risks to you as a healthcare provider and more importantly to safeguard your patient's data. First identify your highly personal and sensitive data, map your operational flows, implement least privilege access at on-network and on-host boundaries as needed and monitor with solutions that integrate well together – then iterate to ensure your plan is working as it should.

An ounce of prevention is worth a pound of cure. Rethinking your approach to security can help you stop something from happening in the first place which is easier than repairing the damage after it has happened. To protect against today's threats, you need intelligent technology that keeps up with the threat landscape – technology that can detect and block both known and unknown threats, technology that can be deployed across your entire ecosystem, as well as comply with regulations and give you complete visibility into the security operations of your company. Check Point's integrated solution for healthcare allows your company to be proactive in its approach to security, rather than reactive.

APPENDIX: ACTION PLAN FOR HEALTHCARE CYBER DEFENSE



Healthcare Security Zones

In healthcare environments we often find these security zones. Not shown are cloud services or public and private cloud platforms.

Internet Security

- Organization outbound access to the Internet and B2B
- Inbound access to hosted applications and web services
- Outbound guest Wi-Fi access

Data Warehouse Zone

- Access to application servers
- Stores confidential and sensitive data

Users Zone

- Operational access via a LAN from desktops
- Operational access via Wi-Fi from mobile devices and laptops

Medical Operations Zone

- IoT medical devices sub-zone
- IoT operators sub-zone
- Medical applications sub-zone

Healthcare Cyber Defense Plan

1. Classify data
   - Data classification should define what categories and criteria the health organization will use to classify data and specify the roles and responsibilities of employees within the organization regarding data stewardship.

2. Create micro-perimeters and enforce only what is allowed
   - Segment and isolate all medical devices and sensitive servers from the corporate and users network according to the categories defined in the data classification.
   - Network and endpoint segmentation needs to consider grouping components for Internal, Confidential, and Public zones selecting the appropriate security controls.
   - Network segments need to integrate at least three technical security controls: Firewall, Intrusion Prevention System and Identity Awareness.
   - Rule-Based threat prevention (IPS, Antivirus, Anti-Bot) to provide accurate Virtual Patch management for legacy systems and End-of-Life applications.
   - All operations computers, especially that handle medical devices, should be segmented.
   - Data servers with sensitive information should be isolated
   - Business sensitive documents must be encrypted to ensure that contents are protected wherever they go ensuring access for authorized users only.

3. Deploy technologies to achieve Zero-Trust
   - Deploy Identity-Based security rules, Role-based Access Control (RBAC) policy defined around roles and privileges based in the Data Classification groups, providing authenticated access from specific users to the medical devices.
   - Deploy Data Loss Prevention measures to block potential sensitive data exfiltration.
   - Deploy anti-ransomware on computers connected to the IoT devices and servers that store patient data.

4. Verify and Iterate

On-Network Protections

Technology	Capability to Achieve the Goal of Zero-Trust
Firewall	Limit network access to only allowed services and allowed network segments
Identity Awareness	Limit access to users with the proper credentials and to only those who are authorized access
IPsec and SSL VPN	Protect data while in transit and ensure end-to-end communications are private and confidential
Application Control	Limit access to approved applications and enable and educate users on safe use of the Internet
URL Filtering	Limit access to approved sites and enable and educate users on safe use of the Internet
Data Loss Prevention	Protect personal healthcare information (PHI), personally identifiable information (PII), financial data
IPS	Enable virtual-patching of network services and applications that may be vulnerable to exploits
Antivirus	Prevent known malware
Anti-Bot	Detect and block bot behaviors and communications with known Command and Control servers
Anti-Spam	Detect and block known email sources of spam
Sandboxing	Inspect files for malicious content and behaviors
Threat Extraction	Deliver safe content to users while files are analyzed in the background

On-Device Endpoint Protections

Technology	Capability to Achieve the Goal of Zero-Trust
Sandboxing	Inspect files for malicious content and behaviors
Threat Extraction	Deliver safe content to users while files are analyzed in the background
Anti-Bot	Detect and block bot behaviors and communications with known Command and Control servers
Anti-Phishing,	Identify and prevent access to new and unknown phishing sites targeting user credentials
Anti-Ransomware	Prevents cyber-extortion attack and automatically reverses any damage done to files from the attack
Automated Forensics	Monitors and records all endpoint events: files affected, processes launched, registry changes, network activity
Full Disk Encryption	Secures all information on endpoint hard drives including user data and Operating System files
Media Encryption	Enforces encryption of removable storage media
Port Protection	Enables central management of all endpoint ports plus centralized logging of port activity

On-Device Smart Device Protections

Technology	Capability to Achieve the Goal of Zero-Trust
Sandboxing	Inspect apps for malicious behaviors to detect Zero-day malware
Infected App Detection	Monitors all apps installed on protected devices
Configuration Analysis	Monitors all configuration changes on the device to detect weaknesses or rooting that may lead to compromise
Wi-Fi Attack Detection	Validates the integrity of SSL connections to detect compromises and MitM attacks
Anti-phishing	Detects and blocks malicious URLs sent to the device
Safe Browsing	Prevents access to malicious websites
Conditional Access	Control access to corporate resources from compromised devices
Anti-Bot	Detect and block bot communications with known Command and Control servers

Management, Security Analytics, Automation and Integrations

Technology	Capability to Achieve the Goal of Zero-Trust
Unified Console and Policy	Security for physical, virtual networks, on premise or cloud gateways is fully unified under the same console
Automation	Connect security to IT processes and systems across your network with our web services APIs
Logging, Threat Management	Centrally monitor the status of your enforcement points and send logs to major SIEM vendors
Dynamic Policy	Connect to virtual cloud environments to automatically update policy and logs as these cloud objects change
Delegation	Segmented policies that can be independently managed make it easy to operationalize security
Compliance	Built-in compliance and integration with the major firewall auditing and change management vendors
Threat Indicators	Automate imports of IoCs via STIX formatted files
Identity	Integrate with major 3rd party Identity Access Management providers to enforce RBAC
Mobile Device Management	Integrates with major 3rd party vendors to dynamically change access privileges based upon risk level

In essence, our healthcare solution stresses a centralized approach comprised of five components:

- Prevent targeted and zero-day threats with SandBlast Zero-day Protection on the network, endpoints and mobile devices
- Protect data with on-network data loss prevention, endpoint full disk and media encryption and port protection
- Comply with HIPAA, GDPR and PCI DSS 3.2 with built-in Compliance and integrations with 3rd party software
- Consolidate monitoring, logging, reporting and event analysis with SmartEvent and 3rd party security analytics
- Protect mobile devices running iOS and Android with a light-weight, unobtrusive SandBlast Mobile app

REFERENCES

[1] MarketResearch.com: IoT Deployments in Healthcare to Reach $117 Billion by 2020, April 2015, https://www.prnewswire.com/news-releases/marketresearchcom-iot-deployments-in-healthcare-to-reach-117-billion-by-2020-says-new-mind-commerce-report-300070129.html
[2] Bruce Schneier, Schneier on Security, The Process of Security, April 2000, https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html
[3] Mary K. Pratt, CSOonline, What is Zero Trust? A model for more effective security, January 2018, https://www.csoonline.com/article/3247848/network-security/what-is-zero-trust-a-model-for-more-effective-security.html
[4] Forrester Research, Five Steps To A Zero Trust Network, December 14 2017, https://www.forrester.com/report/Five+Steps+To+A+Zero+Trust+Network/-/E-RES120510
[5] Forrester Research, The Zero Trust eXtended (ZTX) Ecosystem, Jan 16 2018, https://www.forrester.com/report/The+Zero+Trust+eXtended+ZTX+Ecosystem/-/E-RES137210
[6] HIPAA Journal, Healthcare Data Breach Statistics, https://www.hipaajournal.com/healthcare-data-breach-statistics/
[7] The Forrester Wave™: Endpoint Security Suites, Q2 2018, https://www.forrester.com/report/The+Forrester+Wave+Endpoint+Security+Suites+Q2+2018/-/E-RES137973
[8] Verizon, Mobile Security Index 2018, February 2018, http://www.verizonenterprise.com/verizon-insights-lab/mobile-security-index/2018/

CONTACT US
Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-628-2177 | www.checkpoint.com