



The Ransomware Treatment Plan

+++++

The healthcare industry is in a unique and particularly vulnerable position when it comes to cybersecurity. Healthcare organizations face a high level of regulation and compliance surrounding patient privacy and data protection. And at the same time, they are a preferred target for cybercriminals due to the high residual value of healthcare records. Let's take a closer look at why healthcare is at risk, and ways to address these escalating threats.

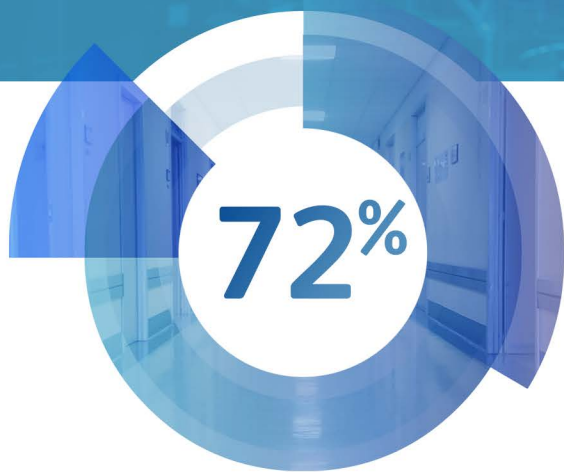


Ransomware is on the Rise

While there are many IT security risks, ransomware has been dominating the malware market—evolving to become the most profitable malware type in history. And cybercriminals have their sights on healthcare:

- Campaigns targeting healthcare organizations are becoming more widespread and potent
- Faster, more effective, and more sophisticated propagation methods maximize the impact
- Costs of restoring systems compromised by ransomware may be greater than the cost of paying the ransom





Healthcare is More at Risk

Ransomware accounted for 72 % of healthcare malware attacks in 2016¹

+++++

And here's why:



Many healthcare organizations operate on outdated, disparate systems that are vulnerable to attacks



There is a shortage of cybersecurity talent



Medical records are a rich source of complete personal profiles, and healthcare data breach costs are more than 2.5 times the global average across industries²

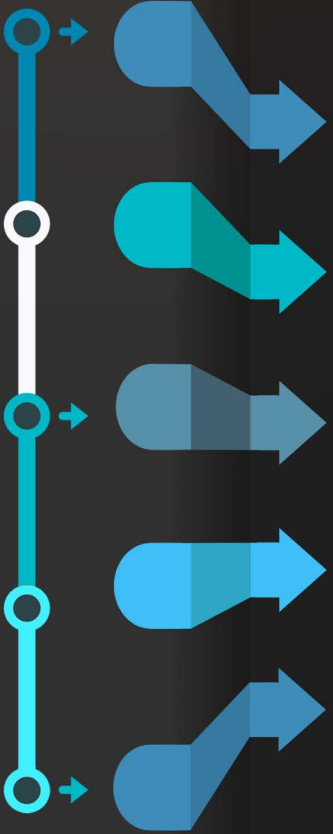
- The average healthcare data breach cost is \$380 per record vs. the \$141 average global cost per record for all industries.²
- Stolen health credentials can go for about 10 or 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cybercrime protection company³

Sources:

- 1 Healthcare IT News April 27, 2017
- 2 2017 Cost of Data Breach Study, Ponemon Institute
- 3 HealthIT Security

Unique Demands Create Further Obstacles

Unfortunately, the bleak news continues. Additional factors contribute to the already precarious situation for healthcare as it relates to IT security:



Healthcare organizations are constantly expanding their operations model, bringing more services and applications closer to patients with remote care, remote clinics, and online services as well as sharing big data across their distributed networks.

Pharmaceutical companies need to secure their intellectual property, potentially worth billions of dollars.

Insurance providers are required to accommodate data exchange with countless providers, agencies, and brokers with exploitable potential security gaps.

The “Internet of Medical Things” introduces new threat vectors and pushes even more data into the network.

A myriad of federal, state, and local cybersecurity regulations introduce more complexity and compliance requirements, raising the stakes with substantial penalties for violations.

Security Is a Brand Issue

100+ DAYS

2,400+ HOURS*

+++++

That's the average time it takes for most organizations to know they've had a data breach. Think about the amount of financial and patient data that can be compromised. And then think about how that affects your hospital's reputation.

- Lost credibility, trust, and prestige
- Increased patient risk
- Impact on top-line revenue and profitability

* As of November 2017



What Should You Do? ⁺⁺

With a growing attack surface, escalating threats, complexity of environments, and outsourced services and partner-providers, a new approach to cybersecurity for healthcare is needed. One that is:

Broad:



Cybersecurity that covers the entire attack surface through industry-leading solutions and technologies that collaborate, scale, and deliver protection across the entire network including endpoints, access points, applications, and the cloud.

Powerful:



Cybersecurity that can meet the bandwidth demands of the underlying network infrastructure without affecting network performance.

Automated:



Proactive cybersecurity that can quickly respond to threats with all security elements exchanging real-time threat intelligence and coordinating actions.

ePlus and Fortinet:

A Team of Security Architects



ePlus' team of security architects provides a full suite of services for healthcare to:

- Review and evaluate pre-existing security controls and environments
- Identify proper calibration to prevent / detect
- Strengthen security controls through Security Awareness Training, Vulnerability Assessments, Penetration Tests, End Point Controls Assessment, System Hardening, Incident Response Exercises, Restoration Strategies, Security Infrastructure, Application Whitelisting, and Egress Whitelisting
- Optimize your Fortinet deployment and strengthen your defenses against ransomware attacks



Consultative Services

ePlus' consultative services and team of experts, combined with the industry-leading Fortinet security fabric that provides protection from the edge to the cloud, deliver the security and performance healthcare providers need in today's threat landscape.

ePlus and Fortinet: A Partnership for Your Protection

With ePlus and Fortinet working hard on your side, we can help you assess, design, implement, and monitor a comprehensive security program to address your unique concerns and strengthen your security posture.

+++++



Fortinet meets the varied and critical security needs of today's healthcare organizations worldwide without sacrificing performance through integrated and scalable solutions that offer security effectiveness and deliver third-party validated performance.

By design, the different parts of the Fortinet Security Fabric work collectively to address the threat trends that today's enterprises face.

1. Enterprise Firewall: Core firewall and security management platform, providing internal segmentation, next generation firewall and security operations
2. Cloud Security: Virtual security solutions for public and private cloud deployments
3. Advanced Threat Protection: High performance detection, mitigation, and prevention security solutions with rapid global intelligence to impede the volume of ransomware and other advanced threats
4. Application Security: Robust and integrated set of products to protect web applications, databases, and email systems
5. Secure Access: Solutions that secure the access layer, including mobile devices, users, WLAN/SD-WAN, and the Internet of Things
6. Security Operations: These tools help to manage, monitor, and report on multiple fabric components from a single control point



Protect your Patients and your Organization

+++++

Contact ePlus today to learn how you can leverage Fortinet network security solutions to protect your patients' medical records and stay ahead of today's escalating ransomware threats.

www.eplus.com/fortinet
888-482-1122
healthcare@eplus.com

©2017 ePlus inc. All rights reserved. ePlus, the ePlus logo, and all referenced product names are trademarks or registered trademarks of ePlus inc. All other company names, product images and products mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2017 Fortinet, Inc. All rights reserved.