WHITE PAPER

# Healthcare Providers are Suffering from Ransomware Epidemic

## Integrated Security is the Critical Care They Need

## No Respite for Medical Organizations during Global Pandemic

The past few years have been extremely tough for healthcare providers. If the global pandemic wasn't challenging enough, the healthcare industry has been experiencing additional pain and suffering from an epidemic of ransomware attacks.

When the pandemic burst onto the scene in early 2020, cybercriminals saw the COVID-19 crisis as an opportunity to increase ransomware attacks on vulnerable healthcare organizations. While the world was distracted by rampant disease and death, attackers showed no mercy on healthcare organizations—like thieves ransacking the firehouse, while the firefighters were out battling blazes.

Taking advantage of the disruptions caused by the pandemic, cybercriminals increasingly targeted organizations in the healthcare sector. In October 2020, the U.S. Cybersecurity and Infrastructure Security Agency, the Department of Health and Human Services, and the FBI issued a joint advisory, warning U.S. hospitals and healthcare services of increased ransomware activity involving TrickBot and BazarLoader malware.[2]

Healthcare organizations have always been an attractive target for cybercriminals and their attacks have had serious consequences. Therefore, the massive increase in volume and sophistication of ransomware must be immediately addressed. With ransomware, attackers can take down entire systems and cut off computer access for essential services. Most concerning is the impact a successful attack can have on patients and their ability to access care.

"Average weekly ransomware activity across our sensors in June 2021 was, in fact, 10.7x higher than levels set one year ago."[1]

"A recent global ransomware survey also showed that 67% of organizations have been a ransomware target—with nearly half saying they had been targeted at least twice."[3]

## How Ransomware Targets the Healthcare Industry

With the rapid increase in ransomware attacks, any healthcare organization that hasn't yet been targeted probably will be soon. While the healthcare industry is disproportionately attacked by ransomware, cybercriminals also use it to attack every industry and every size organization around the globe.

Like most malicious software, ransomware can gain access to a system in multiple ways, often with just a click—or even no click at all. It can be distributed via digital means, including email, website attachments, business applications, social media, and USB drives. Phishing email remains the most prominent delivery vector, baiting victims with tempting hyperlinks and/or attachments.

## Targeting OT and IoMT

Traditional ransomware goes after data, locking files until the ransom is paid. With the emergence of Internet-of-Things (IoT) devices, a new strain of ransomware has emerged. It doesn't go after an organization's data, but instead targets control systems (e.g., vehicles, manufacturing assembly lines, power systems) and shuts them down until a ransom is paid. In the healthcare industry, cybercriminals are attacking Internet-of-Medical-Things (IoMTs) in the same way.

Healthcare organizations have hundreds of operational technologies and IoMT devices in play—everything from patient monitors to imaging devices to infusion pumps to even HVAC systems. Any of these connected devices can be hacked to gain access to a healthcare organization's critical information systems.

## What's Behind Ransomware's Staggering Growth

Ransomware grew over 1,000% between July 2020 and June 2021.[4] While several high-profile incidents have grabbed international headlines, the impact is also being felt by tens of thousands of organizations worldwide.

The top three reasons for its staggering growth are:

- Ransomware-as-a-Service (RaaS)
- Extraction of increasingly larger ransoms from big targets (aka "Big Game Hunting")
- Threats to disclose compromised data if demands aren't met

**Ransomware-as-a-Service.** Tools like Ransomware-as-a-Service and selling the names of companies that have already been compromised have commoditized the criminal process. A novice cybercriminal, acting as a sort of franchisee for a cybercriminal organization, can now successfully target healthcare organizations with little or no technical skills.

All the back-end processes, from target acquisition to pricing, to collecting funds, are offered as a service—for a fee—by sophisticated criminal enterprises that even provide help-desk services for their criminal cohorts.

**Big Game Hunting.** The recent enormous paydays that ransomware has delivered to attackers have been broadly discussed in the news and online forums. This has triggered a "malicious goldrush" on vulnerable organizations and industries by both veteran and aspiring cybercriminals.

Threat actors study their targets before launching an attack. Once they enter the victim's network, they may spend months searching for the high-value data that will result in an exorbitant ransom payment.

"Big game hunters" pursue organizations that are particularly sensitive to an extended downtime ruining their businesses and/or reputations. Cybercriminals know these enterprises are much more likely to pay bigger ransoms. Consequently, healthcare, manufacturing, technology, and financial services industries are frequently targeted for attacks.

**Data exposure.** One of the most troubling aspects that has come with the latest ransomware attacks is data exfiltration and the threat to release that data if a ransom is not paid. The use of data theft became a feature of many ransomware attacks in 2021. The operators of most major ransomware strains—including Sodinokibi, Ryuk, Egregor, and Conti—all deployed data exfiltration as part of their standard operations.


"Colonial Pipeline paid $4.4 million to DarkSide, the Russian threat actor behind the attacks, to regain control of its pipeline… JBS, the world's largest meat processor, raised the specter of a similar disruption to meat supplies across the US…paid $11 million to attackers to resolve the issue."[5]

"At least 39 ransomware groups have attacked the healthcare sector across 27 countries in the past 18 months."[6]

Some ransomware victims reported incidents where attackers falsely claimed theft of data and then tried to scare them into paying a ransom. In other cases, when victims paid to get attackers to delete stolen data, the attackers reneged and instead leaked or sold the data anyway. Even worse, we have seen ransomware destroy a victim's network by wiping the disks of desktops and servers—despite having paid a ransom!

For healthcare organizations, this is a perfect example of why even robust data backups alone are not enough protection against ransomware demands.

## How Best to Defend Against Ransomware Attacks

The Cyber Kill Chain® framework, developed by Lockheed Martin, is a model that identifies seven steps that attackers must complete in order to be successful. The seven steps are:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on Objectives

By using the steps as a guide, the IT security teams of targeted organizations have a good understanding of any attacker's tactics and a better idea on how to defend against attacks.

Clearly, healthcare providers and their CISOs need to design, build, and install better defenses against ransomware, especially as attacks become more frequent and harmful. IT security managers must deploy protections that get ahead of ransomware and shield organizations before, during, and after an attack—and that all "talk to each other."

Many mature enterprises already have incident response plans, but to reduce the risk and scope of potential threats, other proactive strategies also need to be implemented. When an organization is in the middle of a ransomware attack, it's too late to put the proactive strategies, processes, and technologies in place to stop the damage.

Obviously, planning and preparation before an attack occurs is always smart. Another wise move is having a comprehensive overall security strategy that includes processes and integrated security controls at each stage of the kill chain.

### An integrated approach

To effectively protect against ransomware, an integrated approach is required. While there is a wide range of security technologies available to reduce the risk and impact of ransomware, if they are not working together, there will be many gaps for criminals to attack through.

Regardless of their pedigree and features, individual point products alone will never provide the prevention, detection, deception, and response that a fully integrated system does. Therefore, in addition to evaluating the effectiveness of network, email, sandbox, web, and endpoint security controls individually, it is essential to look at how they can work together—how they mesh—to provide stronger, faster, and more manageable protection from ransomware.

This is where the Fortinet Security Fabric comes in. Powered by FortiOS, it is the industry's highest-performing cybersecurity platform. It has a rich open ecosystem. And it spans the extended digital attack surface and cycle, empowering self-healing security and networking to protect devices, data, and applications.

## Fortinet's Security Products, Services, and Training

To reduce the risk of a ransomware attack, healthcare organizations need to deploy the right mix of security controls to thwart delivery, shield vulnerabilities from exploits, prevent installation, block execution, cut off external communication, and contain lateral movement.

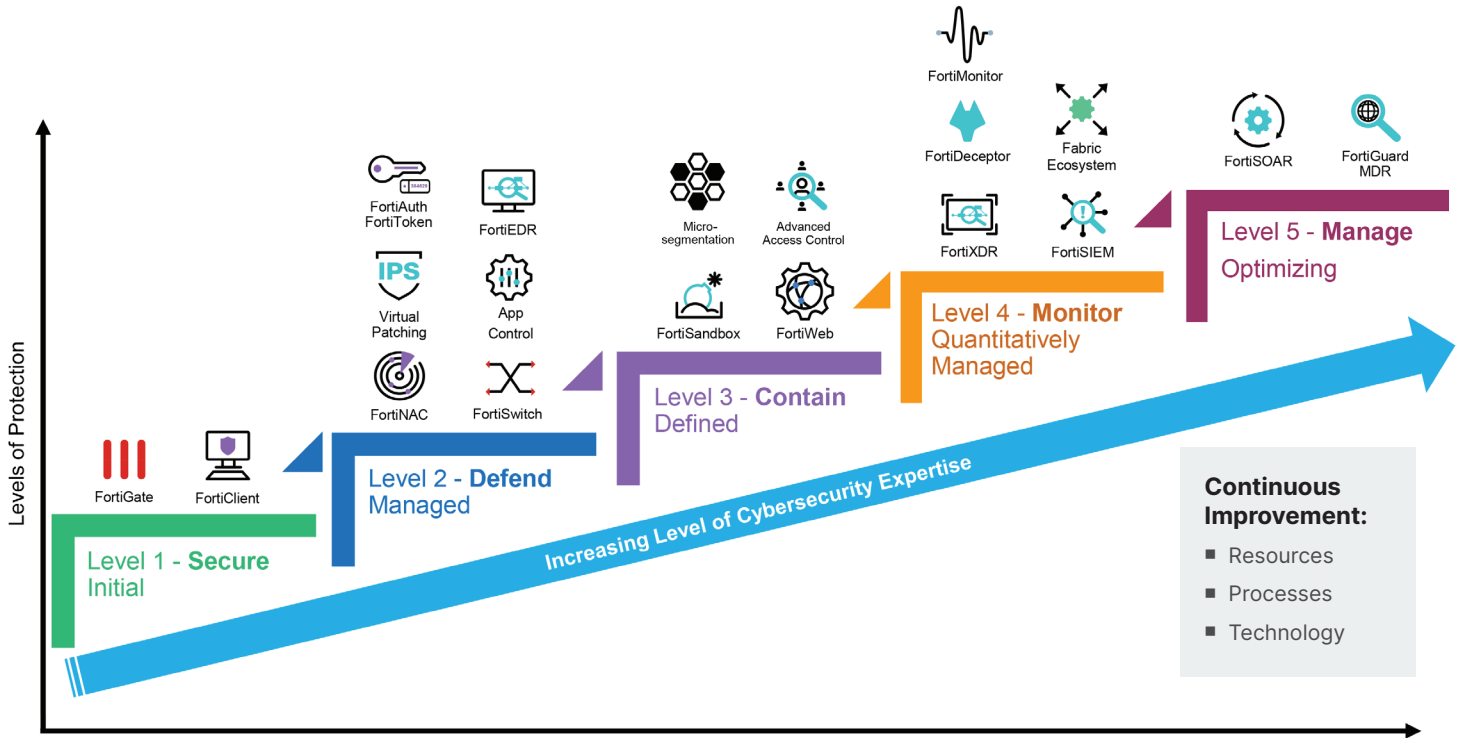


Figure 1: Cybersecurity Maturity Scale applied to Fortinet's portfolio of solutions.

## Fortinet Solutions

The key Fortinet solutions that mitigate ransomware attacks include:

- **FortiGate** (NGFW) provides inspection of encrypted traffic, web filtering, and intrusion prevention (IPS).
- **FortiEDR** proactively reduces the attack surface, prevents malware infection, and detects and defuses potential threats in real time. Customizable playbooks automate responses and remediation procedures.
- **FortiDeceptor** uses deception technology to engage attacks in progress and slow their spread.
- **FortiSandbox** leverages two machine-learning models that enhance static and dynamic analysis of threats.
- **FortiMail** brings powerful antispam and anti-malware capabilities complemented by advanced techniques like outbreak protection, content disarm and reconstruction, sandbox analysis, and impersonation detection.
- **Fortinet's Professional Services Organization and Managed Detection and Response (MDR)** provides expert assistance for architecture planning, playbook setup, threat monitoring, forensic investigations, remediation services, etc.

## Smart Cybersecurity Solutions Can Ensure Patient Care Continuity

The Fortinet Security Fabric is a portfolio with products for every level of cybersecurity maturity. We are unique in having an integrated approach with the broadest set of security products, services, and training to reduce the risk of a ransomware incursion at all stages of the cyber kill chain.

Unlike competitors, our solutions all "talk to each other" and process real-time threat intelligence, detect threat patterns and fingerprints, correlate massive amounts of data to detect anomalies, and automatically initiate a coordinated response.

Our portfolio features two of the most important solutions needed to prevent ransomware damage. One is FortiEDR that delivers automated, real-time response critical to address advanced threats that target endpoint devices. The other is FortiDeceptor that deploys a fake network as a decoy for ransomware and can immediately detect malicious activity and slow down the encryption process while leveraging other security tools to automatically limit or prevent damage.

The Fortinet Security Fabric integrates unique technologies to stop ransomware and protect critical assets. We have a proven track record helping healthcare organizations of all sizes secure their networks—and patients.

For more information or to speak to one of our healthcare cybersecurity experts, contact us at: healthcare@Fortinet.com.

[1] Global Threat Landscape Report, A Semiannual Report by FortiGuard Labs, FortiGuard Labs, August 2021.

[2] Ransomware Activity Targeting the Healthcare and Public Health Sector, Cybersecurity and Infrastructure Security Agency, November 2, 2020.

[3] Global Threat Landscape Report, A Semiannual Report by FortiGuard Labs, FortiGuard Labs, August 2021

[4] Ibid.

[5] Ibid.

FORTINET

www.fortinet.com



March 7, 2022 11:01 AM

1419356-0-0-EN