# Healthcare cyber resiliency strategy: Beyond cyber recovery

## Cyber and ransomware attacks are the enemy of today's data-driven healthcare organizations

Healthcare organizations today are working with highly sensitive patient information where maintaining the security and integrity of their data is of the utmost importance. Furthermore, many care providers may need to work in remote locations, like ambulances and mobile clinics, where secure network connections are essential. Challenges abound, from finding and retaining knowledgeable security professionals, to interpreting fragmented data from disparate security products, to standing up 24x7 security operations.

Cyber attacks have become a serious and continuous threat to businesses of all sizes and verticals. Even though global ransomware attacks fell almost 25 percent in the first half of 2022, continuing the downward trend that has been observed for the previous four quarters, this is not the case for the healthcare industry, which saw a 328 percent increase in attacks during the same period.[1] Cyber attacks disrupt operations, damage reputation and can result in lawsuits related to data protection regulations. However, in healthcare, these attacks can have life threatening consequences—about 70 percent of the care providers facing ransomware attacks said that it led to longer hospital stays for patients

1. HIPAA Journal - Ransomware Attacks Drop by 23% Globally but Increase by 328% in Healthcare: hipaajournal.com/ransomware-attacks-drop-by-23-globally-but-increase-by-328-in-healthcare/

**328%**

**increase in attacks targeting healthcare orgnaizations in the first half of 2022.[1]**

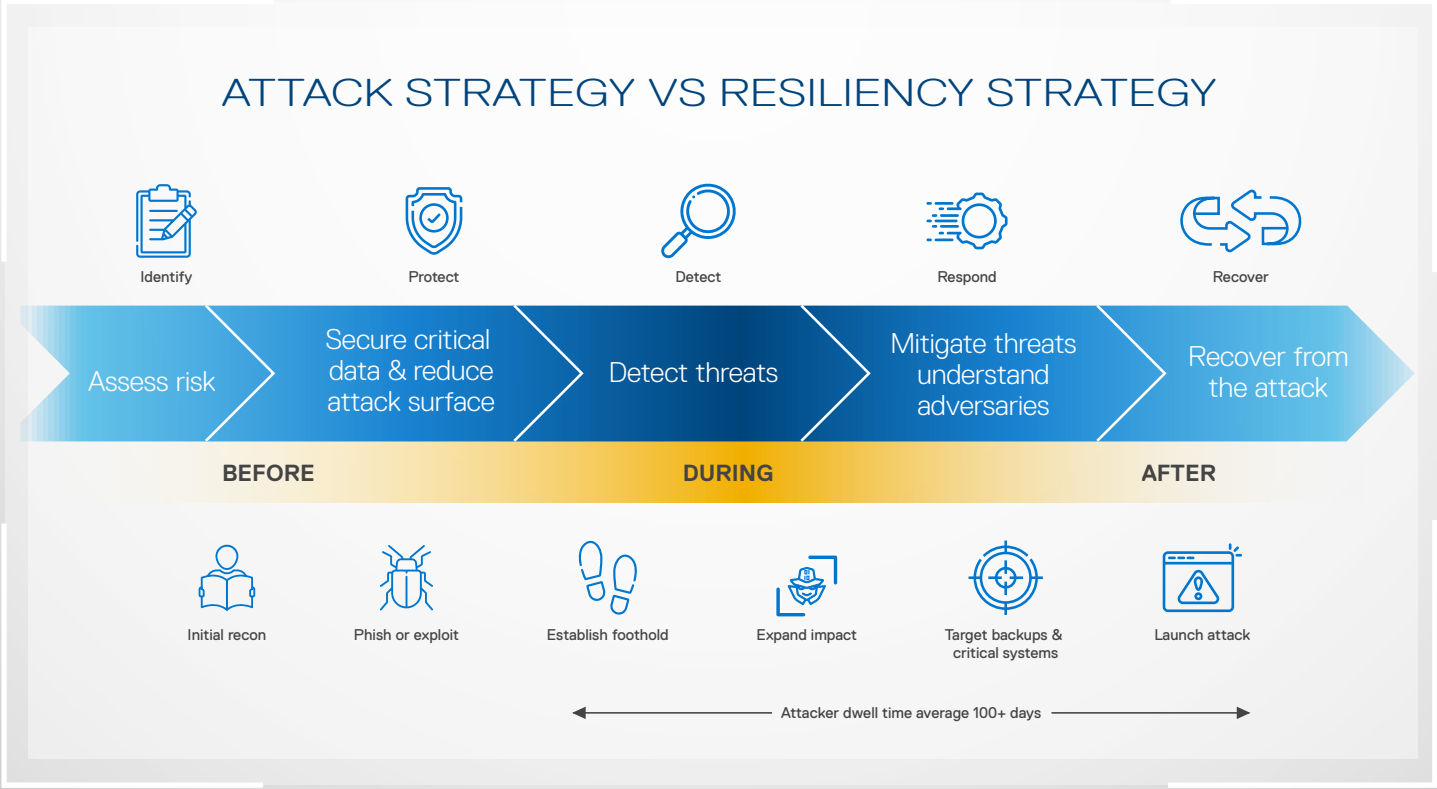
and delayed tests or procedures. In addition, almost 25 percent said they had increased death rates.[2] In this rapidly-evolving—and escalating—threat landscape, organizations need to keep ahead of the threat vectors and adopt more advanced security solutions, without bogging down their IT or productivity. While 100 percent immunity is not practical, IT organizations can do a lot to significantly improve the cyber resiliency of the systems to protect business-critical data and setup systems for faster recovery of business operations. Stopping attacks before damage is done requires quick and effective threat detection and response.

In addition, digital transformation demands we supplant manually intensive practices with automation and insights that drive better business results. And with accelerated digital transformation, coupled with pandemic-driven labor shortages, it's a great time to consolidate security tools and utilize security services experts to help relieve your already strained security personnel.

## Secure care: healthcare cyber resiliency as a comprehensive strategy

Before we discuss specific capabilities to help you enhance cyber resiliency, let's clarify what we mean when we use the term resiliency. It's important to note that resiliency is not a technology; it is a strategy, or better yet, an outcome. Think of it as a "ready state" for withstanding attacks that is the combined result of planning, technology, and discipline so that healthcare technology teams know exactly how they're going to act when a breach is discovered. Many care providers don't think past cyber recovery to the necessity of a complete and mature cyber resiliency program. While cyber recovery is an important part of cyber resiliency, there is an entire emerging discipline about what it means to be cyber resilient.

Following the industry-standard NIST framework of "Identify, Protect, Detect, Respond and Recover," you can see how Dell Technologies lines up our resiliency strategy before, during and after a cyber attack. The rest of this brief provides more information on the key solutions for each of these three phases.




2. theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients/

# BEFORE A CYBER ATTACK

### Data and threat protection: Cyber resilient healthcare multicloud data protection

The first step in fortifying with modern security is to rethink how healthcare organizations protect data and systems. While there are literally thousands of providers of threat management security software, Dell Technologies brings two unique advantages to these solutions with significant incremental value—intrinsic security features and a holistic presence across the ecosystem.

The first big advantage Dell provides is that we start with devices and processes that are designed for security as a baseline. Preexisting intrinsic security features in the hardware, the firmware, and the security control points provide an architectural foundation that is ahead of the game. Dell delivers incremental value with intrinsic security features built into its platforms and internal processes. As a global leader in IT technology for decades, Dell has had many years to drive intelligent innovation for security deep into our product designs and processes. Our customers utilize our hardened devices and processes for an intrinsic advantage.

The second advantage Dell brings to security solutions, is the holistic vantage point for security. Dell as a core-to-edge-to-cloud IT provider, can offer solutions across the IT spectrum. This integrated approach is not something many providers can claim. It all starts with a trusted infrastructure. Since Dell Technologies is a global leader in cloud, IT, and mobile infrastructure, our platforms for virtual compute, network, and storage technologies are sitting under an enormous portion of the world's workloads and applications, so we're already a huge part of IT security systems. This gives us a unique perspective, and advantage, for addressing security holistically.

We develop intrinsically secure infrastructure platforms and devices that enable healthcare providers to generate and process vast amounts of data, while making sure IT assets are secure, protected and available.

### Zero trust: modern healthcare security needs zero trust

The path to Zero Trust looks different for every healthcare and life sciences organization and it is a complex journey to implement this architecture. Dell Technologies is committed to simplifying the adoption of Zero Trust by streamlining integration across the full range of healthcare technology environments.

Dell Technologies created an accelerated approach to protecting Microsoft ecosystems using Zero Trust principles, Microsoft solutions and our security expertise. Our Identity and Endpoint Protection with Microsoft Zero Trust services are designed to quickly help organizations understand their current security posture and priorities to achieve Zero Trust alignment, then provide the expert guidance, implementation services, adoption and change management strategies to drive secure outcomes.

Dell data and threat protection, along with zero trust solutions, help care providers and academic research organizations to build cyber resilience to be as well prepared against cyber- attacks as possible.

**70%**

**of care providers facing ransomware attacks said that it led to longer hospital stays for patients and delayed tests or procedures.[2]**

**THERE ARE THREE COMPONENTS IN DELL'S ZERO TRUST REFERENCE MODEL:**

1

Zero trust should be defined and driven by business controls, or business rules, about what systems should do.

2

Business controls should be converted to technology and action, which can be done via a control plane that consists of identity management, policy management and threat management tools.

3

Make sure that only known, authenticated entities are allowed on the infrastructure and well-defined policies define known good behavior – embedding threat detection across the ecosystem.

## DURING A CYBER ATTACK

### Managed detection and response: Detect and respond to threats across your organization

Responding to modern threats takes the latest approaches which bring together the tools and a team of experts to better identify, respond and mitigate threats in real-time. Turning to Dell's managed security services is a proven way that customers are extending their constrained resources and reducing complexity. And having access to Dell's team of certified security experts, who use the latest AI-based capabilities, strengthens their security posture, helping them confidently address the most pressing threats.

Beyond selecting a modern threat detection and response solution, it's imperative to choose a provider with expertise in operationalizing the solution in the healthcare sector. This helps ensure you're provided with not only with 24x7 threat detection and investigation, but also with response and active remediation, along with an in-depth understand of the healthcare and life sciences industry. While building these managed services, Dell focused on these capabilities specifically because of their value in helping customers better manage their security operations and enhance their cyber resiliency.

Dell Technologies Managed Detection and Response utilizes Secureworks Taegis™ XDR software to monitor, detect, investigates and automate response to threats across the entire IT environment, applying analytics gleaned from threat data across thousands of customers.

Dell also assists customers in deploying Taegis XDR security controls and integration of technologies across their data sources. When a threat arises, expert security analysts investigate and provide recommended actions and step-by-step instructions to contain and remediate them.

**25%**

**of care providers facing ransomware attacks said patient death rates also went up following the attack.[2]**

Designed for organizations with 50 endpoints or more, this service combines the power of the Taegis XDR security analytics platform and the expertise of Dell Technologies security analysts, gained throughyears of helping care providers worldwide to better protect their businesses.

Dell data and threat protection, along with Zero Trust solutions, help healthcare and life sciecnes organizations build cyber resilience to be as well prepared against cyber-attacks as possible.We help secure healthcare technology environments across endpoints, network and cloud by using our open cloud-native platform that combines the power of human intellect with insights from security analytics to unify detection and response.

## AFTER A CYBER ATTACK

### Dell PowerProtect Cyber Recovery: Proven and modern protection for critical data from ransomware and destructive cyberattacks.

To reduce business risk caused by cyberattacks and to create a more cyber resilient approach to patient data protection, healthcare organizations can modernize and automate their recovery and business continuity strategies and leverage the latest intelligent tools to detect and defend against cyber threats.

Dell PowerProtect Cyber Recovery provides proven, modern and intelligent protection to isolate critical data, identify suspicious activity and accelerate data recovery allowing you to quickly resume normal business operations. Leveraging automation, machine learning identifies suspicious activity and allows healthcare organizations to recover known good data and resume normal business operations with confidence. It also includes protecting and isolating critical data from ransomware and other sophisticated threats in a cyber vault.

### Cyber Recovery vault: automated data copy and air gap

The Dell PowerProtect Cyber Recovery vault offers multiple layers of protection to provide resilience against cyberattacks even from an insider threat. It moves critical clinical and business data away from the attack surface, physically isolating it within a protected environment and requires separate security credentials and multifactor authentication for access. Additional safeguards include an automated operational air gap to provide network isolation and eliminate management interfaces which could be compromised. PowerProtect Cyber Recovery automates the synchronization of data between production systems including open systems and mainframes, and the vault creates immutable copies with locked retention policies. If a cyberattack occurs healthcare technology teams can quickly identify a clean copy of data, recover critical systems and data  and get care facilities back up and running in order to treat their patients.

## Secure Care - comprehensive security for clinical and business staff, network, endpoints, data and recovery

Dell Technologies understands that today's security challenges include managing an evolving threat landscape with a modern work environment in mind. Cybercriminals are leveraging sophisticated attacks to target multiple vulnerabilities—with an increasing focus on Protected Health Information (PHI). As a result, an effective security strategy must address the entire attack surface.

At Dell, our vision for Secure Care is that it should be holistic, intelligent and scalable, spanning the entire healthcare organization with consistent objectives and policy application. Dell Technologies will stop at nothing to be your trusted, end-to-end security partner, and has positioned itself to be an industry leader in providing holistic, scalable and intelligent security solutions.

With cyber resiliency that includes built-in protection, continuous innovation and intelligence, and automation, healthcare and life sciences organizations can advance their digital transformation goals and thrive in the data era.

Connection
we solve IT

**Contact your Connection Account Team for more information.**

| Business Solutions | Enterprise Solutions | Public Sector Solutions |
|---|---|---|
| 1.800.800.0014 | 1.800.369.1047 | 1.800.800.0019 |

www.connection.com/Dell

DELL Technologies



C2923239-0125