opentext™ | Cybersecurity

Building cyber resilience with layered security

How healthcare providers can achieve cyber resilience to ensure compliance and security

Introduction

In 2023, one in three Americans, over 100 million people, were affected by a medical data breach[1]. The average cost to healthcare providers of a data breach rose to almost US$11 million[2]. This explosion in the scale of the threat is happening against a backdrop of rapid digital transformation.

By 2026, American healthcare providers will spend almost US$30 billion a year on digitizing their workflows, their supply chains, and their patient interactions [3]. These investments are a response to changing business needs, with customers increasingly demanding a digital or hybrid customer experience.

But this rapidly expanding digital footprint makes providers more vulnerable than ever to cybercrime, at exactly the time when the volume of that crime is exploding. To avoid regulatory, reputational, and other types of risk, the healthcare sector needs a way to defend itself.

The answer is defense in depth, using a multi-layered system of healthcare cyber resilience. A layered approach to security minimizes the attack surface the organization exposes to cybercriminals, maximizes the protection against unauthorized access of data breaches. It also gives the business the greatest possible flexibility and resilience in its response and recovery to any cyber incident.

In this ebook, we explain how a layered approach to security can give your organization the edge over cybercriminals and a head-start in the market. We cover the technologies you need to protect your patients and your business. We explain how market leaders are using those technologies to safeguard their investment in digital transformation — and more.

1. https://www.chiefhealthcareexecutive.com/view/health-data-cyberattacks-have-affected-more-than-100-million-people-in-2023
2. https://securityintelligence.com/articles/cost-of-a-data-breach-2023-healthcare-industry-impacts
3. https://www.insiderintelligence.com/insights/healthcare-industry

Contents

Executive summary

Today, healthcare providers are digitizing at breakneck speed, spending billions to transform both their business and their clinical workflows. Protecting this investment has never been more important.

Any data breach or unplanned downtime risks damage to the provider's reputation, its digital infrastructure and operating model. Healthcare providers also face significant regulatory and financial risk, with the prospect of state and federal authorities imposing hefty fines for avoidable data breaches.

Because of this, it's never been more important for healthcare providers to protect themselves against cybercrime and other more physical or natural threats to their digital infrastructure.

But it's also never been harder to achieve this. The volume and the complexity of threats are growing and multiplying all the time. Whether it's the rise in ransomware or the increasingly sophisticated attacks via social engineering, security has never been more complex.

The best way to overcome this challenge, and deliver market-leading protection, is with a defense-in-depth approach that relies on a sophisticated, layered security strategy The layers of a modern security strategy include:

- **Prevention:** combines technology such as endpoint and DNS protection with robust security-awareness training to stop threats before they even reach your network.
- **Protection:** with email protection, encryption, and continuity, you can minimize the risk of threats damaging devices and systems or causing downtime.
- **Recovery:** with sophisticated backup and failover, as well as SaaS and business continuity measures, you harden your resilience and minimize time to recovery.

These layers go together with training to sustain a culture of security awareness among all colleagues. And they work best when underpinned by a single, unifying layer of management control and intelligence that gives access to all the cybersecurity data and tools they need through a consolidated platform.

OpenText Cybersecurity is a market leader in intelligent cybersecurity for healthcare providers. Through Secure Cloud, it gives companies a control panel of advanced cyber security tools, including email encryption and protection, endpoint security, software-as-a-service (SaaS) backup and information archiving.

Layered security at a glance

Prevention

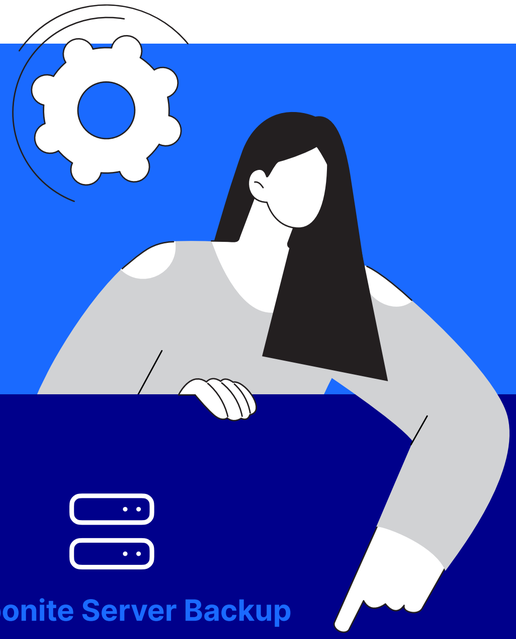
Securing your devices, your people, and your domain name services

- Webroot Endpoint Protection
- Webroot DNS Protection
- Webroot Security Awareness Training

Protection

Securing your communications and all corporate data

- Webroot Advanced Email Encryption powered by Zix
- Webroot Advanced Email Threat Protection and Email Continuity



Recovery

Protecting your data and business continuity

- Carbonite Recover
- Carbonite Cloud-to-Cloud Backup
- Carbonite Server Backup

management control

Why does healthcare need to think cyber resilient?

As we've already seen, cyberattacks on healthcare organizations hit an all-time high in 2023 [1]. And 80% of data breaches at US healthcare providers happen because malicious actors can take advantage of gaps in an organization's security [4].

Across the healthcare sector in the US, the incidence of most types of cybercrime remained high:

- **Between 2018 and 2023, the volume of ransomware attacks doubled [5].**
- **In recent years, the volume of cyberattacks on US hospitals has doubled [6].**
- **Phishing and advanced email attacks increased by almost 170% [7].**
- **77% of US healthcare providers say supply-chain attacks threaten patient care [8].**

Of all the sectors in the US economy, healthcare is one of the most vulnerable to cyber threats. According to the FBI, healthcare organizations were hit with more ransomware attacks in recent years than any other critical sector [9].

To protect patients, practitioners and their business model, healthcare providers must mitigate cyber risks. The more digitized healthcare becomes, the more exposed it is to the cybersecurity threats. The answer is to move from protecting just the network edge to a layered protection model.

4. https://securityintelligence.com/news/hacking-caused-80-of-2022-healthcare-data-breaches
5. https://www.fiercehealthcare.com/health-tech/new-jama-study-scrapes-dark-web-find-true-frequency-healthcare-ransomware-attacks
6. https://www.weforum.org/agenda/2023/05/cyber-attacks-on-healthcare-rise-zero-trust/
7. https://healthitsecurity.com/news/advanced-email-attacks-skyrocket-in-healthcare
8. https://www.fiercehealthcare.com/health-tech/supply-chain-email-attacks-against-healthcare-groups-frequently-threaten-patient-care
9. https://www.chiefhealthcareexecutive.com/view/fbi-healthcare-hit-with-most-ransomware-attacks-of-any-critical-sector

The fastest route to the right security expertise

The best way to do that is to partner with a technology provider that delivers a comprehensive, integrated security approach — protecting business networks, clinical infrastructure, patient data, and more.

The partner should have extensive experience working with healthcare providers and a management platform that accommodates a layered security approach. This will enable you to streamline and automate policies, permissions, and business rules across the workforce.

Through a single pane of glass, your security administrators should be able to manage organization-wide security measures, apply real-time threat intelligence and security status updates across the IT infrastructure. They should have instant access to the tools they need to prevent data breaches and protect assets wherever they are — in the cloud, on site, at remote locations, or in workers' homes.

And if there is a cyber security incident — whether it's a breach attempt by a cybercriminal or simply a natural or man-made incident that impacts business continuity — your IT staff should have all the tools they need to recover and minimize downtime, through the same consolidated platform.

The prevention layer

Prevention, as the saying goes, is better than the cure. With the right systems and the right methodology, it's possible to detect and intercept most cyber-threats before they lead to a data breach, a loss of service, or a deterioration in patient care.

To achieve this, you must invest in a market-leading prevention layer — and the knowledge and methodologies that make the technologies of which that layer is composed, work. Examples of the prevention-layer technologies and supporting measures include:

- **Endpoint protection:** dynamically protects endpoints from malicious files, scripts, URLs and exploits via a cloud based architecture.
- **DNS protection:** intelligent DNS protection filters even encrypted DNS traffic — for roaming and network users — thus preventing them from accessing inappropriate websites.
- **Security awareness training:** prevents criminals from taking advantage of your employees to gain access to networks and data, with frequent and automated training campaigns.

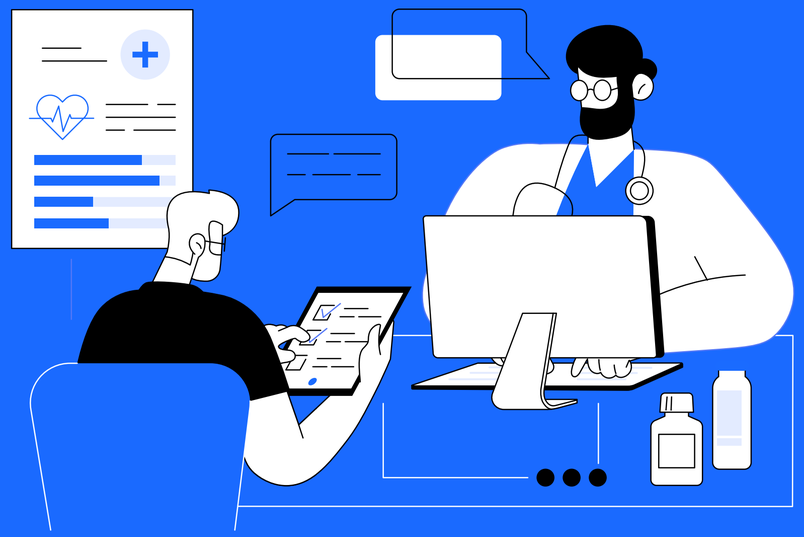
Prevention technologies must be supported by a security culture. That's why training — ensuring employees understand how to avoid threats and how to best use prevention-layer technology — is essential. But culture and prevention-layer tech aren't enough on their own. Both need to be underpinned by an intelligent layer of coordination.

Threat intelligence platforms, harnessing artificial intelligence (AI), should power the prevention-layer technologies with the data they need to understand what 'normal' looks like, across a range of different contexts. This enables them to instantly spot and stop developing threats in real-time.

The same underlying assistive layer should give IT staff instant access not only to prevention-layer technologies, but also to complementary technologies from other layers, all through a single control panel. So, when a threat is detected, your IT team can coordinate the response across all domains, rapidly, and without limitations.

The protection layer

The next part of any defense-in-depth system is the protection layer. If a threat can penetrate the prevention layer, the protection-layer technologies kick into action. They neutralize that threat before it can damage your technology assets or your business.



Examples of the protection-layer technologies and supporting measures include:

- **Email threat protection and email continuity:** analyze messages' links and attachments for malware, and even control who can forward or reply to messages.
- **Email encryption:** protect sensitive, confidential data with industry-leading easy-to-administer encryption that's invisible to users and requires no extra training.

Using the same single pane of the glass they use to manage their prevention-layer technologies, your IT team can instigate cloud back-up procedures to prevent unplanned downtime.

And the same real-time threat data that underpins prevention-layer technologies, along with advanced heuristics, allows protection-layer technologies to detect malicious links, attachments and other payloads. They then prevent them from executing, keeping your systems and data safe.

In an era of hybrid working, the protection-layer ensures that every node, network segment and potential vector of attack is continually watched over and safeguarded by advanced security technologies. This is true whether any given device, software or system is on the network edge, inside it — or on mobile.

The recovery layer

Adding a recovery layer to your defense-in-depth architecture is crucial to achieving and maintaining cyber resilience. In practice, the prevention and protection layers will catch most incoming threats. But relying on just the first two layers alone is risky.

Without robust recovery technologies the organization cannot protect itself against ransomware, fire, flood, power outages and other natural or man-made disasters. It is also open to the charge that it isn't complying with best practice and regulatory requirements.

Examples of the recovery-layer technologies and supporting measures include:

- **SaaS application continuity:** build data resilience into SaaS applications and other off-site services to protect yourself against loss due to unplanned downtime.
- **Cloud-system recovery:** back-up local or cloud servers, manage your backups and recover specific data or entire systems.
- **Disaster recovery:** continually updated, live copies of your critical servers and systems, ready for instant failover in just a few minutes.

As with the other layers, these technologies should be available through a single control panel. The IT team should be able to seamlessly track any developing issue through the different tools and systems available to them, all through a single interface.

When they decide it's time to recover data or systems, or to switch entirely to a disaster-recovery backup, they should be able to do so quickly, with minimum overheads. This is only possible when all the relevant control systems are unified in a single, easy-to-use interface.

OpenText Cybersecurity: building the cyber resilient organization

OpenText Cybersecurity is a new breed of provider. Our tools offer a layered security approach — including prevention, protection, recovery, and more.

The cyber security tools and services provided include but are not limited to:

Webroot Endpoint Protection: secure your PCs, desktops, clinical devices, and other endpoints against even the most sophisticated malware and cyber-attacks.

Webroot Advanced Email Threat Protection & Email Continuity: secure inboxes and systems by dynamically detecting threats in links and attachments.

Webroot DNS protection: block threats at a domain level, with policy-based, advanced DNS protection that even protects encrypted DNS traffic.

Carbonite Server Backup: a secure, continuously updated backup for critical servers, for rapid recovery and near zero downtime.

Webroot Security Awareness Training: education to prevent risky employee behaviors that can lead to IT related security compromises.

Carbonite Cloud-to-Cloud Backup: protect critical data stored on cloud and SaaS platforms, with this automated, encrypted, and secure cloud-to-cloud backup.

Webroot Advanced Email Encryption powered by Zix: run industry-grade encryption in the background, without disrupting workflows or requiring user input.

Carbonite Recover: failover to an up-to-date backup in just minutes, and a few clicks. With this continuously updated, running backup of critical server systems.

Most of these solutions are available in OpenText Secure Cloud: a single-pane-of-glass platform through which to monitor and control all your security services, across the prevention, protection, and recovery layers. It gives your IT teams real-time cyber intelligence and all the tools they need to protect your business, your reputation, and your investment in digital transformation.

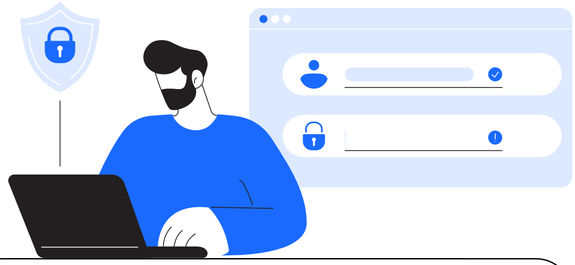
OpenText Cybersecurity provides clients across all business sectors, on six continents, with market-leading protection. In 2022, OpenText Cybersecurity helped clients reduce rates of malware infection to just a fifth of what they were in 2020 [10]. Our experts help businesses. from across the globe and many different sectors build industry-leading cyber resilience, based on intelligent, layered protection.

opentext™ | Cybersecurity

10. https://www.opentextcybersecurity.com/threat-report

A sample business: Healthcare insurance company

Let’s explore how a hypothetical business with sophisticated, complex, and demanding requirements can benefit from a layered approach to security.



In healthcare, companies require a high level of well-documented cyber security. Failure to comply could mean severe penalties under HIPAA and other relevant laws.

An insurance company with 500 staff will need to regularly exchange high volumes of sensitive and personal data with hospitals, clinics, patients, and a range of other entities.

Working with OpenText Cybersecurity allows the insurer to handle, exchange, and store data in a way that complies with regulatory standards and best practice:

With Webroot Security Awareness Training, the company educates workers to recognize and avoid threats, across all relevant channels.

Using Webroot Endpoint Protection and Webroot Advanced Email Encryption powered by Zix, the company secures sensitive and regulated data both at rest and while it’s in transit.

Using Carbonite Server Backup, the insurer secures their data and serves against ransomware and downtime, providing near instant failover when needed.

The company uses Webroot DNS to prevent threats reaching the many devices on its highly distributed and decentralized network.

By using Carbonite Cloud-to-Cloud Backup, the insurer has peace of mind, knowing that even severe disruption won’t cause downtime that could harm patients and the business.

Technicians use the OpenText Secure Cloud to track and manage developing threats. The platform puts all the cyber-security tools they need at their fingertips, so they can respond instantly.

opentext™ | Cybersecurity

Next steps

Achieving layered cyber defense in depth need not be a time-consuming process or one that involves prohibitive upfront overheads. With the right approach, the right technology, and the right partner, you can start the process of adopting layered security today.

OpenText Cybersecurity is a new breed of provider with extensive experience of working with healthcare providers. Our experts can help you understand what mix of technologies you need to become cyber resilient and protect your investment in digital transformation.

Contact OpenText Cybersecurity today, to begin your journey toward smarter and simpler cybersecurity.
https://go.zixcorp.com/Email-Security.html

About OpenText

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio.

Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, compliant experience, and simplified security to help manage business risk.

opentext™ | Cybersecurity

opentext™ | Cybersecurity