HEALTHCARE CYBERSECURITY

12 Ways To Thwart Healthcare IT Cyberattacks and Data Breaches

ManageEngine

Table Of Content

01

Healthcare challenges: This too shall pass

From the coronavirus to climate change, it's impossible to chalk out solutions to systemic threats faced by humans on a global scale without the aid of modern medicine. As we make major breakthroughs within months instead of years, we realize that operational challenges in the healthcare industry also keep evolving. From adopting cyber-security and digital transformation to reimagining public health and healthcare delivery, we must ask if the healthcare industry has what it takes for sustained growth that could vastly improve our lives. In this e-book, we'll be focusing mainly on the challenges in healthcare information technology and operational technology, the cousins IT and OT. IT refers to computer technology, including the hardware and software, and primarily focuses on data. OT, in contrast, deals with the processes and devices which, in a healthcare environment, often include legacy and disparate on data. OT, in contrast, deals with the processes and devices which, in a healthcare environment, often include legacy and disparate equi-pment. We'll analyze the current state of healthcare IT and look at ways to minimize the risks of cyber threats towards the goal of delivering seamless, secure health-care services.

02

Major IT hurdles faced by the healthcare sector

- What challenges does an IT admin in healthcare face?
- Security incidents
- Data breach risks patient privacy and sensitive business information
- Lack of network visibility
- Adapting to digital transformation
- Dealing with Compliance

Minimizing Security Incidents

Security incidents in healthcare range from ransomware attacks crippling hospital IT systems to the compromising of patient privacy, such as through a breach of personally identifiable information. Beyond these harmful operational disruptions, evolving cyberattack strategies in recent times have created serious impacts. ***The first documented death due to a cyber-attack happened in September 2020 when a Hospital in Germany was under a ransomware attack and was unable to take in a 78-year attack and was unable to take in a 78-year old female patient suffering from an aneurysm.***

The reason: a failure in the digital systems responsible for coordinating the medical teams and hospital beds. By the time she could be admitted to another hospital, it was too late.

Curbing Data Breach

In the healthcare and pharma sector, there are two specific groups that are primarily targeted by hackers. One is the customers, aka the patients, and the other is the healthcare vendor or organization. Both groups have their own set of sensitive data and resources that can be accessed and tampered with. A significant chunk of data is also stored and maintained by multiple vendors who process the data on the hospital's behalf. With so many variables, and the data

stored and processed by multiple entities, it becomes hard to map and secure it.

Lack of visibility into the hospital's IT/OT network

Apart from IT assets, such as computers, laptops, and mobile devices, the hospital's network also consist of OT systems and devices, such as HVAC systems, patient monitoring systems, equipment used in intensive care units, and so on. The use of smart devices and IoT devices has also spiked as more devices are integrated and connected with each other. With so many different types of devices in the network, an IT admin might not have a complete understanding and the tools to cater to all devices, resulting in IT blind spots. These network blind spots are basically the dark areas that are neglected, but play a major role in the hospital IT/OT systems. Things might get worse when there's a merger or acquisition, as organizations struggle to gain a solid understanding of the behavior of the network, data, and applications. In the process, more blind spots can result.

Curbing Data Breach

In the healthcare and pharma sector, there are two specific groups that are primarily targeted by hackers. One is the customers, aka the patients, and the other is the healthcare vendor or organization. Both groups have their own set of sensitive data and resources that can be accessed and tampered with. A significant chunk of data is also stored and maintained by multiple vendors who process the data on the hospital's behalf. With so many variables, and the data stored and processed by multiple entities, it becomes hard to map and secure it.

Adapting to digital transformation and disruptive innovation

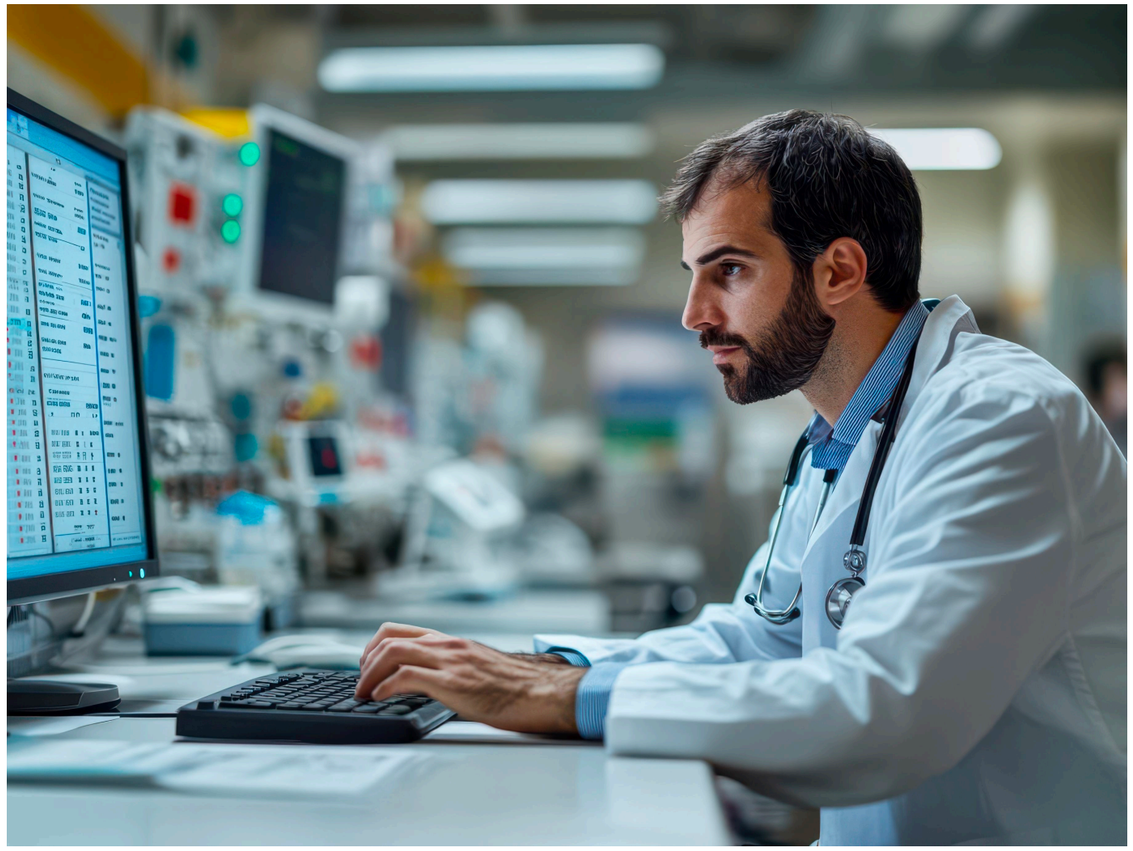
While the healthcare industry is massively driven by innovation, it also has a bad reputation for being the sector that's most vulnerable to cyberattacks. The average cost of a healthcare data breach stands at $9.8 million, more than finance sector, which ranked second in terms of data breach costs.

As hospitals and medical teams try to embrace new life-saving technologies and transformative practices, they also risk leaving their critical infrastructure unguarded at the whims of intruders and threat actors.

The Third-Party Breach Report found that the healthcare industry was the most targeted victim of cyberattacks in 2023 at 33%. But the investment to accommodate new technologies can be a huge limiting factor to organizations looking to adopt digital transformation.

Compliance and regulatory bodies

Most healthcare organizations see compliances, like HIPAA, as roadblocks. In reality, these compliances are more like guardian angels that help organizations deal with ePHI in a safe and secure manner, away from the prying eyes of cybercriminals. Though it might be a challenge to enforce regulatory bodies' stringent policies, the result is worth all the hassle.



03

Analyzing and learning from healthcare exploits in the recent past

A typical healthcare ecosystem is comprised of multiple IT and OT systems ranging from computers and servers to niche devices such as bedside monitors and ventilators. As hospitals modernize their infrastructure and utilities with innovative devices and smart IoT solutions, they also risk exposing these assets to various attackers and threat actors. According to the 2023 Cost of a Data Breach Report compiled by the Ponemon Institute, healthcare organizations experienced the highest average cost of a data breach.

Average cost of a healthcare data breach in:

$9.77 million in 2023.

Healthcare is the sector most prone to cyberattacks, followed by financial services

After understanding the nature of the cyberattacks occurring in the healthcare landscape, some of the common sources of the breaches can be attributed to:

- Compromised business email
- Unauthorized access
- Data theft
- Ransomware
- A hacked network server
- Phishing
- Unsecure server/ database

Instead of diving into the what and how of every cyberattack above, which can be performed with a simple Google search (or by checking out this article), let's try to reduce the risk posed by these vectors and safeguard your IT against cyberattacks

04

12 Ways to Minimize Cyberattacks in Healthcare

1. Enable Zero Trust

Zero Trust is a network defense model deployed to restrict access to the network and applications. It's a network model based on the premise that no one should be trusted. Zero Trust network access (ZTNA) considers every network device hostile until it is proven to be trustworthy, which is contrary to the traditional network approach that considers a device trustworthy once it passes the security layer. ***The ZTNA approach of "trust no user or entity by default" can be applied to VPN and proxy services, and to other services that rely on trust between the client and server.***

2. Enforce MFA

Multi-factor authentication (MFA) is a way to add another layer of security to verify an identity during the sign-in process. With MFA enabled, users will have to authenticate themselves in two or more ways to access their organization's information. That way, even if an employee's password is compromised, their other authentication will prevent threat actors from logging in. These additional authentication factors are usually a time-based one-time password, a biometric scan, or a code from an authenticator app. MFA provides many benefits and is, perhaps, the easiest cyber-defense mechanism for organizations to set up

3. Reduce the attack surface

The attack surface is the combined physical and digital assets in your network through which an unauthorized user can access your network and extract private data. Common examples of your attack surface include computers, switches, applications, code, ports, servers, and websites. You can manage and secure your attack surface by mapping your assets on the cloud and on-premises by uncovering potential vulnerabilities or weaknesses, vetting user roles, and privilege levels. As the healthcare

industry grows smarter, with innovative solutions taking us to the next frontier, expanding the enterprises' digital footprint shouldn't be a reason for worry.

It's better to monitor and secure your existing attack surface instead of trying to reduce it. In short, embracing new technology should not be hindered by the threat of potential cyberattacks

4. Patch and update OS and applications automatically

Applying the latest patches and updating software and applications on time continues to be vital for any cyberattack prevention plan. IT managers can’t afford to downplay the importance of patching and keeping their software up-to-date.
Since timing is crucial for applying patches and software updates, it is important to automate these processes to limit the exposure of your healthcare IT to vulnerabilities. Unpatched systems remain a major target in cyberattacks, so automating software updates and timely installing patches as soon as they are released is the right thing to do

5. Ensure strong device and application control

Attackers using a memory device to hack into hospital systems are not just a thrilling scene from a sci-fi movie. Threat actors can plug devices into your USB ports and run a script that can render health facilities useless. One way to mitigate this is by blocking the use of external storage devices. This can be accomplished using a device control solution that lets you keep tabs on peripheral devices and ports. You can also vet plugged-in devices and analyze user behavior across your facility to help prevent insider threats.

In addition to monitoring potentially harmful actions surrounding hardware, you can also elevate your enterprise endpoint security actions by granting access privileges only to a particular group, or restricting the use of unauthorized apps or software on corporate machines.

6. Enforce access control

From the chief surgeon to the junior nurse, all hospital staff need quick, easy access to data to foster a wholesome patient experience.

Adequate access control ensures that every user has the correct amount of access, cutting down on the need to provide admin access to everyone, all the time.

If healthcare personnel need access to resources that require admin privilege, you can temporarily elevate their privileges so they can accomplish their work efficiently. Access control secures your data, provides accountability by tracking user access, and ensures compliance with IT regulations.

7. Remediate vulnerabilities

Traditional patching accounts only for the known vulnerabilities that are documented by vendors. The remaining unknown vulnerabilities are not documented and usually stay under the radar before creating havoc. ***Vulnerability management solutions ensure continuous visibility, detect weakness, assess the risks, and remediate threats. As a result, you can audit and maintain your systems in line with compliance benchmarks and stay up to date with detailed remediation insights.***

8. Incorporate multiple security layers

Your enterprise security perimeter needs multiple layers of security to provide added depth. Depending on the need, you can implement multiple security layers with varying levels of protection like:

- Firewalls
- Intruder detection and prevention systems like antivirus and malware software
- Network monitoring systems
- Secured authentication

9. Implement encryption and data backups

Encryption makes your organization’s sensitive information, like hospital info and patient records, unreadable to anyone who shouldn’t have access to it, like unauthorized users or hackers. This is especially useful during a ransomware attack. Even if your data is compromised, threat actors won’t be able to divulge the contents of the data, keeping your organization out of danger

Encryption is incomplete without

adequate data backups. It is crucial to back up the operation's important and sensitive information. By doing so, you can transition seamlessly in the event of a data breach. Having a data backup and recovery plan is a vital process, too.

This involves listing items that need to be saved offline in storage devices or in secure cloud storage, like data files and folders, OS images, customer databases, machine images, operating systems, and registry files. The needs of each department, from the biochemistry to the x-ray department, need to be addressed. Many vendors offer HIPAA compliant backup and data recovery solutions that streamline this process and ensure minimal interruptions.

10. Ensure endpoint management and protection

Endpoints can be office computers, mobile phones, tablets, routers, and other devices, and they can access a network from both on-premises and remote locations. Endpoint protection is a broad term that includes multiple facets such as vulnerability management, browser security, and application control.

11. Have a robust Next Gen Antivirus

Traditional Anti-viruses, with the signature-based approach to mitigate malware attacks, are increasingly capable of defending your endpoints. Next-Gen Antivirus is the next-level approach to secure your enterprise endpoints.

With AI-assisted real-time behavior detection, you can be assured of a comprehensive malware defense and zero downtime of your endpoints.

12. Prevent Data leakage with Data Leakage Prevention (DLP) solutions:

In order to be HIPAA compliant , you will need powerful data loss prevention feature. ***The DLP solution should classify data—especially personally identifiable information (PII) - given that patient data is extremely confidential.*** To understand how the data flows in their IT environment, you can implement file tracing to track sensitive files, especially when you move them to external devices. You can also perform file shadowing operations for sensitive data whenever you copy or modify them in peripheral devices.

ManageEngine Endpoint Central serves as an endpoint protection solution that protects your endpoints in multiple ways, from securing end-user browsers to controlling your external devices and applications. You can utilize the complete suite of security features with a single security add-on. Additionally, Endpoint Central can centrally manage and monitor all your devices across multiple platforms spread across a distributed network. A well secured network is one that is well managed.

Roadmap for healthcare IT/OT

01 Gain visibility

- Determine the attack surface by mapping the assets
- Identify network blind spots
- Perform compliance checks
- Initiate a gap analysis and health checks
- Analyze requirements

02 Strengthen your security perimeter

- Utilize firewalls
- Enable Zero Trust
- Install intrusion detection systems
- Deploy threat prevention systems
- Harness secure authentication using MFA
- Enact password management
- Engage VPNs

03 Monitor continuously

- Deploy endpoint security tools
- Implement data loss prevention strategies
- Adopt device and application control
- Enforce privileged access
- Utilize a vulnerability scanner

04 Ensure maximum uptime of healthcare services

- Ensure availability of critical health services
- Take data backups
- Encrypt information
- Balance cyber resilience with productivity
- Utilize endpoint protection

05 Validate and evolve

- Simultaneously test the network's security
- Qualify and check device upgrades and technological roll-outs
- Encrypt information
- Set up a test environment to check the latest software updates and patches

About ManageEngine Unified Endpoint Management and Security

ManageEngine UEMS develops endpoint management and security tools for teams that are looking to adopt change and innovate fearlessly. Endpoint Central, our unified endpoint management (UEM) solution automates tasks, delivers insights, and provides a reliable way to ensure management and security of your workforce. From a single dashboard, you're enabled to secure your organization by minimizing risks without affecting your agility. Work smarter, stay informed, and accelerate your operations without any obstacles.

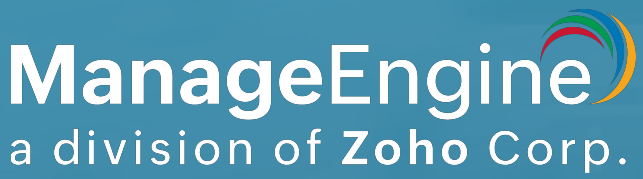
VISIT ENDPOINT CENTRAL

TRY IT FOR FREE

Follow us on:

sales@manageengine.com | +1-925-924-95

05


ManageEngine
a division of Zoho Corp.