

**Lenovo** Health

# Shielding Healthcare from Cyberthreats



# Healthcare was the most breached industry in 2018.

Few were surprised when a focus group of members from the College of Healthcare Information Management Executives (CHIME) revealed cybersecurity to be a top priority for 2019.<sup>1</sup> Patient records are now among the most valuable assets on the dark web, selling for as much as \$1,000 each.<sup>2</sup> Hacking efforts have also intensified, making healthcare the most breached industry for 2018.<sup>3</sup>

**More than 15 million patient records were compromised in 2018, up sharply from 5.6 million in 2017.<sup>4</sup>**



# The sheer magnitude of hacker attention isn't the only concern for healthcare security professionals. The job of securing the healthcare technology ecosystem is made infinitely more complicated by several factors that are unique to healthcare.

## The Rise of Consumerism

An increased focus on patient choice and cooperative care delivery has led to new care options, new workflows, and, of course, new devices and technologies. IoT alone may triple the number of “endpoints” in a healthcare ecosystem by 2023.

These advances stand to introduce new vulnerabilities within a health system, making current security boundaries susceptible to breach. CIOs must be constantly vigilant — not only to secure new devices and technologies, but also to ensure device and technology security is extendable to other connected systems throughout the organization.

## Healthcare Convergence

2018 was a record-breaking year for healthcare mergers and acquisitions, up 14.1% from 2017.<sup>5</sup> When the financial deal is done, it's the healthcare CIOs who execute the herculean task of merging disparate technology systems. Ultimately, these health systems will deliver a more unified and standardized single channel of care. But first, it's a patchwork quilt of technology systems, and each seam holds the potential for data leakage.

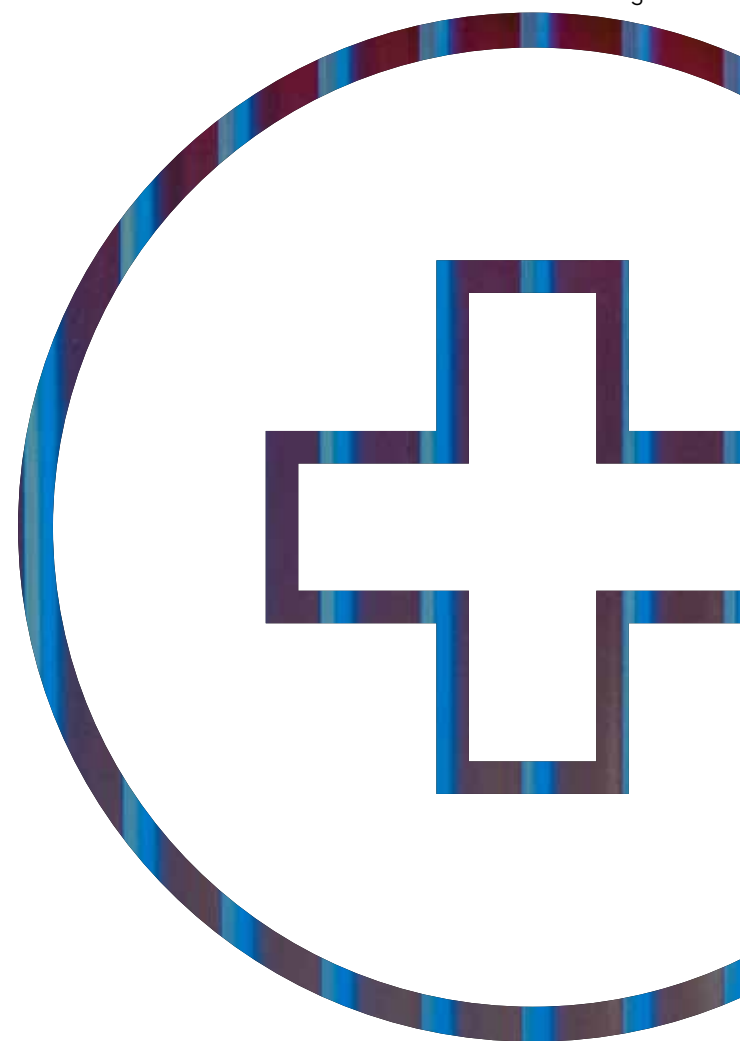
## Regulations and Compliance

A technology solution must be evaluated with one additional criterion before it can be considered valuable for use in healthcare: Does this solution help the organization comply with the highest regulatory standards? Technologies that meet security standards in other industries may not comply with HIPAA patient privacy standards or guidelines for electronic prescribing of controlled substances (EPCS).

## Security vs. Expediency

All these security efforts are happening while clinicians strive to deliver lifesaving patient care as quickly as possible. Layers of security have the potential to significantly disrupt workflow, delay care delivery, and negatively impact patient outcomes.

Clinicians waste as much as 45 minutes per shift simply logging into computer systems.<sup>6</sup> As a result, 41% of healthcare companies say they have knowingly sacrificed security for expediency or business performance.<sup>7</sup> But with the average cost of a data breach at nearly \$4 million per incident,<sup>8</sup> the need for security tools has never been more critical.





Indeed, the healthcare security landscape is fraught with complications, and it can be exceedingly challenging to match the right technology solution to each critical security gap.

This guide simplifies the process, outlining Lenovo's four-step approach to comprehensive end-to-end security. The Lenovo ThinkShield portfolio includes security tools healthcare organizations can use to protect data, devices, user identity, and online security.

## **SECURING DATA**

With every security breach, there's a lot at stake: patient data, millions of dollars, your organization's reputation, and even your job.

## **DEVICE SECURITY**

Device-level security begins at product development, with robust design features to keep users safe from today's privacy threats.

## **PROTECTING IDENTITY**

Every 2 seconds someone's identity is stolen.<sup>9</sup> Deliver care while protecting data access.

## **ONLINE SECURITY**

Phishing attacks are on the rise. Keep users from taking the bait.



# Securing Data

Data is obviously the end goal for hackers. Monetizing healthcare data — ransomware, black market buyers — is simply lucrative. Given the exorbitant price tags attached to healthcare data, malicious outsiders represent over half (56%) of global breaches, and they're using attack methods across all security fronts to gain access. Explore tools that provide a layer of protection around the data itself — protection even before fortifying entry points to the data.



# 50% of participants in a recent Lenovo webinar confirmed that negligent employees represent their biggest security threat.

Following malicious outsiders, a significant 34% of breaches were the result of accidental loss.<sup>10</sup> In fact, 50% of participants in a recent Lenovo webinar confirmed that negligent employees represent their biggest security threat.<sup>11</sup> Threats due to accidental employee loss point directly to weaknesses in user authentication. The most vulnerable authentication entry points often correlate with multi-user devices, high-traffic departments, and on-premise data storage.

Tools that restrict access to data, locking it away from personnel who don't need to interact with it, are the most beneficial — providing first-line defense of data. Also consider remote management tools that help security administrators deliver data visibility no matter where data is stored.

# Tools You Can Use

## Virtual Desktop Infrastructure

From computing to storage, the cloud is redefining “normal” for healthcare data security. A recent Black Book survey revealed that 91% of CIOs believe cloud computing is the most agile and effective way to manage data,<sup>12</sup> and most IT experts believe the cloud offers a step up for security.<sup>13</sup>

ThinkShield VDI technology leverages cloud to deliver a virtual desktop when users log in from any endpoint device. Each user is given access to all the data they need — but only the data they need — for workflows such as nursing, billing and coding, and call centers. Health systems deploy thin or zero clients throughout the organization to significantly reduce the number of disparate devices that house data.

## Absolute Persistence

ThinkShield's Absolute Persistence solution helps IT administrators maintain constant contact with endpoint devices. This software solution notifies IT teams when security applications fail. Its persistent device awareness reduces threat detection time, allows for remote access to resolve access issues, and protects patient data.

## BitLocker Encryption

BitLocker encryption protects against the loss of patient information by encrypting data on devices, even when they are lost or stolen.

## Keep Your Drive

The Keep Your Drive program ensures that data stays within an organization's control even at a device's end of life. While the ThinkShield portfolio includes secure disposal and recycling (see description under “Device Security”), IT administrators may opt for an extra layer of protection that allows them to keep the hard drive of an old endpoint device after recycling.

## ThinkPad® PrivacyGuard with PrivacyAlert

Visual hacking is an insidious way protected patient information can fall into the wrong hands. ThinkPad devices such as the T490 Healthcare Edition offer options that shield vital data from unauthorized viewers.

ThinkPad PrivacyGuard filters the screen to prevent peripheral viewing. This added layer of protection leverages presence detection technology to sense when the user is away from the device, automatically locking the screen. Presence detection also senses when someone other than the user may be gazing at screen and auto-enables the privacy filter.



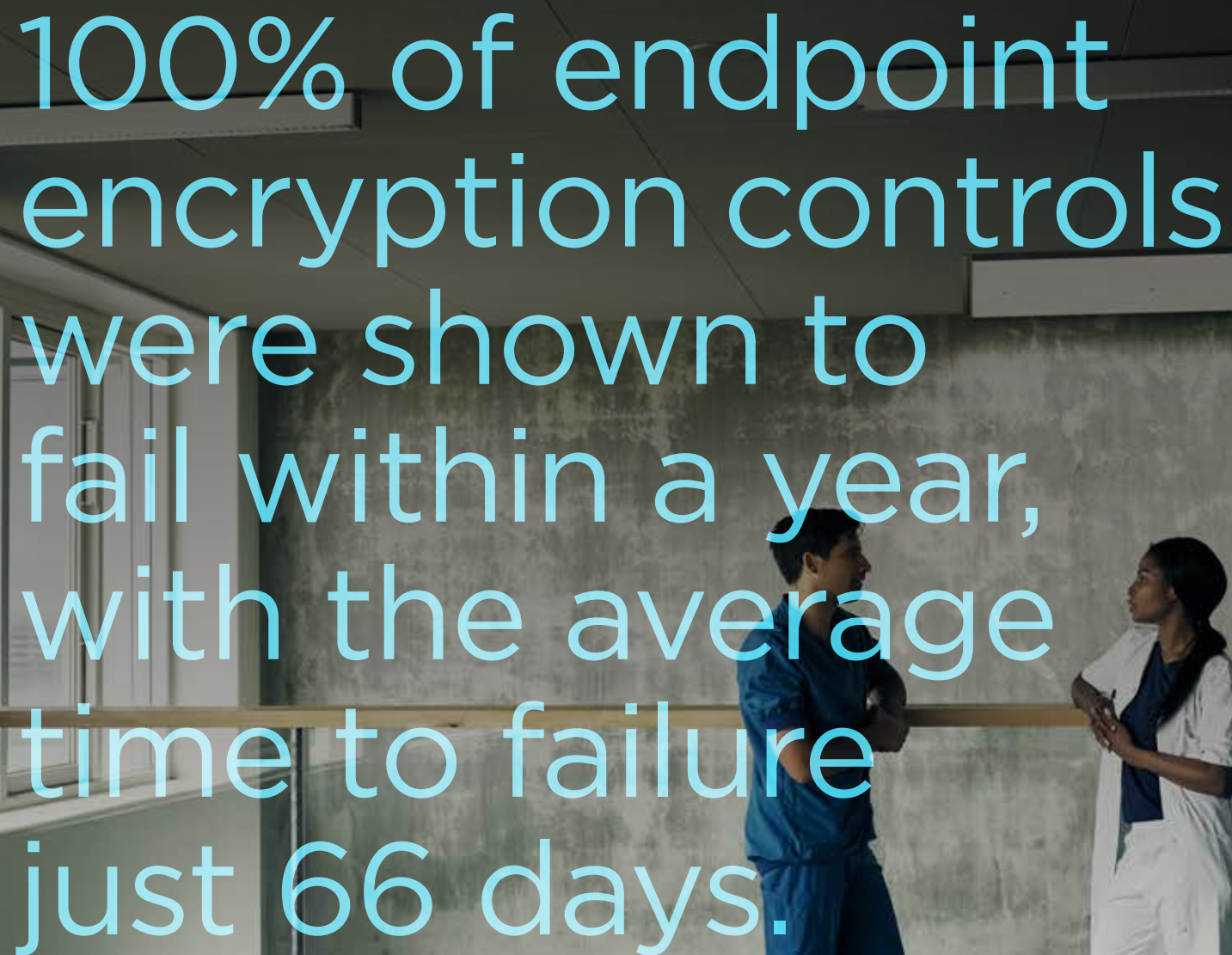
**91% of CIOs believe cloud computing is the most agile and effective way to manage data.**



# Device Security

Cybercriminals are increasingly targeting manufacturing supply chains to introduce device vulnerabilities during the manufacturing process.<sup>14</sup> So, device security should begin during device manufacturing, since hackers can strike a device before the end user even opens the box.





# 100% of endpoint encryption controls were shown to fail within a year, with the average time to failure just 66 days.

After deployment, laptops can be hijacked — stolen or inadvertently given to users with reduced security clearances. Devices are also forgotten, stuck in drawers or closets without maintenance or updates. Security at this level requires that devices be built to withstand attacks and user negligence.

Still, devices must be updated, managed, and maintained. According to a recent study, 100% of endpoint encryption controls were shown to fail within a year, with the average time to failure just 66 days.<sup>15</sup> Security agents installed or incorporated into a device may compete with one another and ultimately cause some protections to fail, so continuous vigilance is always required.

# Tools You Can Use

## Secure Supply Chain

Lenovo locks down the entire manufacturing supply chain — directly overseeing all suppliers, components, and processes. The Lenovo BIOS Reading Room is the industry's first controlled physical environment where customers can visually inspect more than 2 million lines of Lenovo BIOS source code. The secure, built-in BIOS and firmware are constantly updated and optimized.

## Authentication Tools

From passwords and PINs to fingerprint readers and facial recognition technology, numerous authentication tools keep unauthorized users from logging in to a lost or stolen device. (See “Protecting Identity” for advanced authentication tools and healthcare compliance.)

## BIOS-Level Safeguards

Lenovo devices are designed with built-in BIOS-level protections that help IT administrators maintain the health and security of each device. Some examples:

- In the event of attack or corruption, the BIOS will self-heal and revert to a known good backup copy.
- HTTPS Boot allows IT administrators to securely boot from an https network resource.
- Intel® Hardware Shield helps minimize the risk of a malicious code injection. It locks the BIOS when software is running to help prevent planted malware from gaining traction.
- With Smart USB protection, device ports are secured to respond only to keyboards and pointing devices, blocking unknown storage devices and prohibiting the unauthorized transfer of data.

## ThinkShutter

Cameras on devices such as the T490 Healthcare Edition feature the industry's first built-in shutters that physically cover the camera(s) when not in use. The shutter prevents hackers from intruding on patient encounters.

## Secure Disposal

The Keep My Drive program lets users keep their drive at the end of a device's lifecycle. Lenovo ThinkShield protections include complete drive wiping and the secure recycling of computer parts.

**With Smart USB protection, device ports are secured to respond only to keyboards and pointing devices, blocking unknown storage devices and prohibiting the unauthorized transfer of data.**



# Protecting Identity

Healthcare user identities are stolen every two minutes. This makes identity theft the most prevalent type of data breach.<sup>16</sup> Practices like multi-factor authentication (an authorization token, an emailed or texted code, biometric data, etc.) help fortify password security.



# 21% of healthcare employees write down their user names and passwords near their computer.<sup>17</sup>

Security measures aimed at identity protection require special consideration because they're so integrally connected with end user workflow. Done well, identity security works in the background, protecting clinicians and staff from accidental data loss through scams or negligence. Executed poorly, identity protection technology can throw up too many roadblocks that prevent clinicians from efficiently accessing the data they need for urgent patient care.

Well-designed identity security tools offer another advantage: In addition to protecting data, identity tools also help healthcare organizations meet rigorous government compliance standards like HIPAA that require identity verification. Tools often look alike at the first read-through. Healthcare users who require authentication for compliance should take care to ensure the selected tool meets the full range of requirements.



# Tools You Can Use

## T490 Healthcare Edition Laptop

The newest addition to the ThinkPad series delivers the highest level of identity compliance, incorporating numerous technologies for multifactor authentication:

- The RFID reader allows clinicians to badge in to the computer and authenticate to the network at the same time. The reader is Imprivata®-certified for single sign-on, and it works with both RFID and NFC technologies.
- The FIPS 201-compliant fingerprint reader exceeds DEA identity requirements for electronic prescription of controlled substances (EPCS).
- The IR camera utilizes facial recognition technology for compatibility with Windows Hello and other applications.





# Online Security

Email is now the most frequent location of breached protected health information.<sup>18</sup> Phishing scams, unauthorized email access, and misdirected emails accounted for more than 33% of all healthcare data breaches in 2018,<sup>19</sup> underscoring the urgency of online protection in healthcare.



# Email is now the most frequent location of breached protected health information.

Solutions such as VDI and cloud storage are only as strong as the network and edge devices used to access the data. ThinkShield is the first comprehensive security suite to include online security tools, offering a layer of protection to support activities at the point of online access.

# Tools You Can Use

## Artificial Intelligence (AI)

AI is impacting numerous areas of healthcare, not the least of which is security. Machine learning is now being leveraged to learn and identify potential security threats from the inside (innocent or malicious employees) to the outside (malicious outsiders). AI is adept at identifying malicious files or suspicious IP addresses, which allows IT teams to detect and respond to threats considerably faster. AI also looks for unusual usage and access patterns — large downloads of data or user access to patient records in unusual locations.

## Wi-Fi Security with Coronet

This award-winning technology performs a local risk analysis, checking access point details for vulnerable behaviors. It warns users of suspicious behavior with a “safe/not safe to connect” message.

## Endpoint Management Powered by MobileIron®

Unify cloud and endpoint security across multiple devices with this technology that enables both VDI solutions and BYOD programs. Endpoint management allows IT departments to reach remote employees while remaining secure.

## BUFFERZONE Sandboxing

BUFFERZONE uses patented virtualization technology to isolate Internet applications and contain cyberattacks so they cannot get through to the network or to endpoint devices.

## Security Checklist

Use this quick reference to establish and maintain your organization's security process.<sup>20</sup>

- ☐ Pinpoint every endpoint
- ☐ Identify authorized and unauthorized PHI sharing/storage
- ☐ Encrypt every endpoint
- ☐ Develop ongoing asset intelligence for monitoring
- ☐ Benchmark endpoint hygiene and data protection effectiveness
- ☐ Build rapid response protocols through remote command to any endpoint
- ☐ Learn and iterate from direct and indirect experience





## ABOUT LENOVO HEALTH

We have reimagined how technology powers patient engagement and brings excitement back to clinical care delivery. Innovation energizes your imagination and activates your potential. Lenovo Health leverages proven reliability and security leadership to Think Beyond care delivery barriers. Our mobility, collaboration and cloud solutions power care at the pace of life.

**If you're ready to secure devices, user identity, and online action, Lenovo Health can help. Visit [www.lenovo.com/health](http://www.lenovo.com/health)**

### References

- 1 <https://healthitsecurity.com/news/cybersecurity-patient-trust-data-sharing-top-health-cio-priorities>
- 2 <https://www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html>
- 3 <https://www.healthcaredive.com/news/healthcare-again-tops-industries-for-cybersecurity-attacks-data-breaches/552403/>
- 4 <https://healthitsecurity.com/news/15-million-patient-records-breached-in-2018-hacking-phishing-surges>
- 5 <https://www.healthcarefinancenews.com/news/healthcare-mergers-and-acquisitions-had-record-year-2018-144-percent>
- 6 Statistic provided by Imprivata on the webinar "Shielding Healthcare Data from Cyberthreats: Tools You Can Use from A to V," May 2019.
- 7 Statistic provided by Imprivata on the webinar "Shielding Healthcare Data from Cyberthreats: Tools You Can Use from A to V," May 2019.
- 8 <https://www.ibm.com/security/data-breach>
- 9 <https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf>
- 10 <https://www.statista.com/statistics/221285/types-of-attackers-responsible-for-data-breaches/>
- 11 Poll statistic on the webinar "Shielding Healthcare Data from Cyberthreats: Tools You Can Use from A to V," May 2019.
- 12 <https://www.healthcareitnews.com/news/next-gen-cloud-computing-how-healthcare-can-prepare-future>
- 13 <https://www.mobihealthnews.com/content/why-healthcare-data-may-be-more-secure-cloud-computing>
- 14 [https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl-ntt-security-2018-global-threat-intelligence-report-v2-uea.pdf?sfvrsn=c761dd4d\\_10](https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl-ntt-security-2018-global-threat-intelligence-report-v2-uea.pdf?sfvrsn=c761dd4d_10)
- 15 Statistic provided by Absolute on the webinar "Shielding Healthcare Data from Cyberthreats: Tools You Can Use from A to V," May 2019.
- 16 <https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf>
- 17 <https://www.accenture.com/us-en/blogs/blogs-losing-cybersecurity-culture-war>, 2018)
- 18 <https://www.modernhealthcare.com/technology/email-now-top-source-healthcare-breaches>
- 19 <https://www.hipaajournal.com/analysis-of-healthcare-data-breaches/>
- 20 Checklist provided by Josh Mayfield, Global Director of Healthcare Solutions for Absolute Software, on the webinar "Shielding Healthcare Data from Cyberthreats: Tools You Can Use from A to V," May 2019.