
Lenovo
Health
Protecting healthcare everywhere
A smarter approach to stopping evolving threats
ThinkShield
Windows 10
Smarter technology for all
Lenovo

It's not getting any easier out there for healthcare IT security

Ask any C-suite executive what's keeping them up at night, and you can be sure cyberthreats are near the top of the list. That's particularly true in healthcare, as healthcare is consistently the most targeted industry for hackers.

Patient records are among the most valuable assets available on the dark web because they contain such a wealth of information, including date of birth, credit card information, Social Security number, address, and email. A single patient record can fetch as much as $1,000.[1]

With that kind of money to be made, it's not surprising that the rate of attack on healthcare data has increased year after year.

In 2019, 41 million patient records were breached, which is nearly three times as many as the year before.[2]

THE RISING COST OF HEALTHCARE DATA BREACHES

The costs of dealing with data breaches continues to rise for healthcare organizations. Data breaches cost the healthcare sector an average of $6.5 million, which is more than 60% higher than all other sectors. That was $429 for each lost or stolen record in 2019, up from $408 per record in 2018.[3]

MAAS (MALWARE AS A SERVICE)

There are more threats to healthcare IT today due to the proliferation of sophisticated hacking tools. Bad actors no longer need to write complex code to mount an attack — the resources are a click away. Websites now offer malware as a service.[4]

Lenovo

Windows 10

An increasingly complex landscape

The healthcare world is evolving in ways that can compound the challenge of defending against evolving and increasing threats.

Increasing mobility expands the attack surface

One of the most visible trends impacting security is the dramatic increase in mobile technology. A recent survey of healthcare IT decision-makers showed that 90% are either currently implementing or are planning to implement a mobility program.[5]

With more endpoints and more data in motion across more networks, the threat surface quickly expands. As the National Institute of Standards and Technology (NIST) noted in its recent publication, any patient information that's collected, stored, processed, or transmitted on mobile devices is especially vulnerable to attack.[6]

And yet, according to the HIMSS Cybersecurity survey, less than 5% of respondents included mobile devices in their penetration testing.[7]

The increasingly mobile nature of healthcare providers and care delivery in general poses significant challenges for healthcare IT teams, many of which are themselves working remotely.

Regulations and compliance

Any 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

Increasing security safeguards are being woven into the care delivery workflow while clinicians strive to deliver lifesaving patient care as quickly as possible. Layers of security have the potential to significantly disrupt or delay care delivery and negatively impact patient outcomes. Clinicians waste as much as 45 minutes per shift simply logging into and out of computer systems.[8] As a result, 41% of healthcare companies say they have knowingly sacrificed security for expediency or business performance.[9]

Security needs a people-first approach

Healthcare IT security must be seamless and ubiquitous, but it has to work the way healthcare employees work. It must support and empower healthcare workers while protecting the organization and its data.

Security by Design

A smarter approach to healthcare IT security

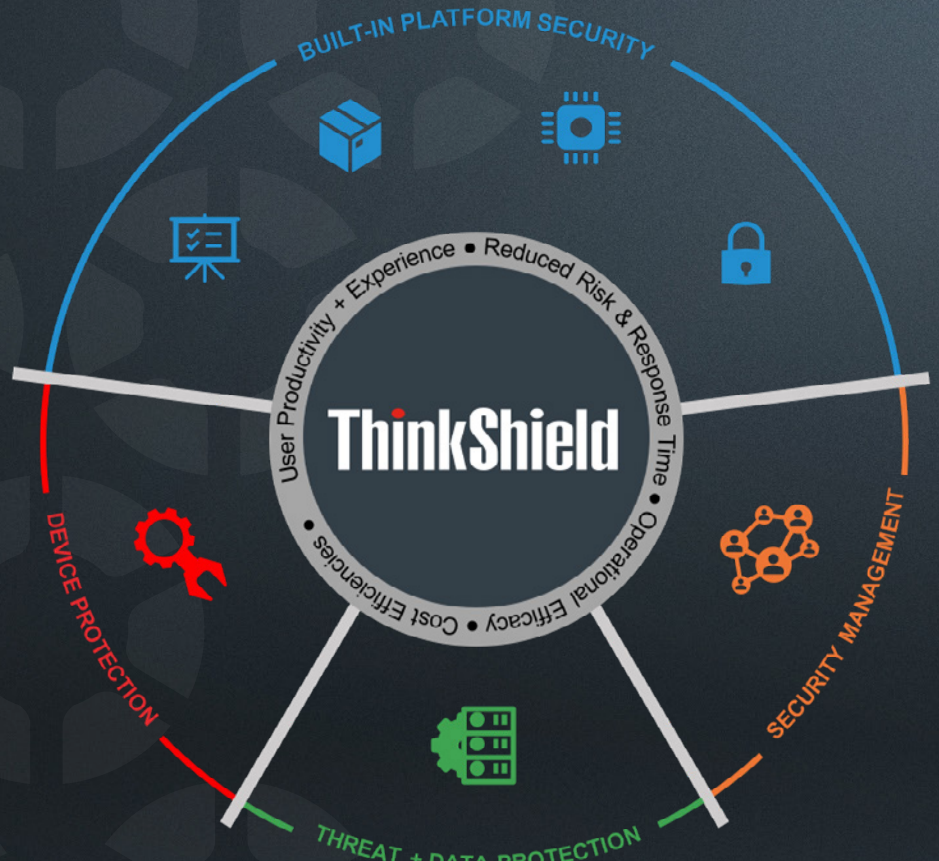
ThinkShield is a customizable solution that secures critical data and business technologies with comprehensive end-to-end protection. It's not a standalone product — it's a unique combination of hardware, software, services, and processes that protect healthcare IT across four key dimensions.

Security by Design starts with developing standard security requirements for each device to address a current and evolving threat landscape.

This approach continues into securing our supply chain with robust practices and policies.

Our Trusted Supplier Program, a rigorous vetting process, ensures every supplier meets the highest standards for end-to-end supply chain security. Requirements for suppliers include quarterly compliance assessments, onsite asset protection reviews, and the implementation of need-to-know control of information security and logistics processes.

For the healthcare IT environment, ThinkShield helps provide privacy, safety, and security.



BUILT-IN PLATFORM SECURITY
Our holistic approach to security starts with the built-in ThinkShield security solutions that come standard on industry-leading Think® devices

DEVICE PROTECTION
Security hardware features and service offerings that add another layer of device protection

THREAT AND DATA PROTECTION
Security solutions that seamlessly integrate with Lenovo devices, ensuring your critical data and business technologies are protected

SECURITY MANAGEMENT
Solutions that provide capabilities to deploy, monitor, and report IT assets

Lenovo Windows 10

Privacy — Keep patient data and clinician activity secure

Healthcare delivery is constantly in motion, and security measures need to keep up. It's not always easy to know who can see a device's screen throughout a shift. That's why we offer PrivacyGuard and Shoulder Surfing Protection.

PrivacyGuard provides an integrated e-privacy filter that prevents others from looking over your shoulder to get valuable information — without the need for third-party aftermarket privacy filters (which frequently get lost or thrown away and need to be replaced). Having a preinstalled e-privacy filter is more secure and is one less thing the IT team and users have to deal with.

Shoulder Surfing Protection incorporates gaze detection technology, which notifies the user if someone else is looking at the screen and even detects which side of the screen they're watching from. Gaze detection can also automatically blur the screen when the user looks away.

Shoulder Surfing Protection includes built-in presence detection that locks the device for walk-away security.

ThinkShield Built-In Platform Security includes a webcam privacy shutter that covers both the regular and IR cameras. This physical camera cover gives patients and users peace of mind that the camera isn't on or being hacked.

The ThinkShield approach to privacy extends through the end of a device's service lifecycle with multiple options for secure disposal to protect patient privacy.

The secure wipe feature in the BIOS reliably deletes all data from a drive without the need for external tools.

The Keep Your Drive service allows customers to keep the hard drive of a device if it should fail, eliminating the need for tracking drives in transit.

THE THINKPAD® T14i HEALTHCARE EDITION

You'll find all these ThinkShield features on the ThinkPad T14i Healthcare Edition, a workhorse laptop that brings all the performance that's made the ThinkPad® family a global best seller to the healthcare workforce with features and options designed specifically to address the needs of the healthcare environment. **solutions.Lenovo.com/Health**

Lenovo

Windows 10

Safety — Keep patients safe by reducing vectors of transmission

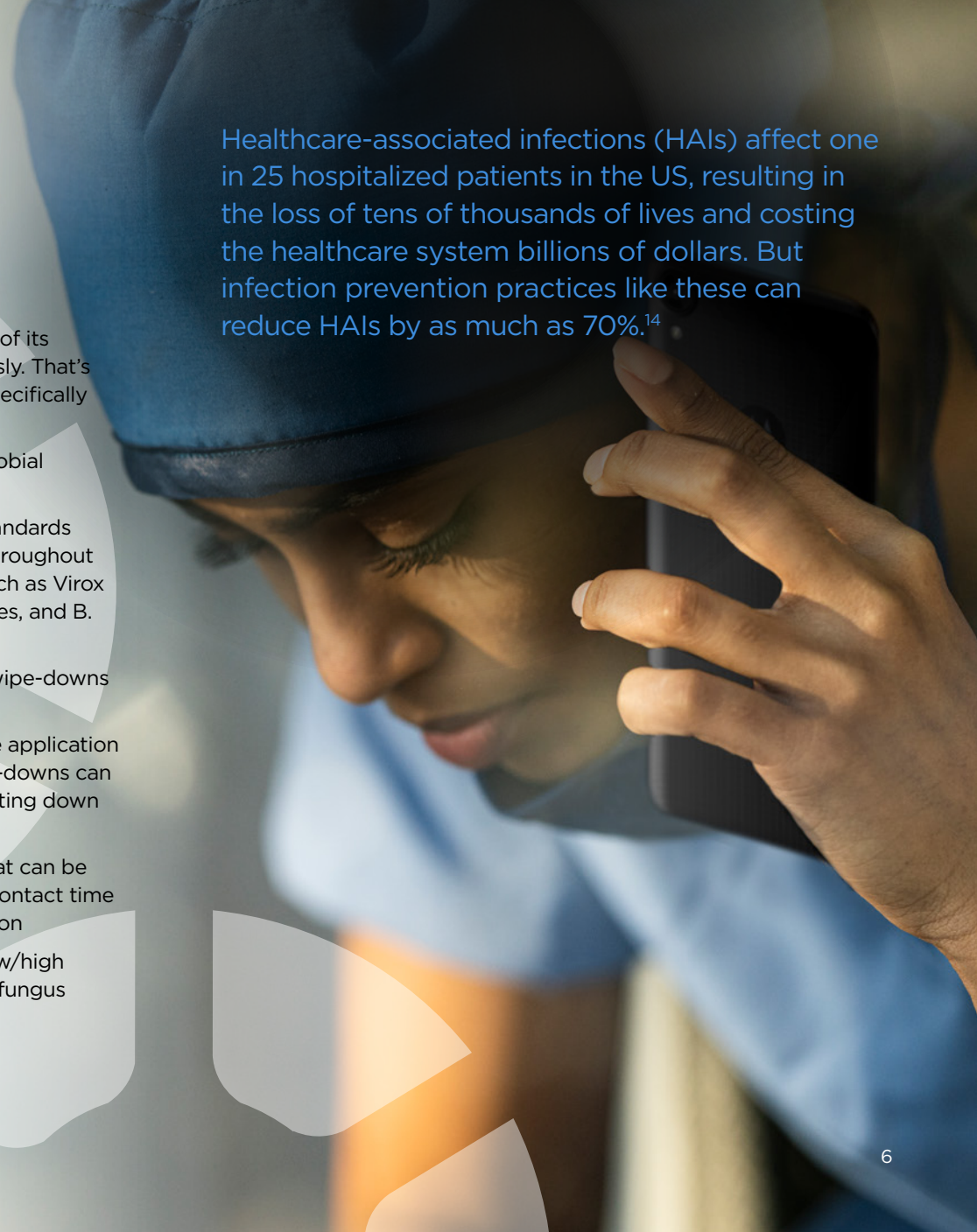
Now, more than ever, following infection prevention protocols is vital. A growing body of literature shows the rate of bacterial contamination of healthcare workers' mobile devices ranges from 40% to nearly 100% — yet a whopping 90% of patient-facing care providers never clean their mobile phones.[10]

But there's good news, too. It doesn't take much to reduce all this contamination. One study found a 36% to 100% reduction in contamination within five minutes of the simple use of an antibacterial wet wipe.[11] Another reported cutting bacterial contamination in half using 70% isopropyl alcohol and 15 seconds of friction.[12]

One study of a hospital showed pathogens on 80% of mobile phones and on 81% of clinicians' hands that handled those phones.[13]

Lenovo takes the health and safety of its users and their patients very seriously. That's why our healthcare devices have specifically engineered features that include:

- An ISO 22196-compliant antimicrobial surface treatment
- Extensive testing against CDC standards to withstand vigorous cleaning throughout the day with reputable brands such as Virox Accel Wipes, PDI Germicidal Wipes, and B. Braun Meliseptol
- Durability for more than 10,000 wipe-downs over the life of the device
- The Lenovo Quick Clean software application that suspends user input so wipe-downs can be executed quickly without shutting down the device
- The Lenovo Quick Clean timer that can be customized to ensure adequate contact time for proper cleaning and disinfection
- MIL-SPEC testing for humidity, low/high temperature, dust, vibration, and fungus



Healthcare-associated infections (HAIs) affect one in 25 hospitalized patients in the US, resulting in the loss of tens of thousands of lives and costing the healthcare system billions of dollars. But infection prevention practices like these can reduce HAIs by as much as 70%.[14]

Lenovo Windows 10

Security — Authentication and data

Limiting access to healthcare data to only authorized users is a cornerstone of any security practice. ThinkShield provides multiple ways to verify a user's identity, including frictionless multifactor authentication.

NETWORK SECURITY
Based on the device's IP address

GPS SECURITY
Based on geo-location

FACIAL RECOGNITION
IR cameras that support Windows Hello

BLUETOOTH
For phone proximity authentication

PASSWORDS AND PINS
Intel Authenticate Secure PIN, Windows 10 typed and visual PINs

MATCH-ON-CHIP FINGERPRINT READER
Includes Quantum Matcher anti-spoofing algorithms

FIPS 201-COMPLIANCE
Exceeds requirements for EPCS

NFC
Secure NFC tap-to-logon compatible with all major single sign-on providers, including Imprivata®

Having all these features built in means devices protected by ThinkShield fit seamlessly into existing security protocols with no additional hardware required.

Lenovo Windows 10

SWITCHING TO SINGLE SIGN-ON SAVES TIME

One recent study showed SSO helped a hospital reduce average clinician sign-on time from 29.3 to 8.9 seconds — a 69% reduction. Over the course of a week at one facility, that added up to 49.7 hours, or about four 12-hour shifts.[15]

Security — Real-time endpoint protection

ThinkShield includes features designed specifically for real-time endpoint protection within and beyond a healthcare facility.

SentinelOne — Autonomous endpoint protection
SentinelOne delivers next-generation antivirus protection powered by patented behavioral AI. This advanced, autonomous threat detection completely replaces an antivirus solution and expands to include active EDR (endpoint detection and response) for known and unknown malware strains, enabling devices to self-heal from broad modes of attack instantaneously.

WinMagic — Drive encryption
A highly configurable, full-scale encryption for the enterprise environment that protects sensitive information stored on devices. Centrally manage encryption on devices across all platforms using a choice of SecureDoc FDE, FileVault2, BitLocker, dm-crypt, and Self Encrypting Drive. Easily track encryption and manage keys for SecureDoc devices and third-party applications, platforms, and entities through a single console.

Absolute® — Endpoint visibility and control
Embedded directly into Lenovo device firmware, Absolute is an endpoint visibility and control solution that provides persistent security management. It automates endpoint hygiene to support self-healing capabilities. Its real-time remediation control allows remote investigation of potential threats and prompts action if a security incident occurs.

Lenovo WiFi Security — Protect data on campus and off
Lenovo WiFi Security automatically detects suspicious activity and protects devices from being attacked through a Wi-Fi network. The local agent checks the access point details for vulnerability behaviors, performs a local risk analysis, and warns users of suspicious access point behavior.

LENOVO VIRTUAL ROUNDING

See how Lenovo's Virtual Rounding solution delivers secure face-to-face communication in the healthcare environment while helping to reduce the spread of HAIs.
solutions.Lenovo.com/Health

Lenovo

Windows 10

Balance protection and productivity

Securing patient data against external threats and internal exposure is a never-ending challenge. At the same time, security measures must support the dynamic workflows found in today's healthcare environment and allow timely access to critical patient data when needed.

Lenovo's healthcare devices protected by ThinkShield help achieve that balance with powerful features designed to provide privacy, safety, and security in the modern healthcare world.

Visit solutions.Lenovo.com/Health today for more information.

Lenovo

Windows 10

Connect with Lenovo Health. We're experts at breaking down barriers and building smart solutions. When you're ready, we're here to help.

Contact your Lenovo Health Account Representative or local Business Partner

Visit solutions.Lenovo.com/Health

Follow us on Twitter @LenovoHealth

Email us at HealthTeam@Lenovo.com

SOURCES

1 https://www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html

2 https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats

3 https://healthitsecurity.com/news/data-breaches-cost-healthcare-6.5m-or-429-per-patient-record

4 https://www.itprotoday.com/cloud-security/malware-taking-new-shape-malware-service

5 https://healthitsecurity.com/news/mobile-devices-in-healthcare-increase-as-do-security-challenges

6 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-1.pdf

7 https://www.healthcareitnews.com/news/protecting-endpoints

8 Statistic provided by Imprivata on the webinar "Shielding Healthcare Data from Cyberthreats: Tools You Can Use from A to V," May 2019.

9 Statistic provided by Imprivata on the webinar "Shielding Healthcare Data from Cyberthreats: Tools You Can Use from A to V," May 2019.

10 https://orb.binghamton.edu/cgi/viewcontent.cgi?article=1001&context=alpenglowjournal

11 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6210060/

12 https://www.myamericannurse.com/mobile-devices-healthcare-associatedinfections/

13 https://www.healthcareitnews.com/news/ensuring-computers-notebooks-andmobile-devices-are-included-disinfection-mix

14 https://www.healthypeople.gov/2020/topics-objectives/topic/healthcareassociated-Infections

15 https://www.beckershospitalreview.com/healthcare-information-technology/how-single-sign-on-within-ehrs-can-save-clinicians-time-reduce-hospital-costs-improve-patient-care.html

Lenovo