Lenovo
ThinkShield

Lenovo ThinkShield for Healthcare and Life Sciences

Protecting healthcare and life sciences everywhere

A smarter approach to stopping evolving threats

intel CORE ULTRA 9

intel vPRO

AI PCs built for business

In 2023, 133 million patient records were exposed in breaches reported to the U.S. Department of Health and Human Services Office for Civil Rights (OCR). This is the equivalent of 364,571 records breached each day. The number of data breaches reported to OCR has doubled in the past five years — from 369 in 2018 to 742 in 2023.[1]

New and evolving challenges for IT security in healthcare and life sciences

Ask any C-suite executive what keeps them up at night, and you can be sure cyberthreats are near the top of the list. That's particularly true in healthcare and life sciences.

Healthcare is consistently one of the highest targeted industries 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.

Clinicians rely on their workflows to deliver lifesaving patient care as quickly as possible. Because security is often woven into these workflows, a breach can have serious implications — potentially disrupting or delaying patient care.

Selling these records is a lucrative incentive for hackers and ransomware criminals. So it's not surprising that the rate of attacks on healthcare data has increased year after year.

Life sciences and pharmaceutical companies are equally at risk, especially as they continue to adopt digital transformation. In addition to clinical trials and other sensitive patient data, these organizations must protect valuable proprietary information. Yet their increased reliance on IT systems and an interconnected supply chain creates a higher exposure to cyber threats.

The rising cost of healthcare data breaches

For more than a decade, healthcare has experienced the highest cost of data breaches among all sectors. In 2024, the average cost of a healthcare data breach was $9.77 million, slightly more than double the $4.88 million average across all sectors.[2]

Ransomware-as-a-Service (RaaS)

As-a-service models have extended to cybercrime and are growing in popularity. RaaS lowers the technical barrier to entry, giving bad actors easy access to the resources for launching a ransomware attack by supplying malware and other tools on a pay-for-use basis.

An increasingly complex landscape

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

Expanded attack surface in remote and hybrid workplaces

Healthcare and life sciences have embraced remote and hybrid work for clinicians, scientists, administrators, and staff, whether delivering virtual care, working from home, or collaborating on the go.

While this holds many benefits, it makes securing devices and data more challenging. With more endpoints and more data in motion across more networks, the threat surface quickly expands. Wireless medical devices such as infusion pumps contribute to the challenge — since they use open airways to transmit data and update software, they create vulnerabilities for remote exploits.

Evolving, AI-driven environments

Emerging technologies such as artificial intelligence (AI) and machine learning (ML) are potential catalysts for medical innovation. Healthcare and life science organizations are embracing AI-powered solutions for diagnostic devices, healthcare analytics, drug discovery, remote patient monitoring, and more.

But this evolution brings new security concerns and further complexity to patient care and medical research environments. As they handle increasingly large and complex AI and ML workloads, healthcare and life sciences must safeguard their AI-powered environments to maintain patient and data security.

Regulations and compliance

Any technology solution must be evaluated with one additional criterion before it can be considered valuable for use in patient care and medical discovery: Does this solution help the organization comply with the highest regulatory standards? Technologies that meet security standards in other industries may not comply with patient privacy requirements across the globe, such as the US Healthcare Insurance Portability and Accountability Act (HIPAA), the German Patient Data Protection Act (PDSG), and the United Arab Emirates' Health Data Law.

Security vs. expedience

Increased security safeguards are being woven into the care delivery workflows while clinicians strive to deliver lifesaving patient care as quickly as possible. Layers of security could significantly disrupt or delay care delivery and negatively impact patient outcomes. Care providers should never have to sacrifice security for expedience or business performance.

A people-first approach to security

IT security must be seamless and ubiquitous, but it has to work the way clinicians, administrators, and medical researchers work. It must support and empower workers while protecting the organization and its data.

Lenovo ThinkShield: Security for the modern workplace

With Lenovo ThinkShield, security is foundational and layered to fully protect your organization, from below the OS to the cloud. We deliver complete protection at every level — wherever and whenever work happens — throughout the lifecycle of a device, including features such as:

- **Endpoint security**
- **Passwordless authentication**
- **Patch management**
- **BIOS security**
- **Remote management**

From supply chain assurance, to firmware integrity, to work-from-anywhere solutions and partnerships, our ThinkShield Portfolio offers integrated layers of protection.

We safeguard component integrity with rigorous standards in every step of our supply chain. And our hardware is engineered to be secure from the chip level up.

ThinkShield is designed to reduce IT workloads and downtime with fully integrated and tested solutions. Advanced predictive technology automates tasks that would otherwise be a burden. Our open ecosystem of leading partners adapts to your needs in a changing security landscape.

As a global technology leader, we bring the breadth and depth of our engineering legacy to deliver a better security experience. Our experts tailor solutions to meet the unique needs of healthcare and medical research environments. And the ThinkShield structure makes it easy to access the right combination of features for your organization's specific needs.

For the healthcare and life science IT environments, ThinkShield helps provide privacy, safety, and security for devices like the ThinkPad T14 laptop and the ThinkStation P1 workstation, powered by Intel vPro® Enterprise for Windows for an unrivaled healthcare PC solution.

intel CORE ULTRA 9 intel vPRO AI PCs built for business

Delivering complete protection wherever and whenever work happens

Security that adapts

- Seamless integration
- Work-anywhere protection
- Automated proactive prevention
- Privacy — keep patient data and clinician and researcher activity secure

Expertise you need

- Smarter security services
- Boundless data protection
- Asset management

Technology you can rely on

- Supply chain security
- Worry-free chip-level inspection
- Straightforward access protection

Lenovo

64%

increase in the frequency of ransomware incidents in 2023 compared to 2022, according to insurance claims[3]

277 days to detect and contain a data breach[4]

ThinkPad T14 for Healthcare

Many of these features are included on our ThinkPads, like the ThinkPad T14 for Healthcare, powered by Intel vPro® Enterprise for Windows, for an unrivaled healthcare PC solution. All the features on this page can be built into a variety of chassis based on your organization's needs.

intel CORE ULTRA 9 intel vPRO

AI PCs built for business

Privacy — keep patient data as well as clinical and research activity secure

Medical discovery and patient care delivery are constantly in motion, and security measures need to keep up. That's why we offer security features such as data protection and management, integrated security, and more.

ThinkShield Firmware Assurance

Many organizations struggle constantly with insufficient firmware attestation and deep visibility into their device fleet. Visibility is an essential principle of Zero Trust security, which has become a best practice across all sectors.

ThinkShield Firmware Assurance offers below-OS security visibility for your Lenovo devices, allowing your security operations team to monitor the firmware health of their Lenovo device fleet. It also prevents physical component tampering, system configuration changes, and malicious firmware installation, reducing the risk of hardware and firmware security breaches.

Data Protection and Management

ThinkShield PrivacyGuard

This solution 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 reduces the security burden for IT teams and employees.

ThinkShield Data Defense

Powered by Cigent, this solution protects data by enforcing Zero Trust-based access control with multifactor authentication (MFA) to prevent malware and bad actors from encrypting, exfiltrating, or destroying protected data.

- Prevent unauthorized data access.
- With the Shields Up™ mode, instantly prevent ransomware from wreaking havoc.
- Hide and encrypt endpoint data in secure vaults.

ThinkShield Data Eraser

Powered by Blancco, this solution meets full compliance and enhances security by automating data erasure routines that selectively erase data on active PCs and servers.

- Supports erasure of multiple file types: free space, recycle bin, temporary files, etc.
- Safely monitor and report on all erasure activity.
- Save time and resources with easy installation and scheduling of integrated erasure routines.

Lenovo

Privacy — keep patient data as well as clinical and research activity secure

ThinkShield Supply Chain Assurance

Our Supply Chain Assurance program adds extra visibility into device integrity, helping protect your PC investment and sensitive data from the factory floor to end of life.

- Protects against emerging supply chain threats.
- Provides supply chain transparency.
- Helps pinpoint counterfeit or dubious components.

ThinkShield Firmware Defense

Powered by Eclypsium, this solution allows you to inventory critical devices and firmware components that are heavily targeted.

- Identify device vulnerabilities and misconfigurations.
- Detect threats and compromises to device and supply chain integrity.
- Fortify devices with automated firmware updates and monitoring for unauthorized changes.

ThinkShield Hardware Defense

Powered by Sepio, this solution provides full visibility into all known and unknown assets across your network and endpoints — even those that lack unique identifiers and are difficult to detect using alternative methods.

- Gain deeper visibility by detecting and identifying all assets.
- Instantly detect hardware-based attack tools that evade existing security solutions.
- Establish trust and enforce hardware usage with granular risk-based access controls.

Lenovo ThinkShield Supply Chain Assurance with Intel Transparent Supply Chain was named **2024 Cybersecurity Product of the Year**

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.

Safety — keep patients and providers safe by reducing vectors of transmission

On any given day, healthcare-associated infections (HAIs) affect one in 31 US hospital patients and 1 in 43 nursing home patients.[5] But HAIs can be decreased by as much as 70% through prevention and cleaning practices.[6]

Lenovo made-for-healthcare devices — like the T14, powered by Intel vPro® Enterprise for Windows for an unrivaled healthcare PC solution — stand up to clinical environments and protect patients and providers. Devices can be cleaned, disinfected, and sanitized.

Lenovo ThinkPad and ThinkStation computing devices are tough and reliable. They undergo MIL-SPEC 810H testing, which includes methods and procedures covering low/high temperature, vibration, dust, and shock.

Lenovo devices also undergo extensive testing against CDC standards to withstand vigorous cleaning throughout the day. For detailed cleaning instructions, visit **www.lenovo.com/CleanPC.**

The **Lenovo Quick Clean** software application suspends user input from keyboards, touchpads, and touchscreens, allowing wipe-down without shutdown. The Lenovo Quick Clean timer can be customized to ensure adequate contact time for proper cleaning and disinfection.

Security — multifactor authentication

A cornerstone of any security practice is limiting patient data access to authorized users only. ThinkShield provides multiple ways to verify a user's identity, including frictionless multifactor authentication. Healthcare and life science organizations can select the factors that best meet their needs.

Facial recognition

IR cameras that enable Windows Hello facial and biometric login, as well as Mirametrix Glance presence detection

Passwordless MFA

Powered by Secret Double Octopus, passwordless authentication coverage across desktop, web, and corporate apps, and privileged access

Passwords and PINs

Built-in Windows multifactor authentication choices

Match-on-chip fingerprint reader

Secure storage and handling of all aspects of fingerprint authentication within a single chip

Geo-fencing security

Location-based, geo-fencing method of authentication that uses GPS and network location detection

FIDO2 support

Open and scalable standards from the FIDO industry alliance enabling simpler and more secure user authentication experiences on select ThinkPad devices

intel CORE ULTRA 9

intel vPRO

AI PCs built for business

Switching to single sign-on (SSO) saves time

In a typical day, clinicians and scientists log in and out of multiple applications, each requiring a username and password. SSO streamlines workflow, eases frustration, and allows for more time for patient care and medical discovery.

The ThinkPad® P1 workstation 5 powered by the Intel® Core™ Ultra processor and Intel vPro® delivers high performance and security on the go.

Lenovo

Security — real-time endpoint protection

ThinkShield has many offerings designed specifically for real-time endpoint protection within and beyond a healthcare or research facility.

AI endpoint protection

Real-time analysis and detection of security threats is needed more than ever before. Devices are now able to handle increasingly complex AI workloads, which reduces latency associated with cloud processing. With Sentinel One protection that leverages contextual AI, your endpoints are hardened to autonomously prevent, detect, and respond to modern-day risks and threats without impacting device performance.

As phishing attacks are often the main entry points, processing AI tasks directly on the device allows anti-phishing solutions to offer increased privacy as well as a faster response and threat mitigation. ThinkShield adds another layer of security with BUFFERZONE — AI-powered, email and web browser anti-phishing protection and threat isolation.

Data protection and encryption

Highly configurable, full-scale encryption solutions for the enterprise environment protect 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. Additionally, protect sensitive patient data with full disk encryption powered by WinMagic.

Endpoint visibility and control

Embedded directly into Lenovo device firmware, endpoint visibility and control solutions provide persistent security management, automating endpoint hygiene to support self-healing capabilities. Real-time remediation control powered by Absolute Secure Access allows remote investigation of potential threats and prompts action if a security incident occurs.

Better together

The Intel® Core™ Ultra processor integrates CPU, graphics processing unit (GPU), and neural processing unit (NPU) capabilities into a single package that accelerates AI on endpoint devices. This enables AI tasks to be processed locally rather than relying on cloud-based services, reducing the risk for data breaches.

The BUFFERZONE® NoCloud™ AI anti-phishing detection system harnesses the computational power of Intel® to use deep-learning engines to uncover malicious behaviors from different threat perspectives and stop evasive phishing attacks.

Security – from edge, to core, to cloud

ThinkShield solutions are part of Lenovo's end-to-end portfolio that enables healthcare and life science organizations to modernize their infrastructure so they can:

- Deploy a reliable, secure infrastructure
- Build a foundation for future-ready IT
- Power hybrid cloud, electronic health record platforms, and AI platforms
- Accelerate time to insight for clinical and administrative decision making
- Improve operational efficiency with advanced automation and management capabilities

Lenovo ThinkSystem servers

A wide selection, including rack, tower, edge, and mission critical servers, deliver a highly reliable, AI-ready infrastructure that allows clinicians and healthcare scientists to perform high-performance data analytics and run AI applications.

Lenovo ThinkEdge servers

Designed to be used as compute endpoints at the edges of your network, these systems operate outside of a traditional data center. ThinkEdge servers include capabilities that detect and protect them from attacks, ensuring that data is secure even in less-controlled environments.

Lenovo ThinkAgile platforms

These purpose-built appliances and fully integrated systems deliver streamlined computing and storage in a single solution, enabling healthcare and life science IT teams to simplify their IT infrastructure and accelerate time to value for clinicians and researchers.

Hybrid cloud computing

Our hybrid cloud solutions allow healthcare and life science organizations to maximize the full potential of their data, regardless of where it resides.

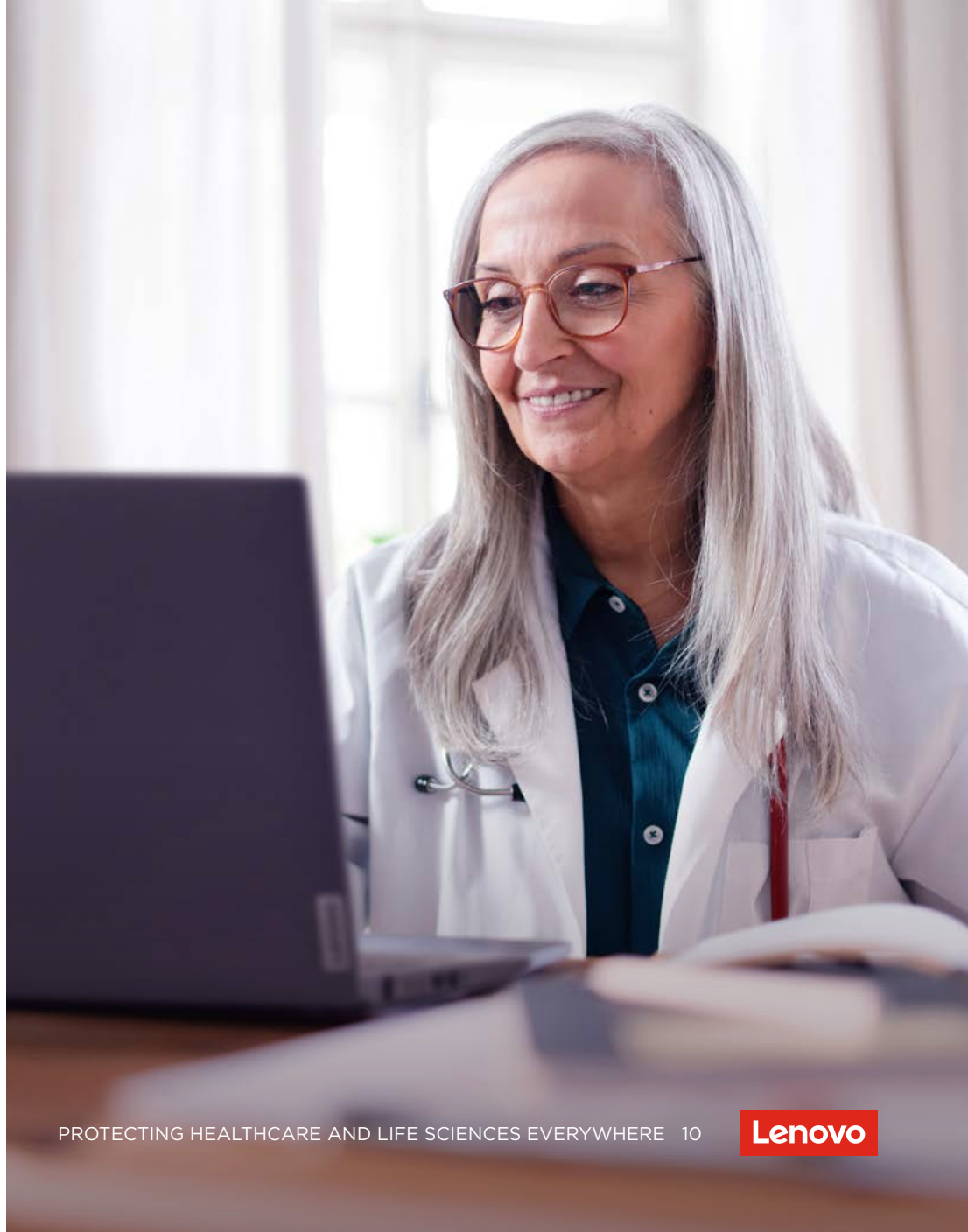
Lenovo servers have the best reliability among all x86 servers for the 10th consecutive year and the best x86 server security for the last five years.

Source
ITIC 2023 Global Security, Reliability Surveys

intel CORE ULTRA 9

intel vPRO

AI PCs built for business



Lenovo

Security Risk Assessment

Powered by C&H (Churchill & Harriman)

The security risk assessment is based on best practices and provides you with empirical evidence of identified gaps in the 17 basic security risks, allowing you to make sound security investment decisions.

The risk assessment can help you address:

- **Access control**
- **Identification and authorization**
- **Media protection**
- **Physical protection**
- **System and communication protection**
- **System and information integrity**

intel CORE ULTRA 9 intel vPRO

AI PCs built for business

Insurance — an important part of protection

Ransomware is skyrocketing across industries. As with other types of cybercrime, healthcare and life sciences are particularly vulnerable. Two-thirds of healthcare organizations surveyed in 2024 had been hit by ransomware.[7]

Healthcare and life science leaders are increasingly looking to insurance to mitigate the extreme financial consequences of an attack and payout. But policies are getting harder and more expensive to obtain — in large part because ransomware is the single-largest driver of cyber insurance claims and accounts for 62% of claimed incident costs.[8]

As insurers become more selective, organizations can improve their coverage options by building strong, demonstrable cyber defenses. Insurers want to see technology and procedures in place that safeguard the environment and defend against ransomware attacks. Minimizing risk can pave the way for lower premiums and more favorable coverage.

Consider a security risk assessment to help you identify your security gaps and guide your defense strategy against ransomware and other threats. A risk assessment can also help you enhance your security efficacy, make sound investment decisions, and meet regulatory requirements.

67%

of surveyed healthcare organizations were hit by ransomware in 2024.

62%

of cyber insurance claims are related to ransomware.

Built-in security helps organizations qualify for insurance — like the features on the ThinkPad T14 and ThinkStation P1, powered by Intel vPro® Enterprise for Windows for an unrivaled healthcare PC solution.

Lenovo

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 patient care and medical research environments and allow timely access to critical patient and research data when needed.

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

Powered by the Intel® Core™ Ultra processor that integrates CPU, GPU, and NPU capabilities, these devices can handle increasingly complex AI workloads. As AI and ML models evolve, having a dedicated NPU safeguards that the system can adapt to more advanced algorithms.

intel CORE ULTRA 9

intel vPRO

AI PCs built for business

Lenovo

Work smarter with Lenovo Health and Life Sciences

Connect with Lenovo Health and Life Sciences. 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 or visit **Lenovo.com/health**.

Sources

1 The HIPAA Journal, "Healthcare Data Breach Statistics," July 18, 2024
2 IBM Security, "Cost of a Data Breach Report," 2024
3 At-Bay, "The 2024 InsurSec Report: Ransomware Edition," 2024
4 IBM, "2023 Cost of a Data Breach," 2023
5 Centers for Disease Control, "HAI and Antimicrobial Use Prevalence Surveys," April 2024
6 SpringerLink, "Hospital Infection Prevention: How Much Can We Prevent and How Hard Should We Try?" 2019
7 Sophos, "The State of Ransomware 2024," 2024
8 NetDilligence, "Cyber Claims Study," 2023

intel CORE ULTRA 9

intel vPRO

AI PCs built for business