Protected. Productive. Prepared.

Cybersecurity guide for
healthcare and life sciences

AMD

Windows 11

Smarter
technology
for all

Lenovo

Do you need an Rx for security threats?

Protecting healthcare and life sciences data is essential for patient privacy and intellectual property, but it's becoming increasingly difficult. Healthcare cyberattacks remain rampant and breaches are longer-lived and more costly than in any other industry.

1,607 weekly attacks in North America, up 20% in a year[1]

$9.77M cost per incident[2]

258 days to identify and contain[2]

The consequences of healthcare breaches go beyond financial, regulatory, and reputational, with more than 60% reporting a moderate or substantial impact on care delivery.[3] The reach of attacks has now expanded to supply chains.

64% averaged 4 supply chain attacks in the last 2 years[4]

77% say they impacted patient care[4]

With the growing cybersecurity skills gap and shortage of qualified talent, healthcare organizations are hard-pressed to defend against the threats coming at them.

94% report a cybersecurity skills gap[5]

3 in 5 say dearth of cybersecurity staff is their biggest challenge[6]

Adding to the challenge is an ever-expanding attack surface from today's highly mobile and hybrid clinicians and staff.

Organizations need to do more than simply react to cyberthreats. They need multilayered security that's proactive, automated, and smart enough to self-heal. Deploying modern technology solutions with the latest security features delivers protection today and takes healthcare organizations safely into a secure future without compromising end-user productivity.

Partnering for performance and protection

Compute endpoints are a critical attack vector for today's cybercriminals. As demand escalates for more sophisticated and effective defenses, innovations at the CPU level are contributing to the security landscape.

Lenovo's strong partnership with leading chipmaker AMD delivers feature-rich security perfect for clinical, research, and drug manufacturing environments.

AMD

Windows 11

Lenovo ThinkShield®: Built-in, adaptive security

- Transparent Zero Trust supply chain
- Built-in security from the chip level up
- Advanced predictive technology and task automation
- AI-driven real-time detection and response
- Firmware-embedded endpoint visibility and control
- Configurable, full-scale encryption
- Next-gen antivirus protection powered by patented behavioral AI
- Physical device privacy protection features and multifactor authentication
- Customizable global security services
- Secure wipe and Keep Your Drive options

ThinkShield defends at every level

- ✓ From OS to cloud
- ✓ Below the OS
- ✓ Supply chain assurance

To learn more about ThinkShield for healthcare, click here.

AMD PRO security: Integrated on-chip security features

- AMD Secure Processor to improve data and application integrity
- AMD Shadow Stack to protect against control-flow attacks
- AMD Platform Secure Boot to continue the chain of trust from the system BIOS to the OS Bootloader
- Microsoft Pluton™ security processor with built-in, next-gen security including TPM 2.0

Unlock AI's potential — securely

As with most industries, artificial intelligence holds tremendous promise for healthcare and life sciences. From diagnosis to treatment, clinical workflows to patient experience, medical research to drug discovery, AI has potential to transform clinical efficiency, outcomes, and how effectively organizations can secure devices and data.

But with the rewards come risks. With its vast volumes of data, AI expands the attack surface, introducing risks like data poisoning and model inversion and challenges like diverse data integration, AI hallucinations, and evolving regulations.

At the same time, AI can be used to automate and streamline threat intelligence, device behavior analytics, and more — helping organizations to more confidently mitigate cyber risks.

67% of healthcare executives surveyed aren't confident in their IT systems' ability to protect the integrity of patient data.[7]

AI solutions must be built on a foundation of strong governance and robust security measures to be responsible, ethical, and trustworthy. Lenovo's security by design establishes this foundation, starting with supply chain assurance to protect your devices from the component level up. Our hybrid AI approach balances on-premises and cloud processing to protect sensitive data. And Lenovo AMD-powered devices give you the performance to power AI-driven security solutions.

Lenovo ranks #10 in the Gartner Supply Chain Top 25 for 2024 list of global companies with exceptional supply chains.

Lenovo's AI-based Cyber Resiliency as a Service (CRaaS) uses Lenovo device telemetry and the Microsoft security software portfolio, including Microsoft Copilot for Security and Defender for Endpoint, to integrate greater visibility with cyber protection, detection, response, and recovery across digital estates and devices.

Our technology services include Lenovo Device Intelligence, Asset Recovery, and Security Services.

AMD Windows 11

The most secure version of Windows yet

Microsoft Windows 11 has powerful built-in protections that seamlessly complement Lenovo and AMD solutions to enhance cybersecurity.

- ✓ Zero Trust-ready operating system to protect data and access anywhere
- ✓ Integrated hardware and OS safeguards
- ✓ Cloud configuration to simply secure devices for curated apps and access
- ✓ App compatibility and cloud management for easy adoption
- ✓ TPM 2.0 security chip turned on by default
- ✓ Pre-enabled virtualization-based security (VBS) and hypervisor-enforced code integrity (HVCI) to safeguard the OS and information stored in memory
- ✓ Simplified steps to deploy Windows Hello for Business* to make passwordless protection easier

reduced risk of successful security attack[8]

99.6%

Lenovo Windows 11 devices are compatible with 99.6% of security applications.[9]

Be sure to upgrade to Windows 11 before the October 14, 2025 end of support deadline.

AMD Windows 11

Gain more control over security

- Deploy, secure, and manage devices remotely from the cloud
- Simplify patient device delivery and save time and money with zero-touch deployment, including hospital security policies**
- Apply the same security policies to all devices with expanded support for group policy administrative templates in MDM solutions like Microsoft Endpoint Manager**

Put the combined security of Lenovo ThinkShield, AMD Ryzen™ PRO, and Windows 11 to work in your organization

Secure VDI

ThinkCentre® M75q Tiny desktop

Perfect for virtual desktop infrastructure needs with IGEL endpoint OS support

Ideal for in-room patient care, mobile medical carts, and nursing stations

- Powered by AMD Ryzen™ PRO desktop processors
- Lenovo ThinkShield and AMD PRO security
- Kensington™ cable lock slot to prevent theft

Secure AI

ThinkPad® T14s Gen 6 laptop

AI PC with performance for Microsoft Copilot features

Ideal for AI-driven processes for operational efficiency, clinical workflows, and administrative tasks

- Powered by AMD Ryzen™ AI PRO 300 Series processor with 50 TOPS
- Lenovo ThinkShield and AMD PRO security
- Microsoft Pluton hardware-based root of trust, secure identity, and cryptographic services

Secure EPIC

ThinkSystem® SR665 V3 server

General-purpose server validated to host EHR deployments

Ideal for powering your EPIC EHR system

- Powered by AMD EPYC™ processors
- Lenovo ThinkShield
- Supports AMD Secure Root-of-Trust, Secure Run, and Secure Move features
- XClarity Systems Management simplifies security-related tasks like patching

> **"Lenovo ThinkSystem servers [have provided] the best x86 server security for the last five years."**
>
> Information Technology Industry Council
>
> 2023 Global Server Hardware, Server OS Security Report

AMD Windows 11

Strengthen your cyber resilience

Pair Lenovo ThinkShield-protected solutions powered by AMD processors and Windows 11 with these cross-industry best practices to close security gaps and strengthen your environment.

End-to-end security-aware culture

- ✓ Adopt a Zero Trust model to prevent unauthorized access
- ✓ Provide training on email safety, device hygiene, and attack protocols
- ✓ Develop an incident response (IR) plan

Proactive, adaptive security

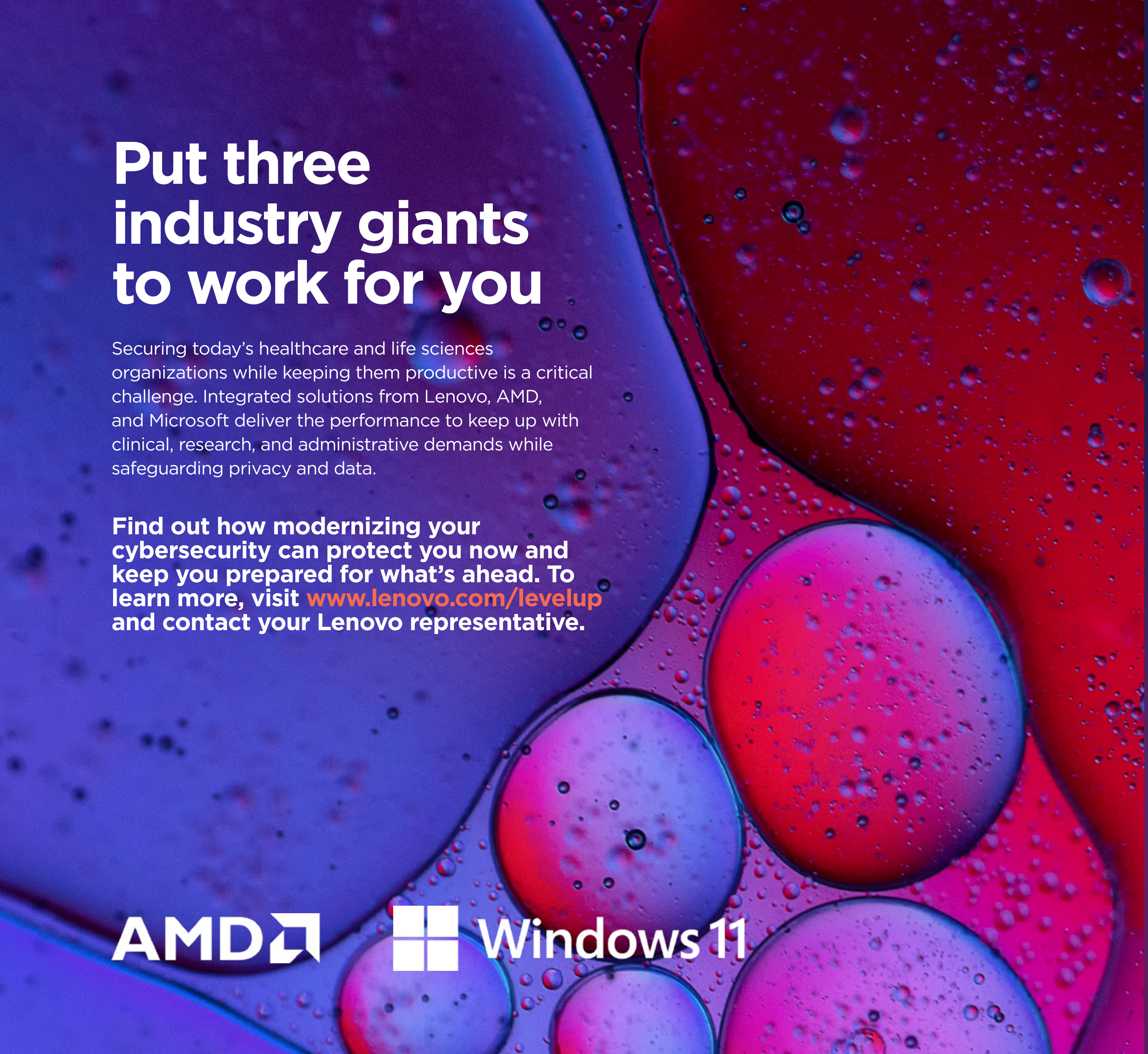
- ✓ Adopt AI-driven and machine learning-based security

Encrypt all data from end to end

- ✓ Audit clinical data provenance and ownership

Responsible technology resource management

- ✓ Choose a trusted partner with full-lifecycle protection in line with your security goals
- ✓ Create digital workspaces where clinicians, staff, and administrators can securely collaborate from anywhere
- ✓ Securely dispose of devices to ensure data protection



Put three industry giants to work for you

Securing today's healthcare and life sciences organizations while keeping them productive is a critical challenge. Integrated solutions from Lenovo, AMD, and Microsoft deliver the performance to keep up with clinical, research, and administrative demands while safeguarding privacy and data.

Find out how modernizing your cybersecurity can protect you now and keep you prepared for what's ahead. To learn more, visit www.lenovo.com/levelup and contact your Lenovo representative.

AMD

Windows 11

Sources

1 Checkpoint Research, September 2024
2 IBM Security, "Cost of a Data Breach," July 2024
3 Claroty, "The Global Healthcare Cybersecurity Study," 2023
4 Ponemon Institute, "Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care," 2023
5 International Information System Security Certification Consortium, "2024 ISC2 Cybersecurity Workforce Study," 2024
6 HIMSS Healthcare Cybersecurity Survey, 2023
7 MedCity News, "Healthcare's Data Problem: So Much Data, Yet So Little Data Fidelity," June 2024
8 Forrester, "The Total Economic Impact™ of Windows 11 Pro Devices," December 2022
9 App Assure program data from October 2018 to February 2022

* Requires TPM 2.0 or greater.
** Requires Active Directory and internet connection.

Smarter technology for all

Lenovo