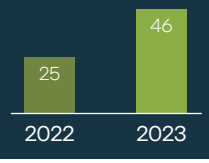
Addressing the Fast-Evolving Threat of Ransomware in Hospitals

Intel helps hospital systems reduce ransomware risks that compromise both patient safety and the organization's financial well-being. Product security assurance and innovative hardware features and capabilities combine to protect hospitals and preserve operational continuity.

Ransomware attacks against hospitals are an escalating threat causing significant harm to both institutions and patients. An 84% increase in hospital systems affected from 2022 to 2023[1] demonstrates the rapid development of the hazard. Attacks compromise operations and threaten patient outcomes by taking critical systems offline, from electronic health records, to lab testing, to billing systems. Recent attacks on hospitals have been devastating medically and financially, interfering with life-saving procedures, critical medications and submission of insurance claims for payment.[2]

Often initiated by tricking staff into installing malware by means of social engineering, ransomware attacks work by encrypting critical data and then demanding a ransom to provide the decryption key. Meanwhile, entire hospital systems struggle to function. Notably, there is no guarantee that paying the ransom will cause the criminals to reverse the attack in good faith, which can leave victim organizations with little or no recourse.

Hospital Systems Affected by Ransomware[1]



Average Ransom Payment[3]

2022: **$5,000**

2023: **$1.5M**

As ransomware has become more lucrative for perpetrators in recent years, it has evolved to become more sophisticated at the hands of well-financed international criminal gangs, many of which are funded by state sponsors. As a result, attacks are better able to evade security controls, making them more challenging to detect and interrupt. Intel helps mitigate these hazards through both operational measures and hardware security features.

Hospital Endpoints are Highly Vulnerable to Ransomware[4]

- **53%** have a known critical vulnerability
- **33%** have an identified critical risk
- **73%** of IV pumps have an exploitable vulnerability
- **21%** are secured by weak or default credentials

Hardware and ecosystem protections against ransomware

Intel platforms provide hardware-enabled security features, enabled by partner software, that help protect the security and privacy of sensitive health data. An IDC study finds that Intel-powered platforms reduce security risk, increase the efficiency of security teams and enable organizations to experience fewer security events.[7] Co-engineering with the security software ecosystem enables security tools to take advantage of features and capabilities built into Intel silicon, for a full-stack solution to protect against ransomware and other attacks.

Security Outcomes: Intel® Hardware Features and Capabilities[7]

- **26%** fewer major security breaches
- **17%** higher security team efficiencies
- **21%** fewer impactful security events

Monitor endpoints and detect ransomware attacks

Hardware-based monitoring built into Intel platforms enhances endpoint detection and response (EDR) solutions to detect malicious activity. Intel® Threat Detection Technology (Intel® TDT) is powered by an industry-leading AI model trained on the latest tactics and techniques employed by cyber criminals. This hardware-based capability monitors code as it executes, applying pattern matching from the CPU's point of view to identify patterns of malicious behavior in both known and unknown malware. This is also critical evidence that can be used to detect insidious living-off-the-land attacks, which leave little or no detectable signature without Intel TDT.

Leading security providers are enabling their tools for Intel TDT, providing a combined hardware-software solution with more comprehensive protection than software alone. Intel TDT delivers almost no impact to system performance and can be offloaded to a GPU or to the neural processing unit (NPU) of an AI PC, to reduce CPU utilization and the impact of these measures on everyday operations.

Protect against and contain ransomware attacks

Standardize and maintain security posture across the enterprise with 24/7 remote access regardless of system state. Intel® vPro™ technology provides out-of-band management capabilities to systems even when they are switched off, enhancing ransomware defenses with up-to-date patches and security software. Intel vPro platforms can make client environments more resilient to attack by enabling remote re-imaging that is orders of magnitude faster than manually touching each system. The technology can also help limit the reach of ransomware outbreaks by detecting when critical security applications fail or stop running and isolating affected machines from the rest of the network.

Mitigating vulnerabilities with Intel's product security assurance

Intel's secure product development lifecycle incorporates security considerations at every stage of product development, from initial planning through release and post-deployment support. More than 500 dedicated security staff embed these practices into corporate processes and create a security-first work culture, supported by routine hands-on training events. These measures contribute to the conclusion by ABI Research that Intel product security assurance leads the silicon industry.[5]

Systematic and continuous modeling of security vulnerabilities at every stage is a core aspect of Intel product development, supported by ongoing analysis, remediation and verification. In addition, its Vulnerability Discloser Program has been a major contributor to Intel's overall proactive security leadership, distributing bug bounties to elite ethical hackers who identify novel security threats. Intel engages hundreds of researchers from throughout the industry, and this program proactively identified 94% of the vulnerabilities disclosed in 2023.[6]

> A competitive assessment of product security assurance by ABI Research ranks Intel as the top innovator and implementer among the five semiconductor companies considered.[5]

Intel maintains a robust program to maintain supply chain security that includes proactive certification and auditing of key suppliers and vendors. The company also invests extensively in personnel and practices as part of its "Security-First Pledge," which prioritizes customer needs in security decisions to help protect hospitals from ransomware and other security threats.

> In 2024, Intel's closest competitor had **3x more** platform firmware vulnerabilities than Intel. Intel achieved a **39% reduction** in combined hardware and firmware vulnerabilities in 2023 compared to 2022.[6]

Conclusion

Intel practices and technologies help guard hospitals against the rising levels of ransomware attacks that threaten the systems they rely on to provide care and keep the business running. Features built into the silicon, including Intel TDT, work with the rest of the security ecosystem to provide full-stack protection. Intel TDT-enabled platforms are just one aspect of a balanced approach to security and privacy that includes physical, administrative and technical safeguards. Intel's product security assurance systematically identifies hardware and software vulnerabilities in Intel products. As ransomware threats continue to evolve and intensify for the foreseeable future, these measures provide a foundation for hospitals to harden their defenses and protect themselves.

Learn more

Intel Healthcare and Life Sciences Solutions
Intel Security
Intel Threat Detection Technology

[1] EMSISOFT Malware Lab, January 2, 2024. "The State of Ransomware in the U.S.: Report and Statistics 2023." https://www.emsisoft.com/en/blog/44987/the-state-of-ransomware-in-the-u-s-report-and-statistics-2023/.

[2] Reuters, March 7, 2024. "Patients or payroll? US healthcare hack creates hard choices." https://www.reuters.com/world/us/patients-or-payroll-us-healthcare-hack-creates-hard-choices-2024-03-06/.

[3] The HIPAA Journal, January 4, 2024. "At Least 141 Hospitals Directly Affected by Ransomware Attacks in 2023." https://www.hipaajournal.com/2023-healthcare-ransomware-attacks/.

[4] US Federal Bureau of Investigation Cyber Division, September 12, 2022. "Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities." https://www.ic3.gov/Media/News/2022/220912.pdf.

[5] ABI Research, February 2024. "Embracing Security as a Core Component of the Tech You Buy." https://go.abiresearch.com/hubfs/ABI_Research%20Embracing%20Security%20As%20A%20Core%20Component%20of%20The%20Tech%20You%20Buy%20v5.pdf.

[6] "Intel 2023 Product Security Report." https://www.intel.com/content/www/us/en/security/intel-2023-product-security-report.html.

[7] Based on IDC's "The Business Value of Intel Security for PCs" report published March 2023 (commissioned by Intel), which cites greater reported efficiencies around security-related implementations and responses with Intel-based PCs versus other PCs. https://www.intel.com/content/dam/www/central-libraries/us/en/documents/2023-03/idc-the-business-value-of-intel-security-for-pcs-whitepaper.pdf.

0924/GR/MESH/PDF 356890-001US