Clearwater

Know Your Risk

What Asset-Based Risk Analysis Is Revealing About Healthcare Cybersecurity

powered by

IRM | Analysis®

Clearwater Bulletin | August 2025

Table of Contents

Cyber threats against healthcare organizations continue to grow in scale and sophistication. As the threat landscape evolves, so too must the approach to identifying and managing risk.

Clearwater's asset-based risk analysis, conducted using its IRM|Analysis® software, offers a detailed view of where healthcare organizations are most exposed. Across hospitals, health systems, ambulatory care centers, and digital health platforms, the same categories of weakness are appearing consistently:

- Insufficient identity and access controls
- Underprotected endpoint devices
- Misconfigured cloud-based applications and services

These recurring issues are not only widespread but often avoidable. They reflect structural gaps that adversaries continue to exploit.

This bulletin summarizes findings from Clearwater's most recent OCR-Quality® Risk Analyses and provides an overview of the most commonly observed vulnerabilities, the systems most frequently targeted, and key implications for healthcare cybersecurity and risk management leaders.

Why Asset-Based Risk Analysis Matters More Than Ever

Healthcare environments are inherently complex. Organizations manage legacy infrastructure, cloud-based platforms, third-party integrations, and medical devices—each introducing different types and levels of risk. At the same time, they must protect large volumes of protected health information (PHI) and meet evolving regulatory requirements.

Traditional, one-size-fits-all risk assessments often fail to account for this complexity. They provide high-level snapshots that overlook the interdependencies between systems, the uneven distribution of risk, and the specific vulnerabilities that adversaries are most likely to exploit.

Clearwater applies an **asset-based risk analysis** methodology, grounded in the NIST SP 800-39 risk management framework and implemented through its IRM|Analysis® software. This approach evaluates risk at the system component level, considering how specific threats, vulnerabilities, and business impacts intersect.

During the analysis phase, IRM|Analysis generates threat-vulnerability

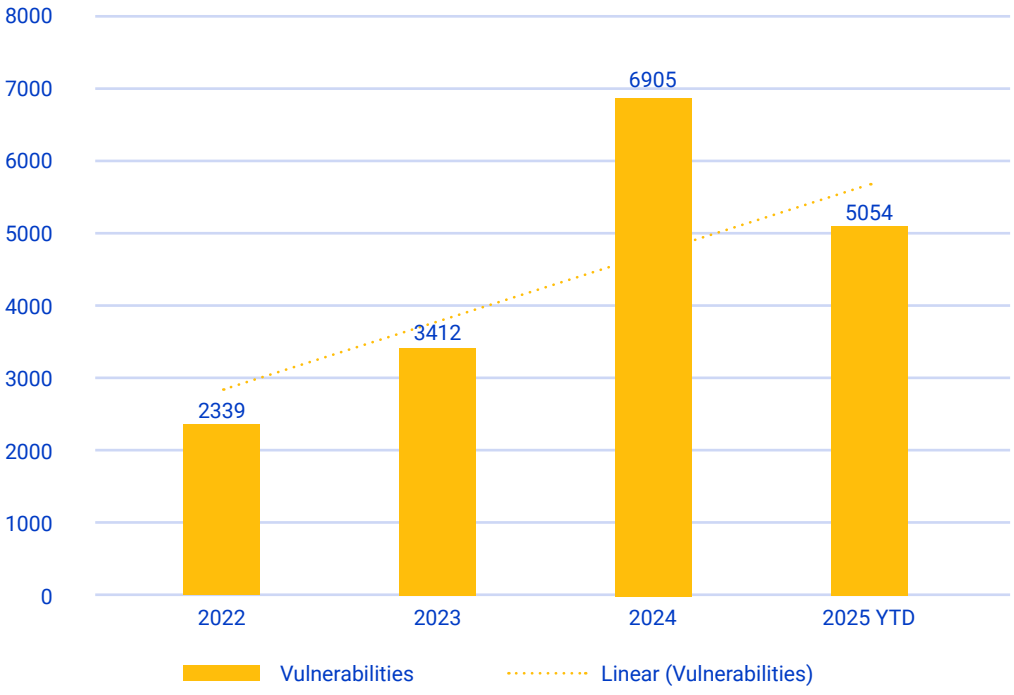
combinations for each asset based on its technical characteristics. Likelihood and impact scores are developed using AI-enhanced logic and expert judgment. The result is a quantified risk score that maps directly to business and compliance objectives.

This level of detail provides a more accurate view of an organization's attack surface, highlighting which risks pose the greatest threat and which gaps should be prioritized for mitigation.

Vulnerabilities Are Rising Sharply Across Healthcare

Since 2022, Clearwater has identified a **nearly 200% increase** in high and critical vulnerabilities during asset-based risk analysis. This trend highlights the growing complexity of healthcare systems — **and the limitations of traditional assessments in addressing today's threat landscape.**

Vulnerabilities Identified from Risks Above the Threshold (Critical and High Risks)



Clearwater's 2025 Findings: The Threat Is Where the Data Lives

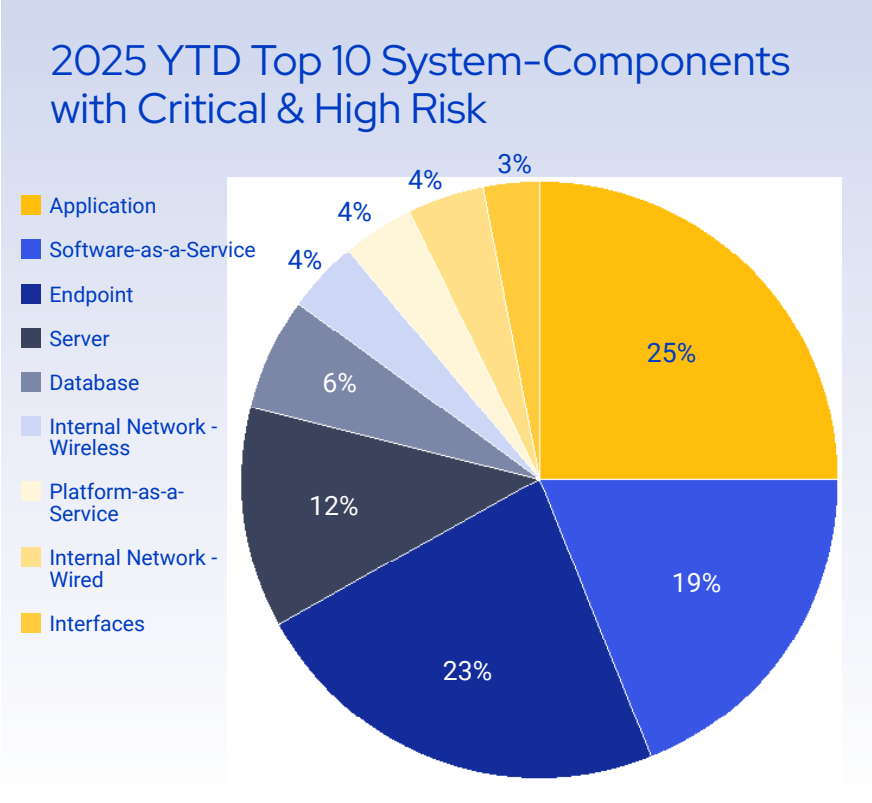
Across hundreds of OCR-Quality® risk analyses conducted in 2024 and 2025, Clearwater has found a consistent pattern: adversaries are focusing their attacks on the core systems that store, process, and transmit sensitive data.

These include:

- Applications and SaaS platforms
- Endpoint devices (e.g., laptops, tablets, mobile devices)
- Cloud services and PaaS environments
- Identity and access management systems

In fact, **Clearwater has found that more than 67% of high and critical risks across healthcare organizations originate from Application, SaaS, and Endpoint components.** In digital health companies, that number climbs to 80%.

This makes intuitive sense—attackers want data, and these are the systems that contain or connect to it.



Top Vulnerabilities Being Exploited

Clearwater's asset-based analysis also has revealed the specific vulnerabilities most likely to be exploited in today's threat environment. The five most common across all segments of healthcare are:

User Authentication Deficiencies

Weak or missing multifactor authentication (MFA), shared credentials, and

unmonitored login activity remain pervasive, making it easy for attackers to gain unauthorized access.

Dormant Accounts

Inactive or orphaned accounts are often left open and unmonitored, providing attackers with stealthy entry points — especially in hybrid IT environments where deprovisioning processes are inconsistent.

Excessive User Permissions

Many organizations fail to adhere to the principle of least privilege, giving users access to more data and systems than necessary. This significantly increases the blast radius of any compromise.

Untrained Staff

Social engineering and phishing attacks remain highly effective because staff are not consistently trained on how to recognize and report threats.

Network Configuration Deficiencies

Flat networks, open ports, and misconfigured firewalls or VPNs allow lateral movement once an attacker gains initial access — dramatically increasing the potential damage.

These vulnerabilities are not new — but the consistency with which they are exploited across environments should concern every healthcare CISO and compliance officer.

67% of hospital risk stems from endpoints, applications, and SaaS. Most common vulnerabilities:

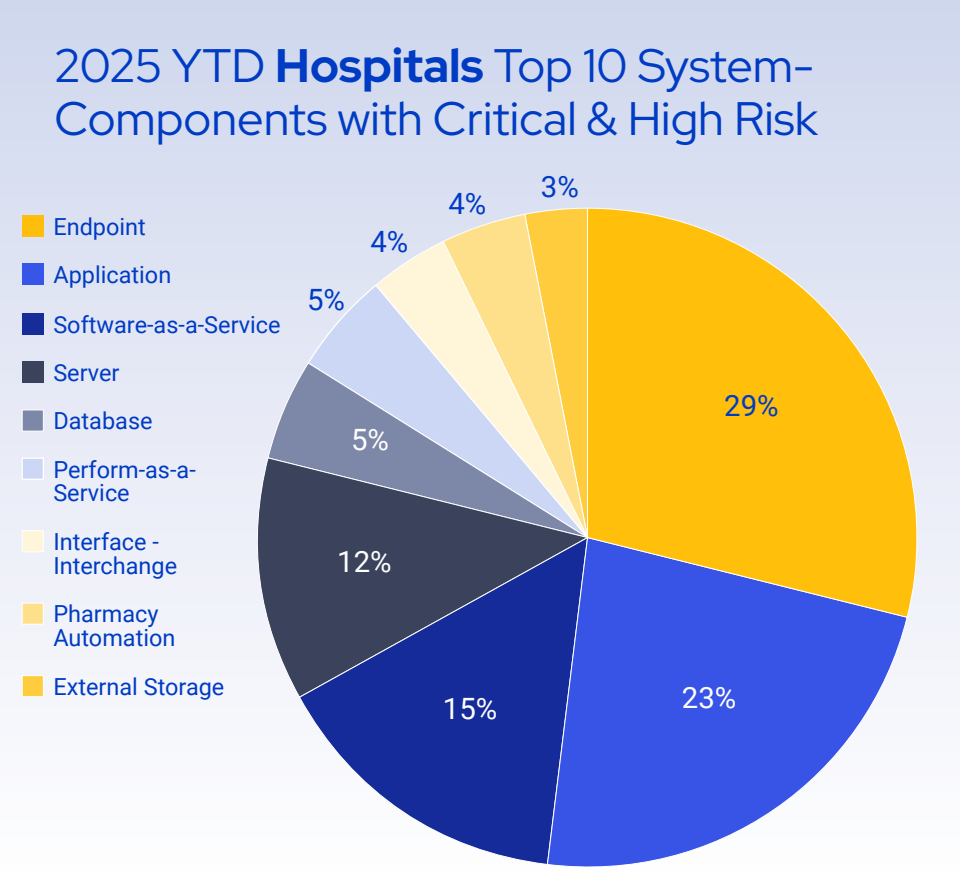
- **Dormant accounts**
- **Weak authentication**
- **Excessive permissions**

Hospitals, Physician Groups, and Digital Health: Shared Risks, Sector-Specific Gaps

While these vulnerabilities cut across the healthcare spectrum, Clearwater's analysis reveals some sector-specific insights:

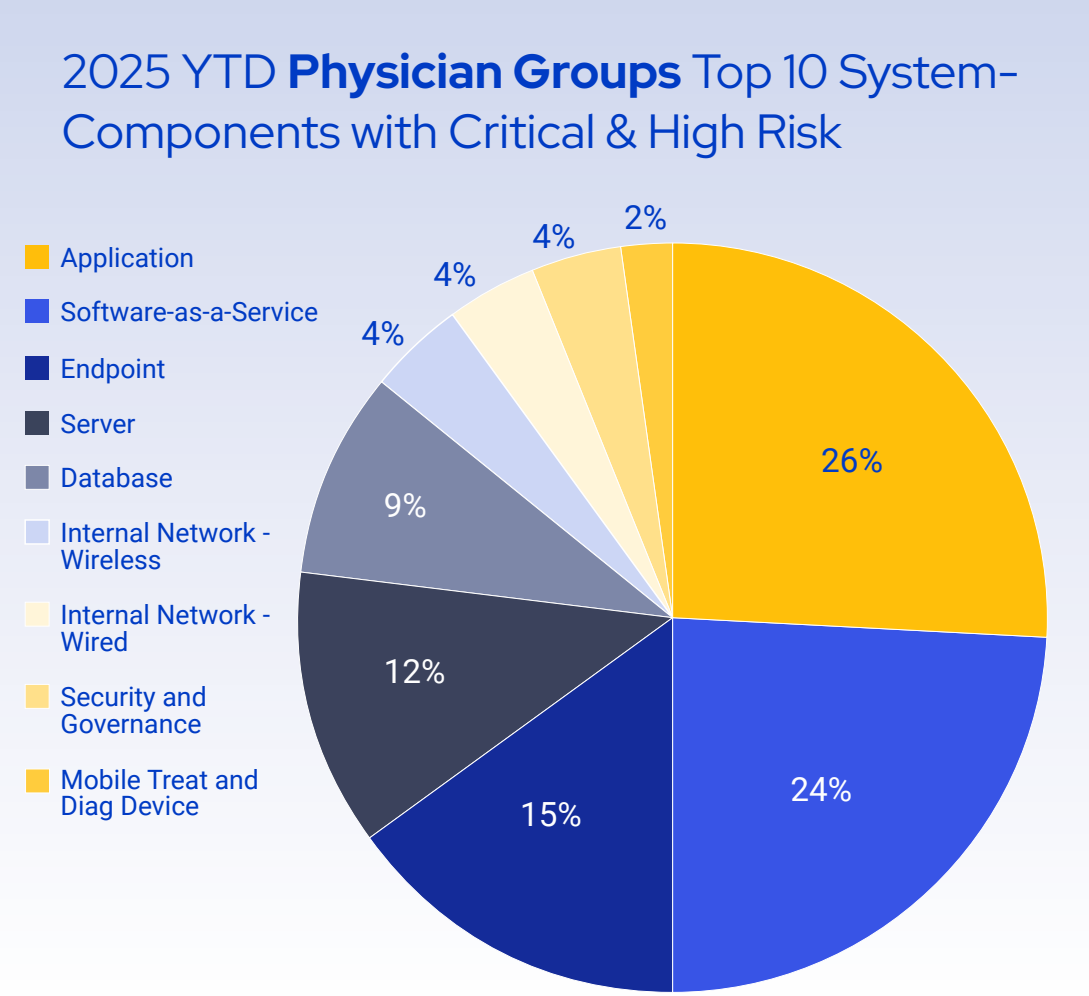
Hospitals

67% of high-risk findings stem from endpoint, application, and SaaS systems. Hospitals often struggle with aging infrastructure and sprawling user bases. Authentication deficiencies and poor permissions management are compounded by contractual weaknesses — such as unclear vendor security requirements.



Physician Groups

In ambulatory environments, the most common risks are tied to network configuration deficiencies and authentication gaps. Smaller IT teams often lack the resources to conduct thorough reviews of firewall rules, remote access, or software patching. These weaknesses make physician practices attractive soft targets for ransomware groups.



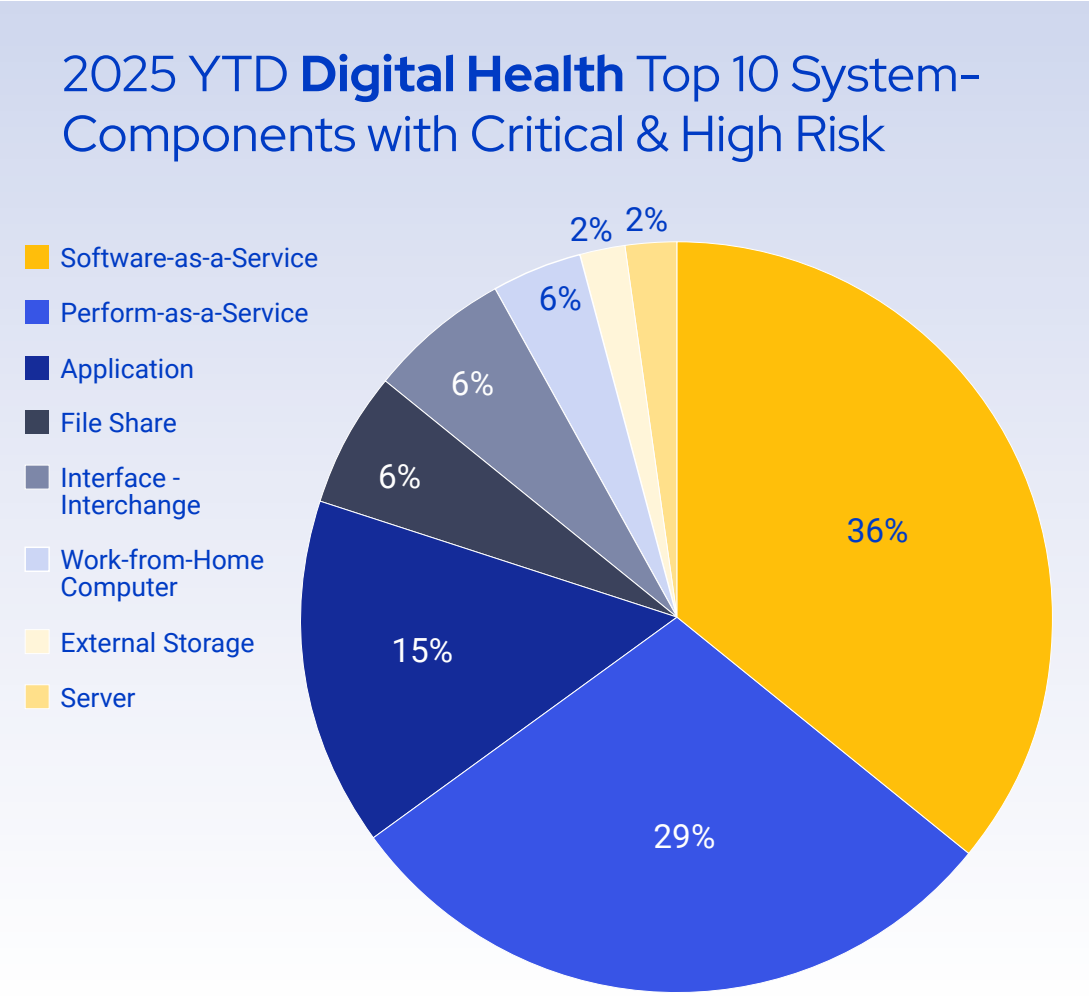
65% of risk is tied to endpoint, SaaS, and application systems.

Most exploited weaknesses include:

- **User Authentication Deficiencies**
- **Dormant accounts**
- **Weak authentication**
- **Excessive permissions**

Digital Health Organizations

Startups and SaaS providers, especially those scaling rapidly, frequently have sophisticated cloud stacks — but lack disciplined identity management and secure DevOps pipelines. Clearwater's findings show that 80% of high and critical risks in digital health originate from application and cloud components. Dormant test accounts, misconfigured APIs, and inadequate monitoring expose these systems to both adversarial and accidental threats.



In digital health, 80% of high-risk components are SaaS, PaaS, or applications. Top vulnerabilities:

- **Dormant accounts**
- **User Authentication Deficiencies**
- **Data Leakage**

Real-World Implications: When Risk Becomes Reality

Recent cybersecurity incidents across the healthcare sector illustrate how commonly observed vulnerabilities are being actively exploited — with significant operational, financial, and privacy consequences.

Ransomware attack at a large health system: An outdated user account, never deactivated following employee departure, was used to gain unauthorized access to internal systems. The breach resulted in widespread disruption and regulatory notification obligations.

Data exposure at a digital health platform: Overly permissive access controls allowed external developers to access and download protected health information (PHI). The exposure went undetected for an extended period, highlighting gaps in access monitoring and vendor oversight.

Business email compromise at a physician group: A phishing email successfully targeted an untrained employee. The attack led to fraudulent invoice payments and unauthorized disclosure of sensitive information.

Each of these incidents reflects a failure to identify and remediate basic, high-impact vulnerabilities — many of which are consistently flagged in Clearwater's asset-based risk analyses.

These cases reinforce the need for continuous, component-level risk analysis practices that inform timely mitigation efforts. Risk analysis must be more than a compliance exercise—it must serve as an operational decision-making tool.

How IRM|Analysis Enables Better Decisions

Clearwater's IRM|Analysis® platform enables a structured, repeatable approach to cyber risk management — supporting both regulatory alignment and operational decision-making.

The software provides healthcare organizations with the ability to:

Conduct a comprehensive **inventory of information systems** and assess their business criticality

Evaluate **threats and vulnerabilities** at the individual asset level

Prioritize risk response based on likelihood, impact, and regulatory exposure

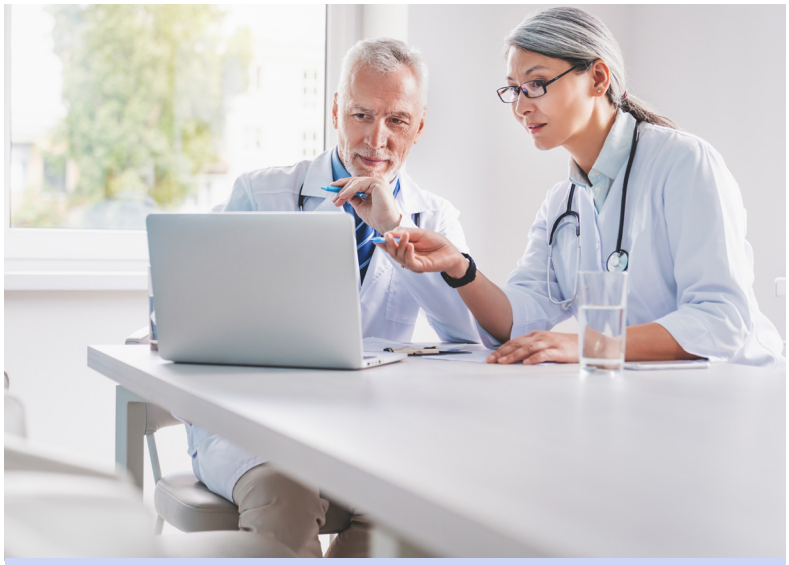
Map results to industry frameworks such as the **NIST Cybersecurity Framework, HIPAA Security Rule, and 405(d) Health Industry Cybersecurity Practices**

Assign risk ownership and track remediation progress across business units

By generating a clear, component-level view of risk, IRM|Analysis supports more informed investment decisions, improves alignment between cybersecurity and business strategy, and strengthens an organization's ability to demonstrate ongoing compliance.

What Healthcare Leaders Should Do Now

- Inventory your assets and dependencies
- Know what systems you rely on, who owns them, and how they connect to sensitive data.
- Conduct OCR-Quality Risk Analysis annually or continuously
- Assess risk at the component level, not just through high-level surveys or checklists.
- Remediate foundational vulnerabilities
- Implement strong MFA, retire dormant accounts, and reduce user privileges across the board.
- Enhance workforce awareness
- Train all staff regularly on phishing and basic cyber hygiene—and test their awareness
- Demand risk transparency from vendors
- Include risk analysis requirements and reporting expectations in all new contracts



Be at the leading edge of healthcare cyber security.

Final Thought: See Risk Clearly Before It's Too Late

While cyber threats continue to evolve, many of the most damaging incidents stem from long-standing and well-understood vulnerabilities. Clearwater's asset-based risk analysis findings consistently show that fundamental security gaps — such as misconfigured access controls, inactive user accounts, and excessive permissions — remain the primary drivers of risk.

Addressing these issues requires more than periodic assessments or compliance checklists. A continuous, component-level risk analysis approach offers a clearer view of where risk resides, how it may be exploited, and what actions are most urgent.

By adopting this methodology, healthcare organizations can strengthen their cybersecurity posture, support regulatory readiness, and improve overall resilience.

For more information about Clearwater's asset-based risk analysis and the IRM|Analysis® platform, contact info@clearwatersecurity.com or visit www.clearwatersecurity.com.

Clearwater helps organizations across the healthcare ecosystem move to a more secure, compliant, and resilient state so they can achieve their missions. The company provides a deep pool of experts across a broad range of cybersecurity, privacy, and compliance domains, purpose-built software that enables efficient identification and management of cybersecurity and compliance risks, managed cloud services, and a 24/7 Security Operations Center with managed threat detection and response capabilities.