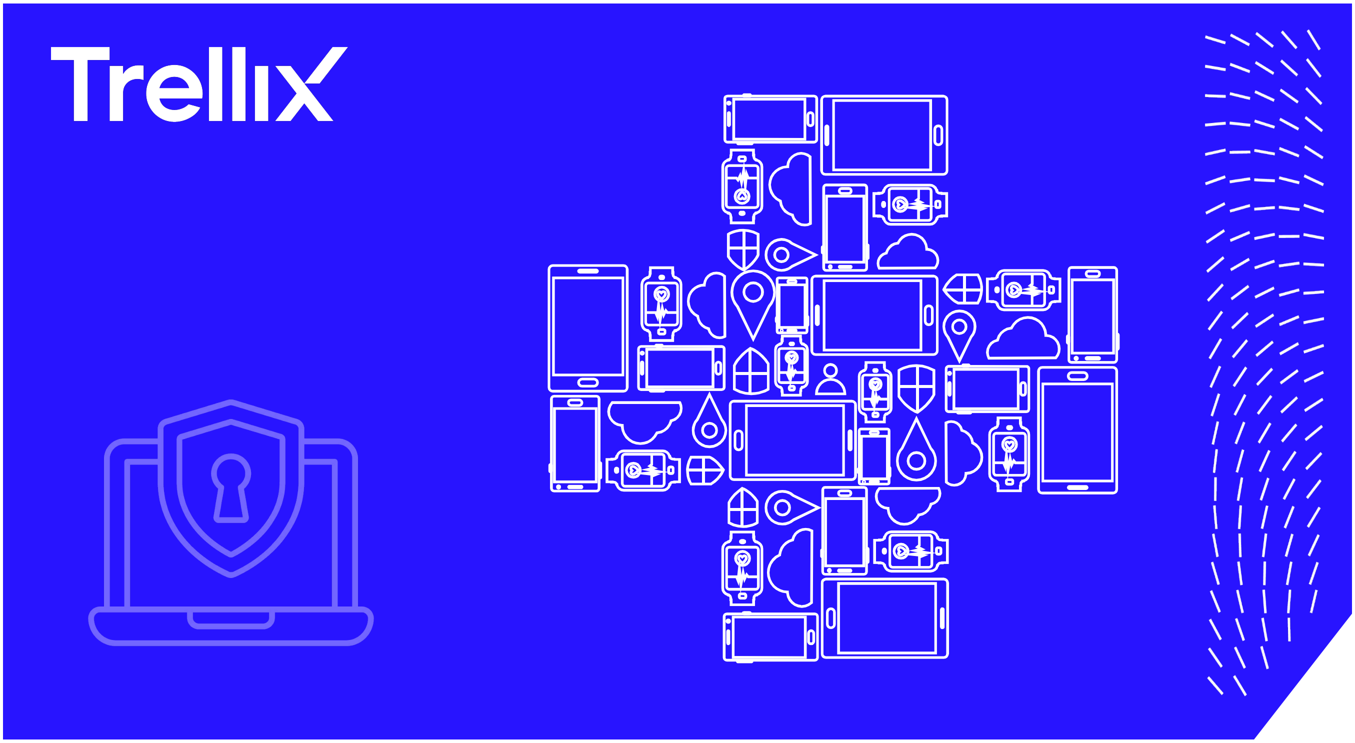


Trellix® Healthcare Executive Perspective

Building Cyber Resilience
with the Trellix Healthcare Security Suite

A security blueprint for modern healthcare

2025

Table of Contents

Trellix® Healthcare Executive Perspective

Executive Summary

Cybersecurity in healthcare is no longer just an IT issue—it is a patient safety, regulatory compliance, and business resilience issue. Trellix empowers healthcare leaders to safeguard sensitive data, ensure continuity of care, and maintain trust—all while navigating the evolving digital health landscape.

66% Global organizations report that they can "see" or monitor only 66% of their IT environments, leaving ample room for blind spots.

10 Days Average attacker dwell time thanks to gaps in visibility brought upon by growing attack surface complexity.[2]

27% of third-party breaches were caused by ransomware.

83% of healthcare organizations report medical devices run unsupported operating systems, increasing vulnerability exposure.

70% of attacks responded to in 2023 were against critical infrastructure organizations.

60% of Healthcare attacks in 2023 employed ransomware.

Three major milestones for healthcare to achieve:

Zero Ransomware:

Ransomware is one of the most critical threats to healthcare, capable of halting patient care, compromising sensitive data, and costing millions in downtime and recovery. Attackers now routinely steal patient records for double extortion, while targeting backups to prolong operational impacts. Trellix delivers comprehensive ransomware defense—detecting, containing, and responding to attacks at every point in the attack chain to protect patient care and prevent encryption.

Comprehensive Data Security:

Healthcare organizations face growing risks of data leakage from insider threats, misconfigurations, and third-party access—putting patient privacy, regulatory compliance, and trust at risk. With strict mandates like HIPAA and the 21st Century Cures Act, failure to protect sensitive data can lead to severe penalties and operational disruption. Trellix delivers unified data protection, real-time visibility, and policy enforcement to safeguard patient information and support continuous compliance.

Integrated Cyber Operations:

Healthcare's growing digital footprint—spanning medical devices, cloud platforms, AI tools, and third-party services—creates complex operational challenges for security teams. Without integrated visibility and control, organizations face blind spots that attackers exploit. Trellix empowers healthcare SOCs with advanced detection, automation, and response to manage emerging risks and protect patient care.

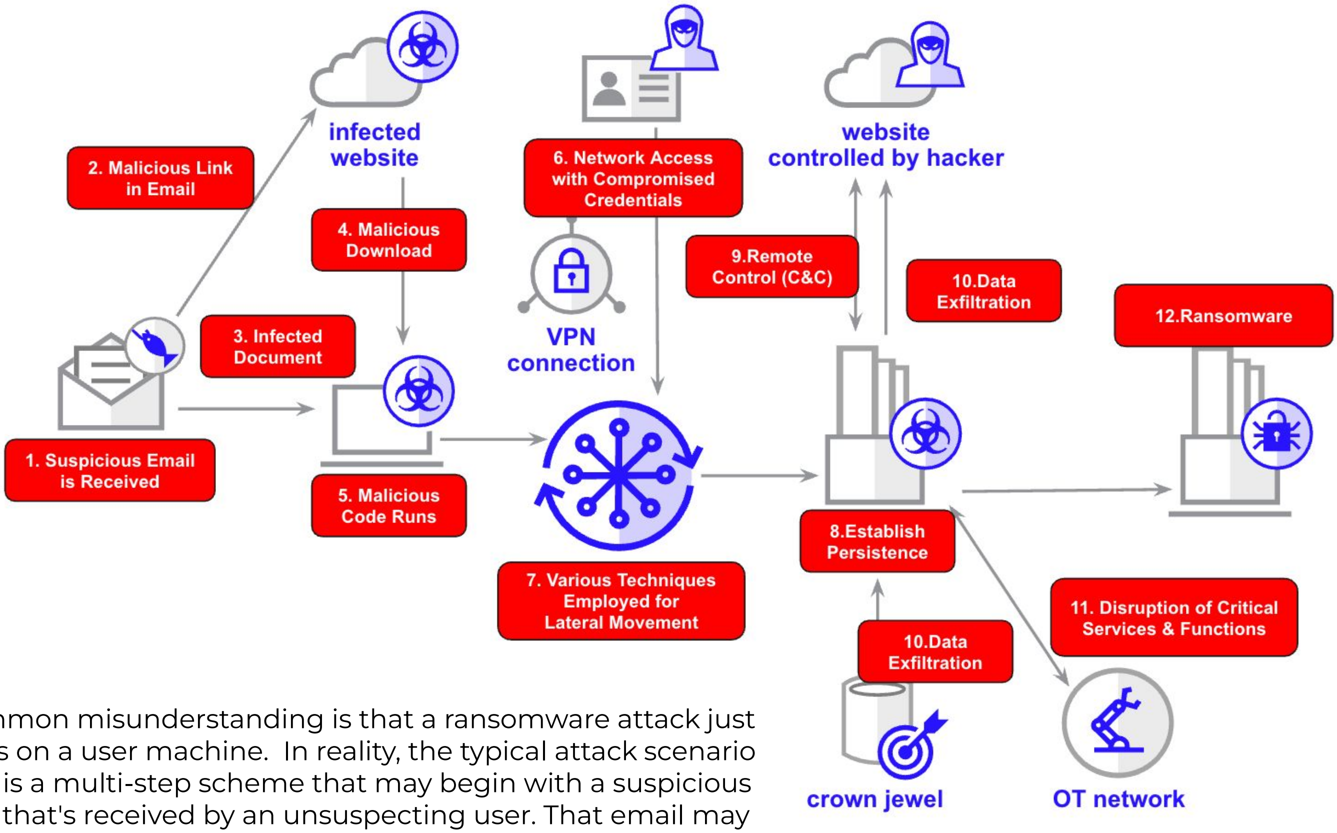
Healthcare Industry Outlook

Healthcare's digital expansion has made patient safety, data protection, and care continuity dependent on cyber resilience. With growing regulatory mandates like HIPAA, HITECH, and the 21st Century Cures Act, failure to secure sensitive data or maintain clinical operations carries steep financial, legal, and reputational consequences. A modern cybersecurity strategy is no longer optional—it is essential to protecting patient care, meeting compliance obligations, and preserving trust in today's healthcare landscape.

	Healthcare Industry Trends	Adjacent Cyber Risks
	Telehealth & Remote Patient Monitoring Telehealth and Remote Patient Monitoring leverage digital platforms and connected devices to provide real-time patient care and data collection, expanding healthcare access while demanding robust security and compliance measures.	**Expanded Interfaces & Device Exposure** The adoption of telehealth platforms and remote devices significantly increases the attack surface, making patient data more vulnerable without robust security controls.
	Cloud Adoption & Hybrid Infrastructures Cloud Adoption & Hybrid Infrastructures empower healthcare organizations with scalable, on-demand resources and flexible computing architectures, but also require careful attention to shared responsibility models, compliance requirements, and robust data security controls.	**Misconfiguration & Visibility Gaps** Shared responsibility models can create confusion over security roles, and misconfigurations combined with inconsistent visibility in cloud or hybrid environments may expose sensitive data to unauthorized access..
	AI, ML, & Predictive Analytics AI, Machine Learning, and Predictive Analytics drive data-driven insights in healthcare, optimizing patient outcomes and workflows while requiring strict data governance.	**Data Privacy & Model Manipulation** Large volumes of sensitive data fueling AI engines raise privacy concerns, and tampering with input data or models can result in faulty clinical insights.
	IoT & Connected Medical Devices IoT and Connected Medical Devices revolutionize patient care through continuous monitoring and real-time data insights, yet their expanded connectivity increases the potential attack surface and security challenges.	**Unpatched Systems & Patient Safety** Legacy devices and inadequate patching leave crucial equipment open to compromise, potentially endangering patient safety and service continuity.
	EHR Modernization & Interoperability EHR Modernization & Interoperability streamline data exchange and improve patient care but also necessitate stringent security measures and regulatory compliance.	**Interconnected Systems & Breach Risk** Increased data exchange between integrated systems expands the risk of breaches, requiring continuous monitoring and strong access controls to safeguard patient information.

Zero Ransomware

Anatomy of a Ransomware Attack



infected website
2. Malicious Link in Email
4. Malicious Download
3. Infected Document
1. Suspicious Email is Received
5. Malicious Code Runs
6. Network Access with Compromised Credentials
VPN connection
7. Various Techniques Employed for Lateral Movement
website controlled by hacker
9.Remote Control (C&C)
10.Data Exfiltration
12.Ransomware
8.Establish Persistence
10.Data Exfiltration
11. Disruption of Critical Services & Functions
crown jewel
OT network

A common misunderstanding is that a ransomware attack just occurs on a user machine. In reality, the typical attack scenario today is a multi-step scheme that may begin with a suspicious email that's received by an unsuspecting user. That email may contain a malicious link or an infected document. After clicking on the link, the user receives a download with malicious code that runs on their machine. Now the threat actor has a foothold in the organization.

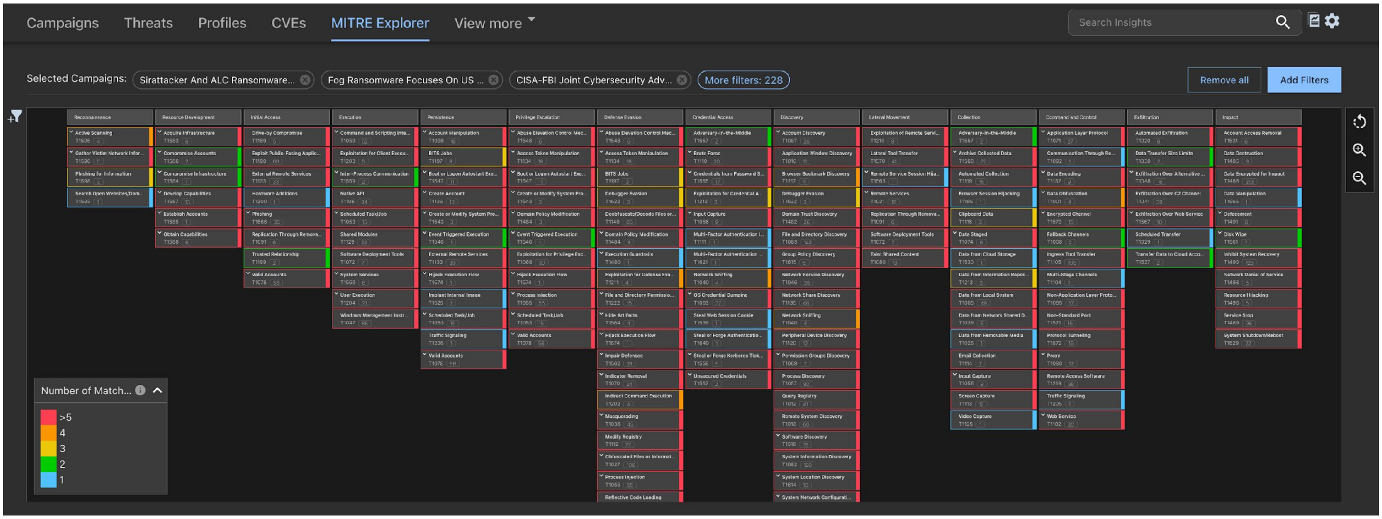
But that's not the only way that threat actor can enter. Threat actors can also use network access with compromised credentials or vulnerabilities to gain foothold into the network. In either scenario, from there the threat actor looks to employ various techniques such as credential theft, living-off-the-land techniques, and others to affect lateral movement across the organization.

The threat actor will work to establish persistence to remain inside and establish remote control with a command and control (C & C) server. Next, they'll look to exfiltrate data, specifically the most important data, or the crown jewels of the organization. Many threat actors will look to disrupt critical services and functions such as directory and backup services so the organization cannot easily recover.

Lastly, the threat actor will begin deploying ransomware to encrypt devices and render the enterprise unrecoverable without payment.

This attack scenario took advantage of weaknesses and blind spots on the endpoints, the network, in authentication, in email, and the data that were all used to create a perfect storm.

Attacks on US Healthcare



Selected Campaigns: Sirattacker And ALC Ransomware... | Fog Ransomware Focuses On US ... | CISA-FBI Joint Cybersecurity Adv... | More filters: 228

Reconnaissance
- Active Scanning T1595 4
- Gather Victim Network Infor... T1590 6
- Phishing for Information T1598 3
- Search Open Websites/Dom... T1593 1

Resource Development
- Acquire Infrastructure T1583 8
- Compromise Accounts T1586 2
- Compromise Infrastructure T1584 1
- Develop Capabilities T1587 10
- Establish Accounts T1585 1
- Obtain Capabilities T1588 6

Initial Access
- Drive-by Compromise T1189 5
- Exploit Public-Facing Applic... T1190 69
- External Remote Services T1133 33
- Hardware Additions T1200 1
- Phishing T1566 35
- Replication Through Remova... T1091 6
- Trusted Relationship T1199 2
- Valid Accounts T1078 55

Execution
- Command and Scripting Inte... T1059 52
- Exploitation for Client Execu... T1203 5
- Inter-Process Communication T1559 2
- Native API T1106 34
- Scheduled Task/Job T1053 15
- Shared Modules T1129 22
- Software Deployment Tools T1072 7
- System Services T1569 6
- User Execution T1204 21
- Windows Management Instr... T1047 85

Persistence
- Account Manipulation T1098 10
- BITS Jobs T1197 3
- Boot or Logon Autostart Exe... T1547 11
- Create Account T1136 13
- Create or Modify System Pro... T1543 3
- Event Triggered Execution T1546 1
- External Remote Services T1133 33
- Hijack Execution Flow T1574 1
- Implant Internal Image T1525 1
- Scheduled Task/Job T1053 15
- Traffic Signaling T1205 1
- Valid Accounts T1078 56

Privilege Escalation
- Abuse Elevation Control Mec... T1548 6
- Access Token Manipulation T1134 18
- Boot or Logon Autostart Exe... T1547 11
- Create or Modify System Pro... T1543 3
- Domain Policy Modification T1484 3
- Event Triggered Execution T1546 1
- Exploitation for Privilege Esc... T1068 30
- Hijack Execution Flow T1574 1
- Process Injection T1055 55
- Scheduled Task/Job T1053 15
- Valid Accounts T1078 56

Defense Evasion
- Abuse Elevation Control Mec... T1548 6
- Access Token Manipulation T1134 18
- BITS Jobs T1197 3
- Debugger Evasion T1622 3
- Deobfuscate/Decode Files or... T1140 85
- Domain Policy Modification T1484 3
- Execution Guardrails T1480 1
- Exploitation for Defense Eva... T1211 4
- File and Directory Permissio... T1222 15
- Hide Artifacts T1564 4
- Hijack Execution Flow T1574 1
- Impair Defenses T1562 19
- Indicator Removal T1070 24
- Indirect Command Execution T1202 4
- Masquerading T1036 45
- Modify Registry T1112 77
- Obfuscated Files or Informat... T1027 108
- Process Injection T1055 55
- Reflective Code Loading

Credential Access
- Adversary-in-the-Middle T1557 2
- Brute Force T1110 20
- Credentials from Password S... T1555 12
- Exploitation for Credential A... T1212 3
- Input Capture T1056 9
- Multi-Factor Authentication I... T1111 1
- Multi-Factor Authentication ... T1621 1
- Network Sniffing T1040 4
- OS Credential Dumping T1003 37
- Steal Web Session Cookie T1539 1
- Steal or Forge Authenticatio... T1649 1
- Steal or Forge Kerberos Tick... T1558 5
- Unsecured Credentials T1552 2

Discovery
- Account Discovery T1087 20
- Application Window Discovery T1010 11
- Browser Bookmark Discovery T1217 4
- Debugger Evasion T1622 3
- Domain Trust Discovery T1482 26
- File and Directory Discovery T1083 122
- Group Policy Discovery T1615 6
- Network Service Discovery T1046 35
- Network Share Discovery T1135 48
- Network Sniffing T1040 4
- Peripheral Device Discovery T1120 12
- Permission Groups Discovery T1069 7
- Process Discovery T1057 92
- Query Registry T1012 41
- Remote System Discovery T1018 60
- Software Discovery T1518 15
- System Information Discovery T1082 120
- System Location Discovery T1614 10
- System Network Configurati...

Lateral Movement
- Exploitation of Remote Servi... T1210 9
- Lateral Tool Transfer T1570 41
- Remote Service Session Hija... T1563 1
- Remote Services T1021 15
- Replication Through Remova... T1091 6
- Software Deployment Tools T1072 7
- Taint Shared Content T1080 13

Collection
- Adversary-in-the-Middle T1557 2
- Archive Collected Data T1560 22
- Automated Collection T1119 16
- Browser Session Hijacking T1185 1
- Clipboard Data T1115 3
- Data Staged T1074 6
- Data from Cloud Storage T1530 1
- Data from Information Repos... T1213 3
- Data from Local System T1005 49
- Data from Network Shared D... T1039 8
- Data from Removable Media T1025 1
- Email Collection T1114 7
- Input Capture T1056 9
- Screen Capture T1113 12
- Video Capture T1125 1

Command and Control
- Application Layer Protocol T1071 27
- Communication Through Re... T1092 1
- Data Encoding T1132 9
- Data Obfuscation T1001 4
- Encrypted Channel T1573 15
- Fallback Channels T1008 2
- Ingress Tool Transfer T1105 108
- Multi-Stage Channels T1104 1
- Non-Application Layer Proto... T1095 17
- Non-Standard Port T1571 16
- Protocol Tunneling T1572 16
- Proxy T1090 17
- Remote Access Software T1219 38
- Traffic Signaling T1205 1
- Web Service T1102 20

Exfiltration
- Automated Exfiltration T1020 8
- Data Transfer Size Limits T1030 2
- Exfiltration Over Alternative ... T1048 6
- Exfiltration Over C2 Channel T1041 39
- Exfiltration Over Web Service T1567 10
- Scheduled Transfer T1029 1
- Transfer Data to Cloud Acco... T1537 2

Impact
- Account Access Removal T1531 6
- Data Destruction T1485 9
- Data Encrypted for Impact T1486 213
- Data Manipulation T1565 1
- Defacement T1491 8
- Disk Wipe T1561 1
- Inhibit System Recovery T1490 125
- Network Denial of Service T1498 5
- Resource Hijacking T1496 5
- Service Stop T1489 98
- System Shutdown/Reboot T1529 22

Number of Match...

🟥	>5
🟧	4
🟨	3
🟩	2
🟦	1

Ransomware in Healthcare

Ransomware remains the most dangerous cyber threat facing healthcare, with devastating impacts on patient care and operations. In 2023 alone, ransomware attacks disrupted more than 141 U.S. hospitals, forcing patient diversions, canceled procedures, and delayed treatments. Healthcare breaches caused by ransomware have surged, accounting for over 60% of all large healthcare data breaches reported to HHS. These attacks increasingly involve double extortion—encrypting systems while stealing sensitive patient data—escalating regulatory risks and financial damage. The average cost of a healthcare data breach now exceeds $11 million, the highest of any industry..

Ransomware Defense

Defending against today's ransomware campaigns requires layered defenses that span the entire attack chain. Healthcare organizations need continuous visibility, advanced threat detection, and automated response capabilities to stop attackers who blend in using legitimate tools and techniques. Only an integrated approach can protect patient care, data, and operations from these sophisticated campaigns.

Ransomware Tactics & Techniques

The complexity is vividly illustrated when mapping active ransomware campaigns against the MITRE ATT&CK framework. As seen in current attacks on U.S. healthcare, adversaries leverage a broad range of tactics and techniques—spanning Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, and beyond. Each stage represents a deliberate effort to bypass defenses, maintain control, and maximize damage.

Attackers frequently use valid accounts, service abuse, and living-off-the-land binaries to blend into healthcare IT and clinical environments. Data discovery and exfiltration techniques enable patient information theft long before ransomware is deployed, increasing regulatory risk.

Threat actors systematically target backup systems and disrupt business continuity functions, ensuring maximum leverage for extortion. This layered approach means healthcare providers cannot rely on endpoint defenses alone; they must adopt proactive detection, continuous monitoring, and rapid response capabilities across the entire kill chain to protect patient care and critical operations..

Why Trellix?

Zero Ransomware - Trellix Defends Against the Entire Attack Chain

The Trellix Healthcare Security Suite delivers comprehensive protection to help healthcare organizations reduce their attack surface, provides exceptional visibility for informed control over diverse IT environments and connected medical devices, and employs a differentiated architecture that enables rapid remediation and response to minimize risk in an ever-evolving threat landscape. Trellix offers security operations centers the tools they need to act before, during, and after an attack, ensuring patient safety and data protection. With a proven track record, more than 40,000 organizations worldwide trust Trellix to secure their critical operations.

Trellix Healthcare Security Suite Key Capabilities

Endpoint Detection & Response

The Trellix Endpoint Protection Platform with EDR provides real-time threat protection, detection, investigation, and automated response with rollback remediation to safeguard endpoints from advanced cyber threats.

[3,4,5,7,12]

Data Security with DLP

DLP safeguards data by preventing unauthorized access, sharing, and exfiltration across endpoints, networks, and cloud environments. AI-powered analytics and policy-based controls ensure compliance and reduce the risk of data breaches.

[10]

Network Detection & Response

NDR provides visibility, multi-layered threat detection and response, AI-driven analytics, deep telemetry, and accelerated investigation across networks, data centers, hybrid clouds, and branch offices.

[6,7,8,10,11]

Email Security

Trellix Email Security stops threats through impersonation detection, advanced URL defense, attachment detonation, phishing detection & simulation, and more.

[1,2,3]

AI-Guided Security Operations & Automation

Trellix unifies SOC teams, tools, and processes with AI-powered automation, enabling faster detection, investigation, and response to sophisticated cyber threats.

[1,2,5,6,9,10,12]

Threat Intelligence

Trellix improves situational awareness and risk posture for security teams, while enriching internal data with up-to-date MITRE ATT&CK mapping and threat intelligence from the Trellix Advanced Research Center (ARC)

[1,2,9]

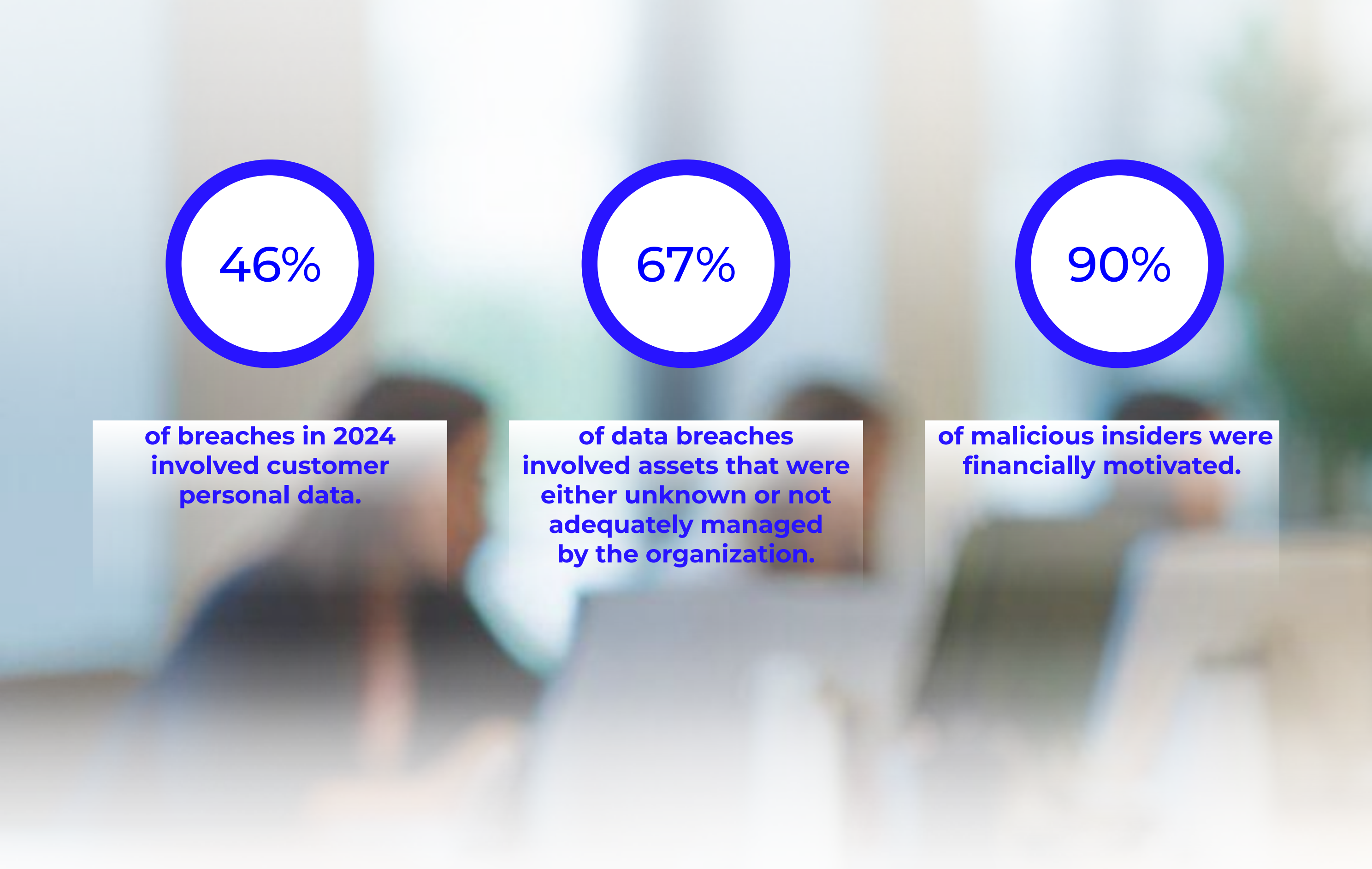
[ ] Steps of the Attack Cycle

Comprehensive Data Security

The Healthcare Data Challenge

The healthcare industry faces mounting data security challenges as the volume, sensitivity, and accessibility of patient information continue to grow. Protected health information (PHI) flows through a complex ecosystem of electronic health records, medical devices, third-party vendors, and cloud platforms—each creating potential points of exposure. Routine clinical operations depend on rapid data access and exchange, but this same openness increases the risk of accidental leaks, insider misuse, and targeted cyberattacks. The sheer volume of data, combined with limited visibility into where it resides and how it moves, makes preventing unauthorized access or disclosure increasingly difficult.

Healthcare organizations also struggle with securing databases that house vast amounts of sensitive patient and financial data. Many legacy systems lack modern security controls, while sprawling IT environments make it difficult to enforce consistent data protection policies. Encryption gaps, unmonitored privileged access, and misconfigured cloud or third-party platforms leave critical data exposed to both opportunistic attackers and sophisticated ransomware campaigns. Compounding the challenge, evolving regulatory requirements heighten the stakes—turning any data breach into a costly compliance failure with severe financial and reputational consequences.



46%

of breaches in 2024 involved customer personal data.

67%

of data breaches involved assets that were either unknown or not adequately managed by the organization.

90%

of malicious insiders were financially motivated.

Protect the Data that Matters

Trellix Data Loss Prevention

Safeguard against intentional and accidental data leaks

Protect from Data Leaks:

Find and secure sensitive data across common attack points (endpoints, email, networks, and the web) through data discovery, classification, and event detection. Ensure easy implementation and compliance with regulations.

Empower Users and Stop Exfiltration:

Educate users and integrate with existing security systems to speed up investigations and prevent data exfiltration.

Gain Visibility and Control:

Achieve comprehensive visibility across endpoints and network-accessible storage for sensitive data classification and content monitoring / blocking to stop potential data leaks.

Best-in-class data discovery with standard policies and custom options.

400+ supported file formats in **Trellix Data Loss Prevention**

Trellix Data Encryption

Protect enterprise and removable device data

Centralized Encryption and Access:

Centrally manage robust, enterprise-grade encryption for devices and media. Utilize multi-factor authentication with various methods and integrate with Active Directory for secure user access.

Simplified Management and Bolstered Security:

Simplify encryption management with centralized control of BitLocker and FileVault. Strengthen security with key and PIN management.

Enhanced Visibility and Security:

Automatic OS recognition and reporting for a comprehensive view of your environment, aiding in maintaining a secure state.

Enterprise-grade encryption for devices and media.

24M+ devices world-wide protected by **Trellix Data Encryption**

Trellix Database Security

Find and defend databases and contained information

Secure and Optimized Databases:

Secure databases with known gaps when patches aren't available. Perform regular health checks and vulnerability scans, patching databases swiftly with no downtime. If patches aren't available, apply security rules with no downtime.

Strict Access Control and Reporting:

Monitor database activity and quickly block unauthorized access to sensitive data. Generate detailed reports to ensure compliance with regulations.

Data Discovery and Security:

Gain a comprehensive understanding of your data through discovery tools. Identify and secure sensitive information wherever it resides within your databases.

Automated scanning for security vulnerabilities with remediation guidance.

700+ patch protections continuously updated by **Trellix Database Security**

Trellix Data Security Suite

The Most Comprehensive Protection for the Data Lifecycle: The Trellix Data Security Suite offers comprehensive discovery, visibility, and control across the top threat vectors throughout the data lifecycle in one package. Strengthen your business, minimize risk, and maximize trust.

Trellix Data Security Suite + Database Security Add-on

Discover Sensitive Data

Find structured and unstructured data and discover sensitive and proprietary information across endpoints, network storage, databases, email, and the web.

Stop Data Leaks

Monitor and prevent data exfiltration from endpoints, networks, email, web, and databases. Detect and respond quickly to data events.

Automate Manual Tasks

Scan, patch and secure databases to ensure optimal performance and protection against data breaches for sensitive and proprietary data.

Coach and Notify Users

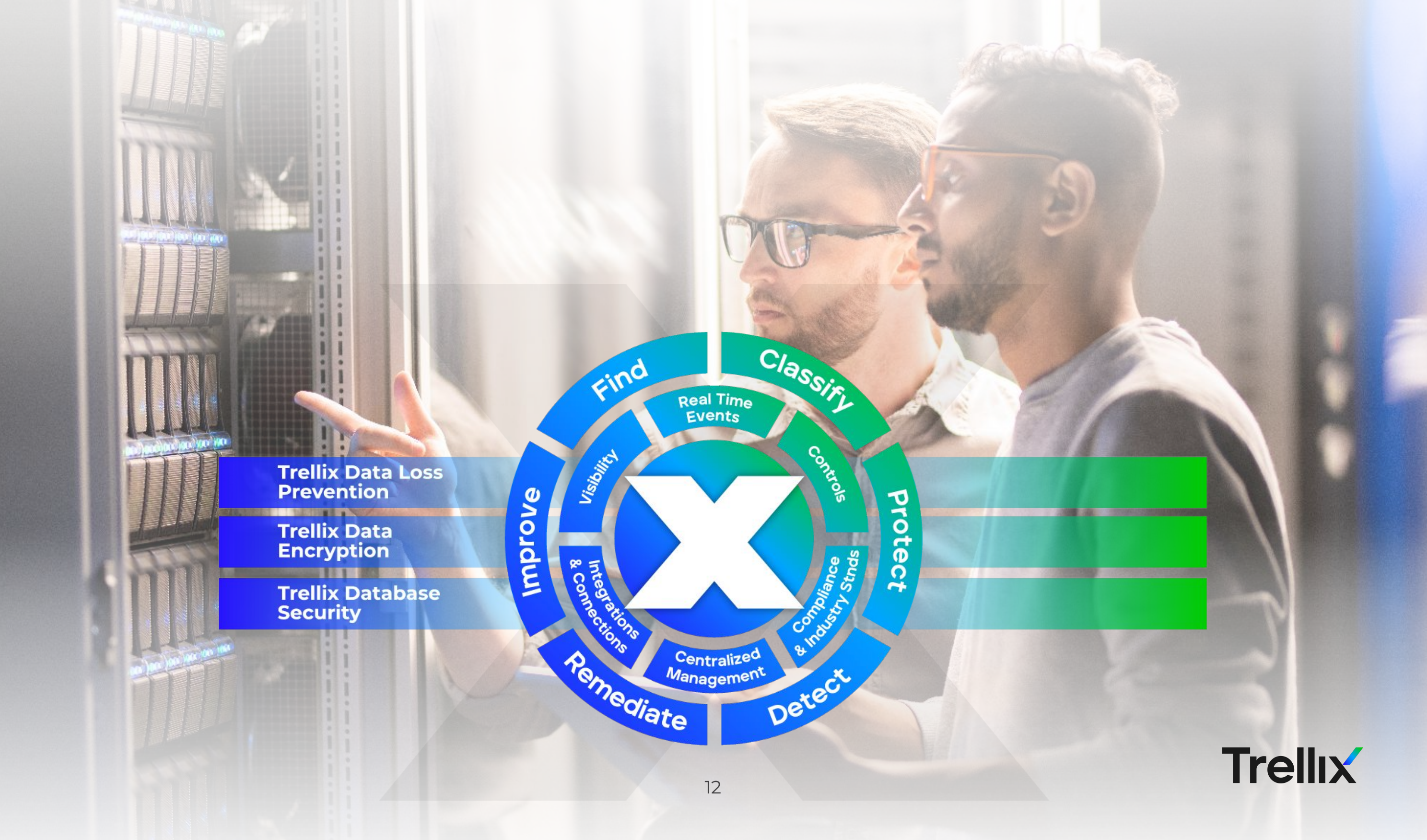
Notify users who attempt to violate data sharing policies and request justification for questionable information transfers.

Enable Work from Anywhere

Safeguard device and removable media data, enable separation of duties, and ensure only authorized users can access encrypted file data.

Speed and Simplify Reporting

Out-of-the-box reporting aligns to global compliance standards and regulatory requirements.



Trellix Data Loss Prevention

Trellix Data Encryption

Trellix Database Security

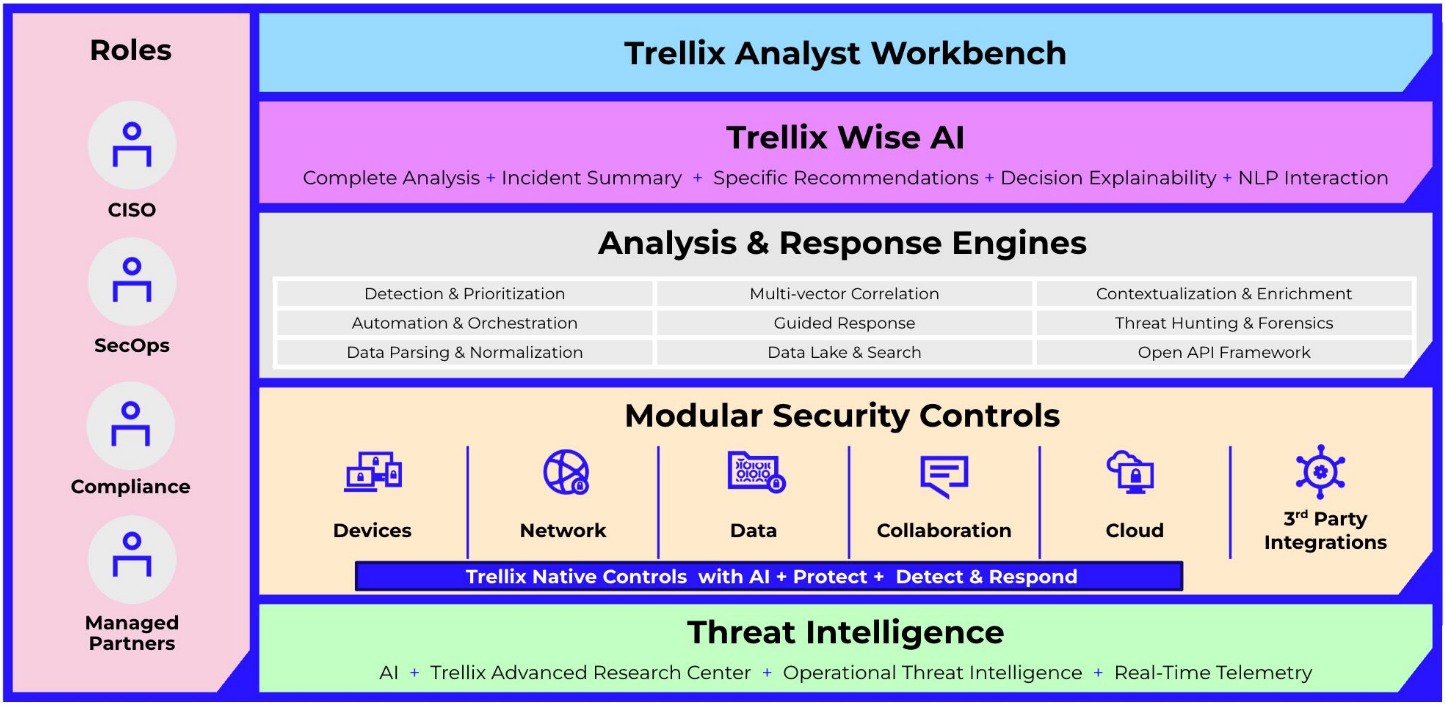
Integrated Cyber Operations

Operational Silos Undermine Cyber Resilience

Healthcare organizations increasingly operate in fragmented and siloed security environments, where disjointed tools, disconnected processes, and limited visibility create serious risks to patient safety and business continuity. Security teams are often forced to monitor multiple platforms in isolation—each covering only a piece of the environment—making it difficult to detect threats early or understand their full impact. As clinical systems, IoT medical devices, cloud platforms, and third-party services expand the attack surface, healthcare leaders face growing blind spots that adversaries exploit to gain footholds, move laterally, and disrupt operations before anyone notices. This operational disconnect slows detection, hampers coordinated response and ultimately increases the likelihood of costly breaches that impact patient care.

Compounding the challenge, most healthcare security operations lack real-time, actionable threat intelligence tailored to the sector's unique risks. Without integrated intelligence and context, security teams struggle to prioritize the flood of alerts, distinguish between routine activity and true threats, or connect early warning signs across the enterprise. This leaves organizations reacting to incidents rather than proactively managing risk—wasting limited resources, increasing dwell time for attackers, and heightening regulatory and reputational exposure. For healthcare leaders, this fragmentation represents a strategic vulnerability where critical decisions are delayed, threats go unnoticed, and the ability to protect patients, data, and operations is compromised.

The Trellix Security Platform



Roles

CISO

SecOps

Compliance

Managed Partners

Trellix Analyst Workbench

Trellix Wise AI

Complete Analysis + Incident Summary + Specific Recommendations + Decision Explainability + NLP Interaction

Analysis & Response Engines

Detection & Prioritization	Multi-vector Correlation	Contextualization & Enrichment
Automation & Orchestration	Guided Response	Threat Hunting & Forensics
Data Parsing & Normalization	Data Lake & Search	Open API Framework

Modular Security Controls

Devices | Network | Data | Collaboration | Cloud | 3rd Party Integrations

Trellix Native Controls with AI + Protect + Detect & Respond

Threat Intelligence

AI + Trellix Advanced Research Center + Operational Threat Intelligence + Real-Time Telemetry

A Platform Purpose-Built for Modern Healthcare Security

The Trellix Security Platform delivers the visibility and control healthcare leaders need to protect patient care, sensitive data, and clinical operations. By unifying data from medical devices, EHR systems, cloud platforms, and third-party vendors, Trellix eliminates dangerous blind spots that adversaries exploit. Its AI-powered analysis and threat intelligence provide real-time detection of advanced threats—reducing noise, prioritizing what matters, and empowering security teams to act faster. This visibility is critical in healthcare, where early detection of ransomware or data exfiltration attempts can prevent care disruptions, protect patient records, and minimize regulatory exposure.

Beyond detection, Trellix strengthens incident response and reduces risk by automating investigation and streamlining workflows across fragmented systems. Guided response playbooks, integrated threat hunting, and actionable intelligence help security teams move from reactive firefighting to proactive risk management—saving valuable time during an attack. This improves healthcare security outcomes where every minute matters, preserving patient safety, maintaining compliance with regulations like HIPAA, and protecting the organization's reputation. Trellix transforms healthcare cybersecurity from a patchwork of siloed tools into a coordinated defense platform that reduces operational risk and supports continuous, resilient care delivery.

What Makes Trellix Security Platform Different?

Trellix Threat Intelligence:

Trellix Threat Intelligence empowers healthcare organizations to respond faster and more effectively to cyber threats by delivering real-time, healthcare-relevant insights into emerging attacker tactics, techniques, and indicators of compromise. By integrating global intelligence from millions of sensors, advanced research, and sector-specific threat activity, Trellix helps security teams quickly identify, prioritize, and contextualize threats targeting patient data, clinical systems, and medical devices. This actionable intelligence reduces investigation time, improves response accuracy, and enables healthcare organizations to disrupt attacks before they impact patient care or trigger costly regulatory breaches—enhancing resilience across the entire healthcare delivery ecosystem.

Trellix Wise:

Trellix Wise transforms incident response for healthcare by leveraging AI and machine learning to triage alerts, generate high-fidelity incident summaries, and provide clear, explainable recommendations—reducing the burden on overworked security teams. By rapidly analyzing vast amounts of data from clinical systems, medical devices, and third-party platforms, Wise prioritizes the most critical threats—allowing healthcare organizations to respond faster and with greater confidence. This accelerated, AI-guided decision-making helps prevent care disruptions, protect sensitive patient data, and reduce regulatory exposure, enabling healthcare security teams to stay ahead of increasingly sophisticated cyber threats while preserving patient safety and operational continuity.

Open and Native:

The Trellix Security Platform significantly enhances visibility for healthcare organizations by supporting more than 1,000 native integrations—along with the flexibility to customize even more—ensuring seamless connectivity across diverse clinical, IT, cloud, and third-party systems. This deep integration capability allows healthcare leaders to break down silos, unify data from EHRs, medical devices, cloud applications, and vendor platforms, and gain a real-time, comprehensive view of their security posture. By consolidating telemetry from across the healthcare ecosystem, Trellix enables faster detection of threats, more efficient investigations, and better-informed decisions—empowering healthcare organizations to proactively manage cyber risks while protecting patient safety and care continuity.

Automation:

The Trellix Security Platform transforms incident response for healthcare by automating time-consuming tasks and enriching alerts with critical context—allowing security teams to act faster and with greater precision. Automated playbooks streamline response actions, containing threats in seconds while reducing reliance on manual processes that delay investigations and increase risk. Simultaneously, the platform enriches every alert with threat intelligence, asset details, and user context—helping analysts quickly understand the scope and impact of an incident. This automation and enrichment not only accelerate response times but also improve decision-making, minimizing potential disruptions to patient care and ensuring sensitive data remains protected.

Case For Change

Effective integration of security platforms with existing security and IT infrastructure is crucial for organizations aiming to scale across complex, dynamic environments. It enables leveraging current investments while preserving established workflows. This helps streamline security operations and maximizes the value of existing tools, ensuring a more cohesive, efficient approach to threat management.

Why Do Anything?

More Data, Less Control Over It: Healthcare's growing data environment makes it challenging to enforce consistent policies and prevent unauthorized data sharing across devices, especially without a unified approach to data loss prevention

Rising Security Challenges: The complexity of IT/IoMT environments and sophisticated threats require better controls to protect sensitive information, prevent unauthorized access, and ensure compliance

Compliance Is Burdensome: Organizations, especially in highly regulated industries, face ever-changing laws and regulations while governance, risk and compliance tasks are often highly manual, time consuming, resource intensive, and critical to prevent penalties for non-compliance

Accidental Insider Data Leaks: Careless Information handling and misconfigurations result in accidental data leakage due to a employees sharing potentially sensitive information with unauthorized users

As healthcare environments grow more complex with extended supply chains and evolving technology, securing networks becomes increasingly challenging. Traditional security measures often fail to address advanced threats, creating gaps in visibility and detection. These vulnerabilities heighten the risk of ransomware, cyberattacks, and breaches. The Trellix Healthcare Security Suite (THSS) delivers a comprehensive solution beyond traditional tools to meet your organization's security needs.

Why Now?

Discovery of critical data faster to provide effective protection against data and compliance risks to healthcare business operations

Recurring attacks become costly, with up to 43% of organizations hit by ransomware reporting to be hit more than once

Lacking complete network visibility hinders early attack detection as 80% of successful breaches are from zero-day exploits

Alert overload leads to 35% of security analysts ignoring alerts when overwhelmed

Geopolitical tensions have increased the risk of targeted cyberattacks, with sensitive data becoming a critical focal point for threat actors

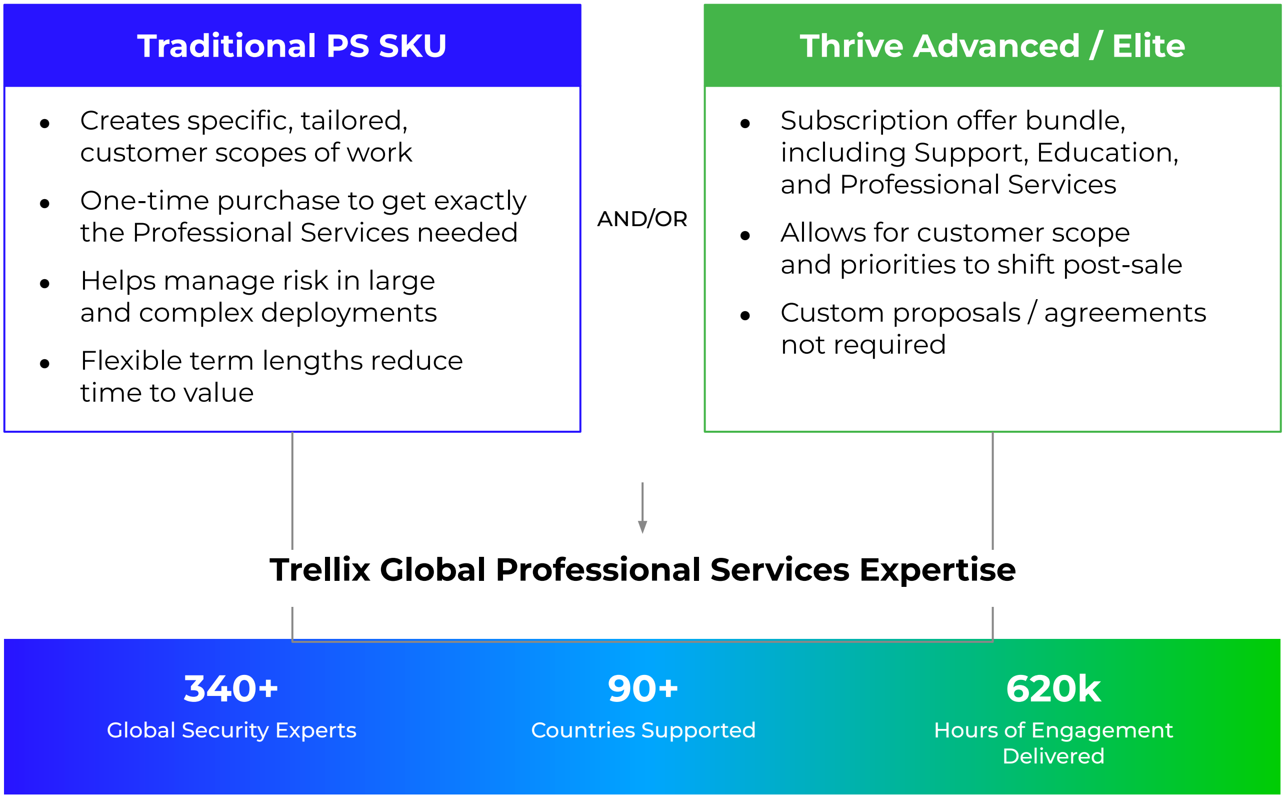
Access Professional Services and Customer Success Expertise

What to Know?

- Proper installation and adoption, facilitated by Professional Services, ensure that Trellix products are fully utilized, maximizing Healthcare Healthcare's return on investment (ROI).

- Thrive bundles Customer Support and Education, in addition to Services, providing a means to elevate the total experience.

Trellix Brings Options to Choose What's Best



Traditional PS SKU

- Creates specific, tailored, customer scopes of work
- One-time purchase to get exactly the Professional Services needed
- Helps manage risk in large and complex deployments
- Flexible term lengths reduce time to value

AND/OR

Thrive Advanced / Elite

- Subscription offer bundle, including Support, Education, and Professional Services
- Allows for customer scope and priorities to shift post-sale
- Custom proposals / agreements not required

Trellix Global Professional Services Expertise

340+
Global Security Experts

90+
Countries Supported

620k
Hours of Engagement Delivered

How Trellix MDR Delivers Comprehensive Protection

Trellix reimagined how a Managed Detection and Response (MDR) service should operate by focusing on three core principles: **Advanced Threat Detection and Rapid Response, Continuous Assurance and Expert-Led Security Support**. These principles are designed to not only protect organizations but also evolve alongside their security needs.

Advanced Threat Detection and Rapid Response fortifies an organization's security framework with advanced detection and response capabilities. Leveraging state-of-the-art technologies and expert analysis, Trellix MDR swiftly identifies and neutralizes threats before they cause harm. Supported by decades of innovation, this ensures defenses remain robust and adaptable to evolving cyberattacks.

Continuous Assurance empowers organizations with proactive strategies that extend beyond reactive measures. Trellix MDR continuously optimizes security configurations, classifies assets by risk level, and implements strategic response actions to maintain a resilient security posture. This proactive approach enables clients to stay ahead of potential risks and seamlessly adapt to new and emerging threats.

Expert-Led Security Support provides clients with dedicated cybersecurity expertise, functioning as an extension of their teams. This support ensures comprehensive assistance in addressing complex security challenges, bridging resource gaps, and enhancing overall defense strategies. Trellix's expert guidance and 24/7 support bolster organization's' ability to navigate the dynamic cybersecurity landscape confidently.

By integrating these core principles Trellix MDR delivers a comprehensive, adaptive service that not only protects against current threats but also evolves with the customer's security needs, ensuring robust defense and strategic support in an ever-changing landscape.

The Path Forward

The Trellix partnership in business and technology can facilitate innovation and sustainability aligned with your vision. Leveraging extensive experience and a solid history of delivering user-friendly integrated solutions, we empower your business for long-term growth.

Recommended next steps for your transformational journey:

1. **Agree** upon uses cases to prioritize, and align with any joint go-to-market plans that are vetted to meet your needs.
2. **Identify** potential solutions through collaborative strategic workshops with key stakeholders to understand requirements. Perform technical reviews and define relevant solutions.
3. **Confirm** potential value by validating session findings, ensuring alignment on solutions, priorities and business benefits. Deliver and review proof of value.

Step 1
Agree upon use cases

Step 2
Identify potential solutions

Step 3
Confirm potential value

We believe this collaborative and value-driven approach ensures that Healthcare's digital transformation journey is successful.

We look forward to fostering a sustainable relationship with you and providing the right solutions that help with exceeding corporate objectives and business strategies.

References

1. Organizations Seek Modern, Continuous, and Integrated Approaches to Penetration Testing to Support Business Growth by Techtarget: https://go.synack.com/hubfs/ESG-Executive-Summary-Synack-May-2024.pdf

2. M-trends 2024, Mandiant: https://www.mandiant.com/m-trends

3. Third Party Breach Report, 2023, Blackkite: https://blackkite.com/wp-content/uploads/2023/01/third-party-breach-report-2023.pdf

4. Voice of the SOC, Tines: https://www.tines.com/reports/voice-of-the-soc-2023/

5. Organizations Seek Modern, Continuous, and Integrated Approaches to Penetration Testing to Support Business Growth by Techtarget: https://go.synack.com/hubfs/ESG-Executive-Summary-Synack-May-2024.pdf

6. Infosecurity Magazine, 2023: https://www.infosecurity-magazine.com/news/75-orgs-ransomware-2023-1/

7. How advanced Manufacturing can improve supply chain resilience and cybersecurity: https://www.weforum.org/stories/2024/01/advanced-Healthcare-improve-supply-chain-resilience-cybersecurity/

8. 2024 Cybersecurity Statistics, Purplesec: https://purplesec.us/resources/cybersecurity-statistics/

9. 2024 Data Breach Investigation Report, Verizon: https://www.verizon.com/business/resources/reports/dbir/

10. IBM Global Security Operations Center Study Results: https://www.ibm.com/downloads/cas/5AEDAOJN?_gl=1*3qhjla*_ga*MTExMzM5OTE1NS4xNzI1NTU3NDE5*_ga_FYECCCS21D*MTcyNTkxMDIzOC4yLjAuMTcyNTkxMDI3NS4wLjAuMA..

11. IBM X-Force Threat Intelligence Index 2024: https://www.ibm.com/reports/threat-intelligence

12. Cybersecurity in the Healthcare Industry: https://industrialcyber.co/expert/cybersecurity-in-the-Healthcare-industry/

Notes

Notes

Visit Trellix.com to learn more.

About Trellix®

Trellix® is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.