What You Need to Know to Survive Ransomware

Ransomware has a longer history than many realize, with its roots going back to the 1980s. The first recorded ransomware attack occurred in 1989 with the AIDS Trojan, distributed via a floppy disk at the World Health Organization's AIDS Conference, also marking it as one of the earliest instances of major hacktivism.[1]

In the 2000s, ransomware's evolution accelerated. The arrival of the Archievus Trojan (also known as the Arhiveus Trojan) emerged in 2006 as the first ransomware to use advanced RSA encryption, leveraging websites and spam email for mass distribution.[2] This marked a significant technological leap, though a uniform decryption password limited its impact. By 2008, the arrival of bitcoin—which officially launched in January 2009—provided a whole new ability that made it harder to trace transactions, fueling ransomware's rapid growth.[3]

More recent attacks showcase high-profile ransomware groups that have dominated headlines with increasingly sophisticated tactics. LockBit, once known for its ransomware-as-a-service (RaaS) model, carried out numerous attacks that targeted critical infrastructure, healthcare, and financial sectors before facing major disruption from international law enforcement in February 2024.[4]

Despite its takedown through Operation Cronos, the group resurfaced within a week, demonstrating the resilience of modern ransomware operations.[5] RansomHub emerged as a dominant force in 2024. Palo Alto Networks threat intelligence and consulting arm, Unit 42®, confirmed it became the most active ransomware variant between January 2025 and March 2025 (figure 1).[6]

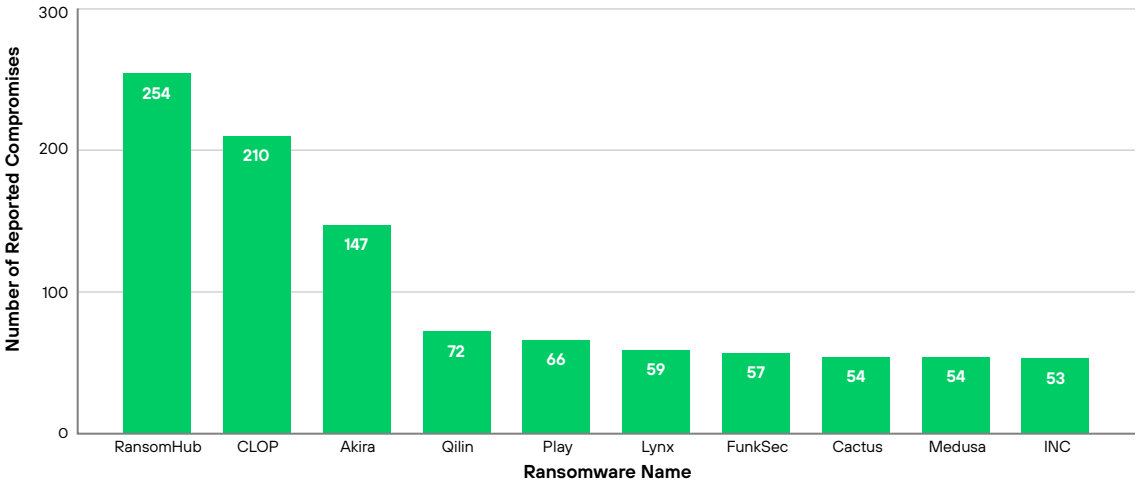

Figure 1. The most active ransomware leak sites—January 2025 through March 2025

In 2024, ransomware attacks escalated significantly. Unit 42 analysis of incident response cases revealed that business disruption had become a primary attack goal, with 86% of incidents in 2024 involving operational downtime, reputational damage, or both.[7] This same year also witnessed record-breaking ransom payments, with Unit 42 data showing the median initial extortion demand jumped almost 80% year over year to US$1.25 million in 2024, though successful negotiations reduced median payments to US$267,500.[8]

1. Samantha Murphy Kelly, "The bizarre story of the inventor of ransomware," CNN Business, May 16, 2021.
2. Joe Stewart, "Threat Analysis: Arhiveus Ransomware Trojan Analysis," Secureworks, May 5, 2006.
3. Terrence August, Duy Dao, Kihoon Kim, et al., "The Impact of Cryptocurrency on Cybersecurity," Institute for Operations Research and the Management Sciences, March 27, 2025.
4. Jenna McLaughlin, "Global law enforcement effort cracks down on LockBit ransomware group," NPR, February 20, 2024.
5. Ravie Lakshmanan, "LockBit Ransomware Group Resurfaces After Law Enforcement Takedown," The Hacker News, February 26, 2024.
6. "Extortion and Ransomware Trends January-March 2025," Palo Alto Networks Unit 42, April 23, 2025.
7. Ibid.
8. Ibid.

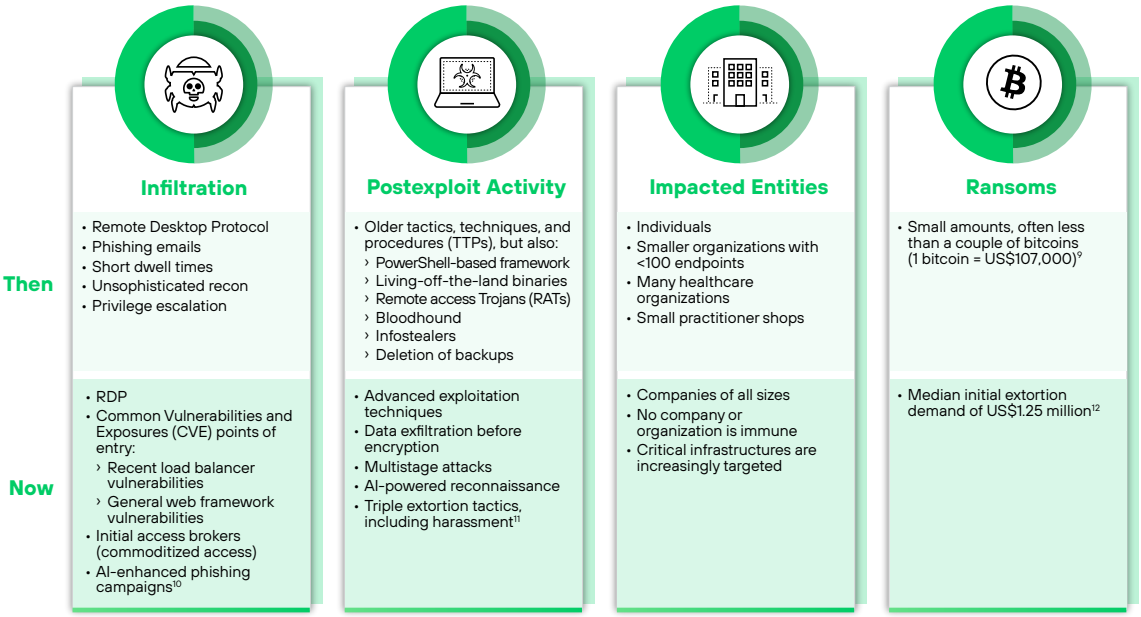

Figure 2. Ransomware: Then (2017–2019) and now (2020 and beyond)

Ransomware Basics

Ransomware is a criminal business model that uses malicious software to hold data hostage, often locking or encrypting a system while demanding a ransom payment in exchange for restoring access. Although it's an increasingly urgent challenge, you can prevent ransomware. Or at least, you can minimize damage through proper training, specific tuning in your current IT environment, and deploying advanced endpoint technology. This technology deployment includes adding solutions such as extended detection and response (XDR) to your security stack.

Ransomware comes in two types:

- **Crypto ransomware** is the most common type and encrypts files and data.
- **Locker ransomware** locks a computer or other device, preventing victims from using it.

Crypto ransomware encrypts the data. Even if the malware is removed from the device or the storage media is moved to another device, the data remains inaccessible. Typically, crypto ransomware doesn't target critical system files, enabling the device to continue to function despite being infected. Besides, the device could be needed to pay the ransom.

Locker ransomware only locks the device, while the data stored on the device typically remains untouched. As a result, if the malware is removed, the data is unaffected. Even if the malware can't be easily removed, you can often recover the data by moving the storage device—typically a hard drive—to another functioning computer.

9. "Bitcoin (BTC) Price Prediction 2025," CoinCodex, July 2025.
10. CISO Advisory, "Artificial Intelligence Fuels New Wave of Complex Cyber Attacks Challenging Defenders," Cyber Security News, May 13, 2025.
11. Konrad Martin, "AI Cyber Attack Statistics 2025," Tech Advisors, May 27, 2025.
12. *2025 Unit 42 Global Incident Response Report*, Palo Alto Networks Unit 42, February 2025.

Typical Steps in Most Ransomware Attacks

Most ransomware attacks consist of the following steps unless the attack is mitigated or the victim refuses to pay the ransom.

1. Compromise and Take Control of a System

Most attacks begin with phishing, tricking a user by sending them a fraudulent email urgently requiring them to unknowingly open an infected attachment. Opening the attachment compromises the system. Or the attacker might include other forms of valid credential abuse for initial access. This can impact a single host, such as a computer or mobile device. Then the compromised host establishes communications to a command-and-control (C2) server. At that point, the attacker might move laterally from the initial host to other systems in the organization to maximize the impact of the ransomware attack.

2. Discover or Exfiltrate Valuable Data

While ransomware in the past would often simply identify and encrypt certain file types likely to be of value to the victim (e.g., business documents like .doc, .xls, and .pdf), attackers have evolved. Now, threat actors silently seek out known sensitive data, including customer data or intellectual property, to ensure they can command higher ransoms. Attackers also often exfiltrate data for use in multiextortion schemes.

3. Prevent Access to the System

Once an attacker infects a system, they either encrypt data or deny access to a system or multiple systems through lockout screens or scare tactics.

4. Alert the Device Owner About the Compromise and Ransom Amount

All previous steps represent the actual bulk of actions in a ransomware attack. If a skilled adversary performs them, they occur without the victim knowing. That is, when the attacker notifies victims of their presence, the attack is complete. This notification often comes in the form of a ransom note with payment instructions and additional steps to unlock their devices.

5. Accept Ransom Payment

An attacker must have a way to receive ransom payments while evading law enforcement. They use pseudoanonymous cryptocurrencies, such as bitcoin, for these transactions.

6. Promise to Return Full Access Upon Payment Receipt

Failure to restore compromised systems destroys the scheme's effectiveness, because no one pays a ransom without confidence that their valuables will be returned.

Acceleration Crisis

Modern ransomware attacks have undergone dramatic speed acceleration. Unit 42 research shows that attack timelines have accelerated dramatically, with the mean time to exfiltrate (MTTE) dropping from nine days in 2021 to just two days in 2023, with some incidents occurring in hours.[13] By 2025, experts predict MTTE could drop as low as 25 minutes for some incidents—representing over 100x faster attacks in just three years.[14] This acceleration fundamentally changes the threat landscape. Traditional detection and response methods that rely on human analysis and manual processes become obsolete when attackers can complete their objectives in under 30 minutes.

13. "Unit 42 Predicts the Year of Disruption and Other Top Threats in 2025," Palo Alto Networks Unit 42, November 21, 2024.
14. Ibid.

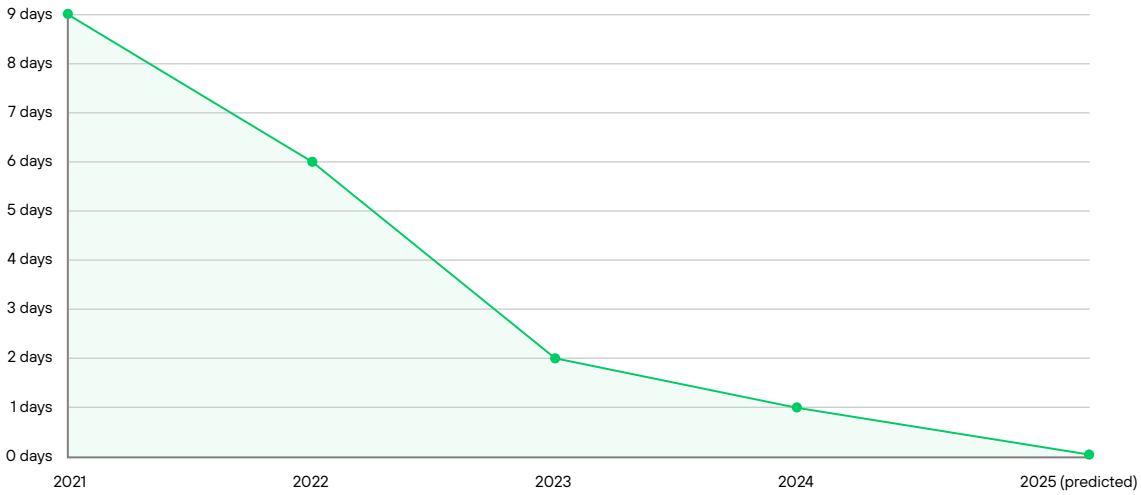

Figure 3. Ransomware speed crisis: Dramatic acceleration in MTTE

Common Attack Methods

To better prevent ransomware, it's critical to understand the tactics attackers use to deliver this threat. Multiple ransomware families operate across multiple attack vectors. For example, these vectors might come through your network, SaaS applications, or directly to the endpoint. This information enables you to focus your security controls on the areas attackers are most likely to leverage and reduce your risk of infection.

Increasingly, artificial intelligence (AI) enhances attack sophistication. AI-generated text can mimic legitimate communication styles, making malicious emails harder to distinguish from genuine ones. By 2024, 82.6% of phishing emails used AI technology in some form, with 78% of people opening AI-generated phishing emails.[15] This evolution in attack sophistication necessitates more advanced detection methods and user education.

Malicious Email Attachments

Historically, with malicious email attachments, an attacker crafts an email to come from a believable source, such as someone in human resources or IT. Then, they attach a malicious file such as a Portable Executable (PE) file, a Word document, or a JS file. The recipient opens the attachment thinking the email was sent from a trusted source. Then, the ransomware payload is unknowingly downloaded, the system is infected, and the files are held for ransom. Today, malware infections often give access to attackers who later deploy ransomware.

Malicious Email Links

Similar to malicious email attachments, malicious email links are URLs in the body of the email. These emails are sent from someone or some organization that you believe to be a trusted source. When clicked, these URLs download malicious files over the web, the system is infected, and the files are held for ransom.

15. Martin, "AI Cyber Attack Statistics 2025."

Vulnerable Credentials

Ransomware operators might also buy credentials from initial access brokers (IABs) or take advantage of poor password hygiene to avoid the whole process of actually compromising the victim. IABs are individuals who gather and collect credentials, selling them to the highest bidder. While IABs aren't exclusively for ransomware, ransomware operators definitely leverage the system, typically at the beginning of the intrusion lifecycle. IABs conduct reconnaissance, identifying networks with vulnerable applications or devices such as virtual private networks (VPNs), open RDP, or servers with exposed software vulnerabilities. You can avoid this vector by following solid best practices, such as multifactor authentication (MFA) and additional identification mechanisms.

CVE Exploitation

Ransomware operators frequently exploit known CVEs to gain initial access to target systems. These attacks take advantage of unpatched software vulnerabilities in operating systems, applications, and network infrastructure. Attackers systematically scan for systems running vulnerable versions of software and then deploy their exploit code to leverage specific CVEs. Popular targets include web servers, VPN appliances, email servers, and remote access tools that contain publicly disclosed security flaws.

After a successful exploitation, attackers establish persistence and can deploy ransomware payloads or sell access to other threat actors. This attack vector is particularly effective because many organizations struggle to maintain comprehensive patch management programs, leaving critical vulnerabilities exposed for extended periods. The window between CVE disclosure and widespread exploitation continues to shrink, with some vulnerabilities being actively exploited within days of public disclosure.

Are You at Risk?

While you might think only large corporations are ransomware targets, small businesses aren't immune to compromises either. The FBI found that healthcare experienced the highest combined total of ransomware and data theft attacks of any US critical infrastructure sector, with 444 reported incidents.[16] Additionally, 92% of US healthcare organizations surveyed experienced at least one cyberattack in the past 12 months.[17]

Targeted Data Goldmines

Ransomware attacks publicly impact the organization they target, because the organization's operations can become severely degraded or shut down entirely, as illustrated by recent attacks on hospitals across the United States. Personally identifiable information (PII) is a veritable goldmine of data for cyberthieves who sell or auction it off on the dark web. PII exposure leads to more identity fraud and targeted scams that impact consumers.

Criminals have realized this is a lucrative business with low barriers to entry. The RaaS model enables affiliates to use already-developed ransomware tools to execute their own ransomware attacks. Consequently, ransomware is displacing other cybercrime business models. Moreover, attackers are becoming increasingly sophisticated in their ability to determine the value of compromised information, assess the victim organization's willingness to pay, and demand higher ransoms.

16. "Report: Health care had most reported cyberthreats in 2024," American Hospital Association, May 12, 2025.
17. Steve Adler, "92% Of U.S. Healthcare Organizations Experienced a Cyberattack in the Past Year," The HIPAA Journal, October 9, 2024.

More Platforms Are Vulnerable

While attackers focused almost exclusively on Microsoft Windows systems in the past, the emergence of ransomware for Android, macOS, and Linux demonstrates that no operating system is immune from these attacks. Nearly all computers or devices with an internet connection are potential victims of ransomware. This is a valid concern with the proliferation of internet of things (IoT) devices and, most recently, an expanded attack surface due to continued remote work trends.

Supply Chains and Critical Vulnerabilities in the Crosshairs

In 2024, the ransomware landscape experienced significant transformations, with supply chain attacks and critical vulnerability exploitations playing a central role in the surge of ransomware activity.

Key Findings from Attacks in 2024

- **Critical vulnerabilities are exploited:** Zero-day exploits targeting vulnerabilities, like CVE-2024-3400 (the Palo Alto Networks firewall) and other critical infrastructure components, drove spikes in ransomware infections before defenders could update vulnerable software.[18]
- **Supply chain impact:** Supply chain compromise surged to become the second most prevalent attack vector (15%), and second costliest (US$4.91 million) after malicious insider threats (US$4.91 million).[19] Unit 42 research confirms that software supply chain and cloud attacks are growing in both frequency and sophistication, with threat actors embedding within misconfigured environments to scan vast networks for valuable data. In one campaign documented by Unit 42, attackers scanned more than 230 million unique targets for sensitive information.[20]
- **Emerging threats:** New ransomware groups continue to emerge, representing the continued attraction of ransomware as a profitable criminal activity.
- **Industry focus:** Healthcare became one of the most targeted industries in 2024. Unit 42 Incident Response data shows the top six targeted industries were professional and legal services, high technology, manufacturing, healthcare, finance, and wholesale and retail. Together, they accounted for 63% of cases.[21]

Evolution of Tactics

Ransomware groups have adapted their tactics to maximize impact and profits:

- **Multistage attacks:** Some groups use ransomware as a distraction or funding source for more complex supply chain compromises.
- **Data exfiltration:** Groups like RansomHub and other major operators updated their tactics to include sophisticated data theft before encryption, increasing efficiency in their extortion efforts.
- **Targeting critical infrastructure:** Ransomware operators increased their focus on sectors with low tolerance for downtime, such as healthcare, manufacturing, and energy.
- **AI-enhanced operations:** Unit 42 research conducted in 2024 explored how threat actors could create malware using GenAI tools, finding that, while initial efforts produced basic code, more methodical approaches using frameworks, like MITRE ATT&CK®, yielded functional results.[22] Looking ahead to 2025, Unit 42 predicts GenAI capabilities will automate portions of ransomware development and distribution, facilitating the creation of customizable ransomware kits and builders with automated encryption, victim targeting, and reconnaissance.[23]

18. Deeba Ahmed, "RansomHub: The New King of Ransomware? Targeted 600 Firms in 2024," HackRead, February 14, 2025.
19. *Cost of a Data Breach 2025: The AI Oversight Gap*, IBM and Ponemon Institute, July 31, 2025.
20. *Global Incident Response Report.*
21. *Unit 42 Attack Surface Threat Report*, Palo Alto Networks, May 6, 2025.
22. *The Unit 42 Threat Frontier: Prepare for Emerging AI Risks*, Palo Alto Networks, October 16, 2024
23. "Year of Disruption."

Law Enforcement and Cybersecurity Response

2024 saw intensified efforts from international law enforcement agencies. Operation Cronos led to the disruption of LockBit, once the world's most prolific ransomware group.[24] However, the group's rapid resurgence within a week of the takedown demonstrated the resilience of modern ransomware operations.[25] These actions reflect both the successes and challenges of global cooperation in cybersecurity.

Future Trends and Predictions

Looking ahead, Unit 42 predicts several key developments that will reshape the threat landscape in 2025:[26]

- **GenAI will accelerate cyberattacks by up to 100 times:** Attack speeds could drop from days to as little as 25 minutes as threat actors use AI to automate reconnaissance, hyperpersonalized phishing, and rapid lateral movement across networks.
- **RaaS will become AI-enhanced:** GenAI capabilities will automate ransomware development and distribution, with threat actor-trained LLMs creating customizable ransomware kits and chatbots to negotiate ransom demands.
- **Critical infrastructure will face increased nation-state targeting:** Rising geopolitical tensions will drive offensive cyber campaigns against essential services like energy, water, transportation, and healthcare as adversaries seek strategic footholds.
- **Supply chain vulnerabilities will intensify:** Organizations will struggle with complex software dependencies while advanced persistent threat groups increasingly target third-party vendors and major cloud service providers to maximize impact through single breaches.

As ransomware attacks continue to evolve, organizations must adapt their defenses to address both the technical aspects of these threats and the potential for reputational damage. They must also protect their employees, customers, and partners who can become targets in these increasingly complex attacks.

Evolution of Multiextortion

Ransomware operators increasingly employ multiple extortion techniques to pressure victims into paying. This trend of multiextortion has evolved significantly since 2021, with threat actors layering various tactics to maximize their chances of a payout. Unit 42 defines this evolution in terms of three waves—traditional encryption for ransom, double extortion combining data theft with encryption, and the latest wave of intentional business disruption designed to maximize operational impact.[27]

Four Commonly Used Ransomware Techniques

The rise of quadruple extortion represents one disturbing trend. Ransomware operators now commonly use as many as four techniques for pressuring victims:

- **Encryption:** Victims pay to regain access to scrambled data and compromised computer systems.
- **Data theft:** Hackers threaten to release sensitive information if a victim doesn't pay the ransom.

24. Kate Whiting, "LockBit: How an international operation seized control of 'the world's most harmful cybercrime group,'" World Economic Forum, February 21, 2024.
25. Lakshmanan, "LockBit Ransomware Group Resurfaces After Law Enforcement Takedown."
26. "Year of Disruption."
27. Ibid.

- **Denial of service:** Ransomware gangs launch DoS attacks that shut down a victim's public websites.
- **Harassment:** Cybercriminals contact customers, business partners, employees, and media to inform them of the hack and increase pressure on the victim organization.

The 2024 incident response data from Unit 42 revealed that encryption remains the most common tactic used in 92% of extortion attacks, followed by data theft in 60% of cases.[28]

Extortion Tactic	2021	2022	2023	2024
Encryption	96%	90%	89%	92%
Data Theft	53%	59%	53%	60%
Harassment	5%	9%	8%	13%

Source: *Unit 42 Incident Response Report 2024*, Palo Alto Networks

Figure 4. Extortion tactics prevalence in extortion-related cases

However, the significant finding is that 86% of incidents now involve business disruption spanning operational downtime, reputational damage, or both.[29] While it's rare for one organization to fall victim to all four techniques, the trend shows that attackers increasingly use multiple methods to achieve their goals.

Among the cases reviewed in 2024, Unit 42 found the median initial extortion demand reached US$1.25 million, representing about 2% of the victim organization's perceived annual revenue.[30] Through negotiation, organizations achieved a median reduction of more than 50% from the initial demands.[31] The ransomware crisis continues to gain momentum as cybercrime groups further hone tactics for coercing victims into paying and develop new approaches for making attacks more disruptive.

Extortion Without Encryption Is on the Rise

As a departure from past tactics, about 10% of incident response matters involving extortion don't involve encryption.[32] These cases often rely on data theft alone, with some threat actors even deleting an organization's data altogether instead of encrypting it. Despite improved backup practices, Unit 42 data shows nearly half (49.5%) of impacted victims were able to restore from backup in 2024, about five times as many as in 2022 when only 11% could restore from backup.[33] Therefore, organizations should be prepared for ransomware actors to apply other forms of pressure to force ransom payment even when data access isn't lost.

As ransomware groups continue to evolve their tactics, organizations must adapt their defenses to address these various methods of applying pressure. Modern incident response plans need to consider both the technical aspects and the safeguards for an organization's reputation. They must also consider the measures to protect employees, customers, and partners who might become targets of increasingly aggressive extortion tactics.

Prepare and Prevent

Ransomware acts quickly—sometimes within minutes of infection—so deploying controls that either mitigate or prevent ransomware attacks is critical. With the evolution of AI-powered attacks, multiextortion schemes, and supply chain compromises, organizations need comprehensive defense strategies that address modern threat vectors.

28. *Unit 42 Incident Response Report 2024*, Palo Alto Network, February 2024.

29–33. Ibid.

Recommendations to Mitigate the Impact of a Ransomware Attack

Develop and Execute an AI-Aware, End-User Awareness Program

With 82.6% of phishing emails now using AI technology,[34] traditional awareness training is insufficient. Implement quarterly training that specifically addresses AI-generated content detection, including deepfake audio and video recognition. Train users to verify requests through alternative communication channels, especially for financial transactions or credential requests. Establish clear escalation procedures when users suspect AI-generated social engineering attempts.

Implement a Zero Trust Backup and Recovery Architecture

Implement the 3-2-1-1 backup strategy: three copies of data stored on two different media types, with one copy maintained offsite and one copy kept offline or immutable. Test your backup restoration procedures monthly and maintain documented recovery time objectives (RTOs) and recovery point objectives (RPOs) for critical systems.

Unit 42 data demonstrates the effectiveness of improved backup practices, with nearly half (49.5%) of victims able to restore from backup in 2024—a fivefold increase from 2022.[35] Ensure backup systems require separate authentication credentials and can't be accessed from production networks.

Establish Comprehensive Privilege Management

Implement just-in-time (JIT) access for administrative functions, ensuring privileged accounts are activated only when needed. Deploy privileged access management (PAM) solutions that monitor and record all administrative activities. Segment network access based on user roles and implement microsegmentation to limit lateral movement.

Regularly audit and revoke unnecessary permissions, as well as establish automated alerts for privilege escalation attempts. Implement automated credential recycling policies that regularly rotate passwords and API keys for privileged accounts, reducing the attack surface and mitigating risks from credential stuffing attacks or long-term credential compromise.

Create Multiextortion Incident Response Procedures

Modern ransomware employs multiple pressure tactics including data theft, harassment, and DoS attacks. Document specific procedures for handling each extortion type, including legal notification requirements, communication strategies with affected parties, and coordination with law enforcement.

Consider establishing procedures to engage specialized cybersecurity law firms and notify cyber insurance carriers, maintaining prenegotiated retainer agreements to ensure rapid response and proper coverage coordination. Establish preapproved communication templates for stakeholders, customers, and the media. Designate specific team members to handle harassment campaigns targeting executives and employees. Consider maintaining retainers with digital forensics firms and crisis communications specialists to expedite response efforts.

Develop Supply Chain Security Protocols

With third-party compromises representing a significant portion of data breaches, implement vendor risk assessment programs that evaluate cybersecurity postures before onboarding. Require security certifications and regular penetration testing reports from critical suppliers. Establish contractual security requirements including incident notification timelines and liability terms. Monitor third-party access to your systems and implement network segmentation for vendor connections, including conducting continuous risk assessment and mitigation protocols if the third party falls outside the risk tolerance parameters.

34. "82% of all phishing emails utilized AI," Security Magazine, March 24, 2025.
35. *Global Incident Response Report.*

Ensure Regulatory Compliance Readiness

Prepare for regulations including the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA, for 72-hour incident reporting), Digital Operational Resilience Act (DORA, for financial services resilience), and emerging state privacy laws. Document all cybersecurity incidents with timestamps and impact assessments to meet reporting requirements. Establish relationships with legal counsel specializing in cybersecurity law and maintain incident response retainers with forensic firms.

Top Recommendations to Prevent Ransomware Infections

Implement AI-Powered Threat Detection and Response

Deploy security solutions that use AI to detect anomalous behavior patterns indicative of ransomware activity. Implement user and entity behavior analytics (UEBA) to identify unusual access patterns or data movement. Use AI-enhanced email security that can detect sophisticated phishing attempts, including those generated by malicious AI tools. Deploy deception technologies that create honeypots to detect lateral movement early in the attack chain.

Integrate solutions with global threat intelligence feeds to provide early warning systems and accelerate threat detection through shared indicators of compromise and attack patterns observed across worldwide networks. Augment your SOC with 24/7 Managed Detection and Response (MDR) experts who can help your team detect, hunt, and respond faster to ransomware attacks to prevent operational downtime or reputational damage.

Consider XDR platforms, like Cortex XDR®, that integrate and use AI to analyze data from a wider range of security layers, such as endpoints, networks, cloud, email, and identity. These platforms offer a more holistic view of threats and an enhanced capability to detect multistage attacks.

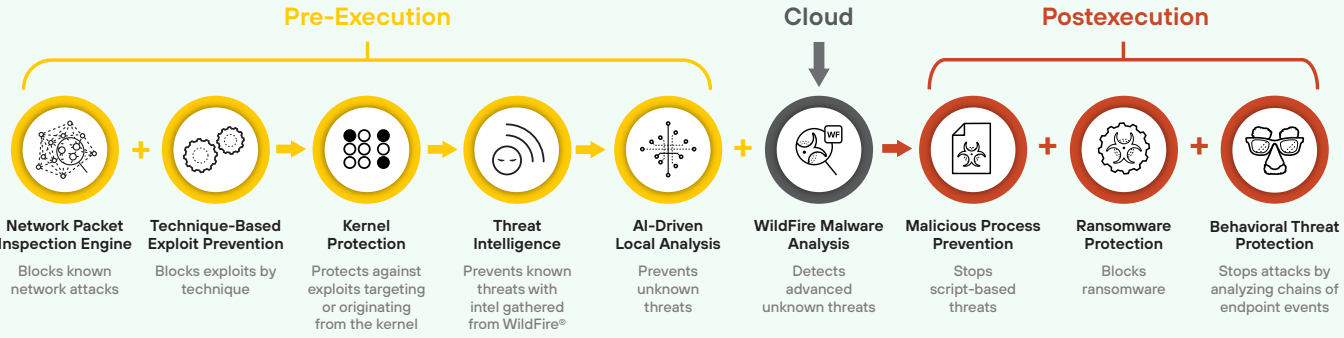

Figure 5. The Cortex XDR Agent layers multiple methods of threat prevention for effective ransomware defense

Deploy a Zero Trust Network Architecture

Transition from perimeter-based security to zero trust models that verify every user and device before granting access. Implement network microsegmentation to limit ransomware spread between systems. Deploy software-defined perimeters (SDP) for remote access instead of traditional VPNs. Continuously monitor and validate all network connections, treating internal traffic as potentially hostile.

Develop Secure Remote Work Policies

Establish secure remote access through zero trust network access (ZTNA) solutions rather than traditional VPNs. Implement mobile device management (MDM) for all corporate devices and bring your own devices (BYODs). Deploy cloud-based security services that protect remote workers regardless of location. Establish policies for secure home office setups and personal device usage.

Top Recommendations to Prevent Ransomware Infections (continued)

Establish Threat Hunting Capabilities

Deploy dedicated threat hunting teams that proactively search for advanced persistent threats and ransomware indicators. Implement behavioral analytics that can detect subtle signs of compromise before encryption begins. Use threat intelligence platforms that correlate internal events with global threat data. Conduct regular penetration testing and red team exercises to validate security controls.

Implement DNS Security Measures

Deploy DNS filtering services that block access to known malicious domains and newly registered domains used in attacks. Implement DNS monitoring to detect data exfiltration attempts and C2 communications. Use secure DNS services that encrypt DNS queries to prevent manipulation and monitoring.

Secure Cloud and Hybrid Environments

Implement cloud security posture management (CSPM) tools to continuously monitor and remediate cloud configurations. Deploy cloud access security brokers (CASBs) to control and monitor SaaS application usage. Encrypt data both in transit and at rest across all cloud services. Implement modern IAM with strong authentication and least privilege enforcement for all cloud resources. It's especially important to protect nonhuman entities, such as service accounts, API keys, tokens, and automated scripts.

Establish Advanced Endpoint Protection

Deploy next-generation antivirus solutions that use behavioral analysis and machine learning to detect unknown threats. Implement endpoint detection and response (EDR) capabilities that provide real-time monitoring and automated response. Deploy application control technologies that prevent unauthorized software execution. Ensure all endpoints have automated patching systems that apply security updates within 72 hours of release.

Strengthen Email Security Against AI-Generated Threats

Implement advanced email filtering that analyzes message content for AI-generated text patterns. Deploy email authentication protocols, including Domain-based Message Authentication, Reporting, and Conformance (DMARC), Sender Policy Framework (SPF), and DomainKeys Identified Mail (DKIM), to prevent email spoofing. Train users to recognize AI-generated phishing indicators, such as overly perfect grammar, unusual response patterns, or requests that bypass normal business processes. Implement email sandboxing for all attachments and links before delivery to end users.

Enhance Vulnerability Management Programs

Establish automated vulnerability scanning and prioritization based on active threat intelligence. Implement virtual patching for critical systems that can't be immediately updated. Deploy threat hunting programs that proactively search for indicators of compromise before attacks succeed. Unit 42 analysis reveals that in nearly one in five cases, data exfiltration occurs within the first hour of compromise, emphasizing the critical need for rapid detection and response.[36] Maintain real-time asset inventories that include cloud resources, IoT devices, and shadow IT systems.

Create Comprehensive Security Monitoring

Implement security information and event management (SIEM) systems with 24/7 monitoring capabilities and MDR experts as an extension of your team. Deploy security orchestration, automation, and response (SOAR) platforms to speed incident response and automated remediation. Establish threat intelligence feeds that provide real-time information about emerging ransomware campaigns. Create automated incident response playbooks that can contain threats within minutes of detection.

36. *Global Incident Response Report.*

Two Ransomware Cases Demonstrate Palo Alto Networks Rapid Response Capabilities

When an infrastructure manufacturer faced dual Black Basta and LockBit attacks and a telecom provider experienced a 13-hour assault halting 50% of operations, Unit 42 delivered swift containment, threat eradication, and operational recovery.

CASE STUDY | Infrastructure Manufacturer

- **73 PERCENT** reduction in ransom payment due to expert negotiation
- **<5 DAYS** to identify patient zero, the extent of data exfiltration, and block all known ransomware IoCs
- **+2.5 MILLION** files prevented from being exposed through negotiations

CASE STUDY | Telecom Provider

- **3 DAYS** to determine attack vector in 50K endpoint environment
- **80 PERCENT** reduction in ransom with expert negotiation
- **2 DAYS** to contain threat and ensure continuity of business operations

The Unit 42 team accelerated investigation through extensive telemetry, faster threat elimination with limited disruption, and expert response backed by over 1,000 incidents annually. Both organizations regained control and restored critical operations while receiving ransom negotiation support.

Get all the details in these stories:

- Telecom Provider Contains Black Basta Attack and Restores Operations
- Infrastructure Manufacturer Reclaims Control After Dual Ransomware Attacks

How Cortex Helps Prevent, Detect, and Stop Ransomware Attacks

Cortex XDR and Cortex XSIAM® empower you to detect and stop advanced ransomware attacks that target any user or asset—all from one platform and one console. Analysts can quickly stop the spread of malware, restrict network activity to and from devices, and update threat prevention lists, like bad domains, through tight integration with enforcement points. With Unit 42 reporting that 70% of incidents span three or more attack surfaces, the end-to-end visibility offered by Cortex® is a necessity, not a luxury.[37]

With the Cortex platform, you can:

- Block ransomware attacks at every step in the attack lifecycle, from initial exploit to file analysis and behavioral protection with the Cortex XDR agent.
- Find stealthy attacks with AI and cross-data analytics.
- Quickly investigate with root cause analysis.
- Contain any threat with a coordinated response.

The XDR agent layers multiple methods of threat prevention for a highly effective defense against ransomware.

Response options in Cortex XDR and XSIAM include:

- **Live Terminal for direct endpoint access**, which includes a graphical task manager and file manager to view and terminate processes, delete or download files, run commands, and more.
- **Search and Destroy**, which indexes all the files on your endpoints to find and delete malicious files anywhere in your organization in real time.

37. *Global Incident Response Report.*

- **Script execution** from our management console to execute virtually any Python script on one endpoint, a group of endpoints, or all endpoints.
- **Endpoint recovery** to restore and revert changes made to your endpoints as a result of malicious activity.

With our remediation suggestions, you can delete malware, restore files using Windows shadow copy, and remove registry key changes. These features are in addition to more traditional response options like quarantine, network isolation, and blocking files.

Cortex XSIAM takes ransomware investigation and response further—extending coverage across your entire security stack. You can enrich events with threat intelligence, disable compromised user accounts, and block network access at the firewall to stop ransomware and root out adversaries from your environment. And, the powerful out-of-the-box workflows take the guesswork out of ransomware remediation.

Additionally, as a proactive blanket for Cortex XDR and Cortex XSIAM, Unit 42 MDR can augment your SOC team with expert managed, AI-driven defense—powered by Cortex—to stop threats 24/7 across your entire attack surface.

Our proactive threat hunters, analysts, and responders use proprietary AI in Cortex and Unit 42 high-fidelity threat intelligence to accelerate detection, investigation, and response. The result is reduced MTTD and MTTR by up to 90%. We both triage and resolve. With tailored executive reporting, continuous posture optimization, and a unified view of your attack surface, you gain complete visibility, faster protection, and the confidence to stay ahead of advanced threats.

Five Musts If You've Been Attacked

1. **Isolate your network**. Disable network access to compromised devices.
2. **Before rebooting**, carefully consider where the attack information is located. Sometimes you can find the encryption key and other attack information in memory.
3. **Verify adequate data backups** and **determine the overall risk to your organization** if you don't pay the ransom.
4. **See if a decryption tool exists** by searching the No More Ransom website: https://www.nomoreransom.org.
5. **Execute an incident response plan (IRP) or call an IR team such as Palo Alto Networks Unit 42**. Unit 42 brings together an elite group of cyber researchers and incident responders with a deeply rooted reputation for delivering industry-leading threat intelligence. If you think you've been breached or have an urgent matter, contact the Unit 42 Incident Response team by emailing unit42-investigations@paloaltonetworks.com or calling:
   - North America Toll-Free: +1.866.486.4842 (+1.866.4.UNIT42)
   - EMEA: +31.20.299.3130
   - APAC: +65.6983.8730
   - Japan: +81.50.1790.0200

Start Building Your Ransomware Defense Today

For more information about how we can help prevent ransomware attacks and minimize damage if a breach has occurred, view our on-demand webinar Best Practices for Stopping Ransomware and download our Extortion and Ransomware Trends January–March 2025.

Defending against ransomware attacks starts with a plan. Jump-start this process with our Ransomware Readiness Assessment.

Stay in the Know

As we've explored, preventing ransomware requires a multifaceted approach combining advanced technology, proactive strategies, and continuous vigilance. The threat landscape continues to evolve rapidly with AI-powered attacks, sophisticated multiextortion schemes, and increasingly targeted campaigns against critical infrastructure.

For more information on Cortex XDR and Cortex XSIAM, see the following resources:

Cortex XDR

- Visit our webpage.
- Download our XDR For Dummies Guide.
- Learn about our outstanding performance in MITRE ATT&CK Enterprise Evaluations.

Cortex XSIAM

- Visit our webpage.
- Download our e-book "Cortex XSIAM: The AI-Driven SecOps Platform That Goes Beyond Reactive Security."
- Take the XSIAM Product Tour.

To learn more about the Cortex portfolio of solutions, visit our homepage.

Unit 42 MDR

- Visit our webpage.
- Download the *2025 Frost Radar™: Global Managed Detection and Response (MDR)* report.
- Schedule a discovery call with an MDR expert.

About Cortex

Cortex by Palo Alto Networks has redefined solutions for security operations to help organizations deliver the modern security operation center (SOC) experience. Cortex delivers best-in-class threat detection, prevention, attack surface management, and security automation in an integrated platform powered by machine learning and Unit 42 threat intelligence. Trusted by companies around the world and recognized by leading analyst firms, Cortex XDR, Cortex XSOAR®, Cortex Xpanse®, and Cortex XSIAM provide proven protection as standalone solutions and also work seamlessly together as a force multiplier across the SOC. To learn more about Cortex, visit www.paloaltonetworks.com/cortex.

paloalto NETWORKS | TD SYNNEX Public Sector | DLT

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

cortex_wp_what-you-need-to-know-to-survive-ransomware_082225