

Ransomware Readiness in the AI Era:

9 Future-Proof Defense Strategies

Insight 






As AI-powered ransomware becomes commonplace, will your organization be prepared?

It's no secret: Ransomware attacks have grown considerably in frequency and sophistication. By 2028, the global cost of cybercrime is expected to reach a new peak at \$13.8 trillion — a 69% increase from 2023.¹ And that's just the upfront numbers — lost business counts for millions more in ransomware damages.

As technology evolves, bad actors are among the first to adopt advancements. So, hot on the heels of a recent AI boom, now is the time to prepare for an increase in AI-powered cyberthreats.

Read on to learn how AI is expected to shift the modern threatscape and discover nine best practices for AI-powered ransomware preparedness.



Assess and enhance your defenses: Get your Ransomware Readiness Scorecard.

Insight's Ransomware Readiness Scorecard will help you determine the nature of your company's threat profile, evaluate your cybersecurity posture and give you recommendations for mitigating risk and improving security.

[Learn more](#) →

CHAPTER 1

Understanding the threat landscape

AI has become an integral part of the way we live. And while much of the technology we take for granted has AI and Machine Learning (ML) embedded behind the scenes, recent AI developments in Large Language Models (LLMs) and generative AI platforms such as OpenAI's ChatGPT have positioned AI in a new light, making the power of AI accessible to a broader user base.

Ransomware is already wreaking havoc.

The average ransom payment is increasing:



2022 Q1:
\$212,000

2023 Q1:
\$328,000

2023 Q2:
\$740,000²

Top ransomware targets by industry:



Education



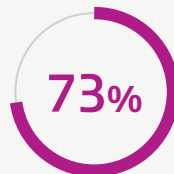
Construction & property



Central & federal government³

24 days

average downtime per attack⁴



of organizations worldwide paid ransom to recover data in 2023.⁵

AI could give bad actors the upper hand.

The vast majority of CISOs (70%) fear generative AI will give cyberattackers the advantage over defenders.⁶ These fears are validated: Action has already been taken against organizations leveraging generative AI for ransomware reconnaissance and development.

The UK's National Cyber Security Centre (NCSC) reports that, while all types of cyberthreat actors are already using AI to some degree, AI — and especially generative AI — will almost certainly increase the volume and impact of cyberattacks in the coming years.⁷

Phishing and other forms of social engineering will likely bear the most notable impacts, at least in these earlier days of AI in ransomware. As phishing is already the number one form of ransomware delivery, AI adoption is especially expected to boost phishing attacks, making them more believable and tougher to detect.

Generative AI: Increasing vulnerability?

75%

of security professionals witnessed an increase in attacks over the past 12 months.

85%

attribute this rise to bad actors using generative AI.

46%

of security professionals say generative AI will make organizations more vulnerable to attack.⁸

Top perceived threats:

- 1 Increase in privacy concerns (39%)
- 2 Increase in undetectable phishing attacks (37%)
- 3 Increase in attack volume and velocity (33%)⁹

AI: Two sides of the same coin

While AI-powered threats are real, the bottom line is this:

The same capabilities that will make ransomware easier for bad actors are the same capabilities that will make threat detection and response more effective for defenders.

AI has been praised for its ability to help users execute with speed, scale and efficiency. This is true for both malicious actors and for cybersecurity professionals. And AI and generative AI are already being leveraged for strong security postures.

Acknowledging AI as part of the modern security team

Skills shortages have plagued the cybersecurity landscape for years, with understaffed, overtaxed teams struggling to maintain a high level of control in the face of alert fatigue. AI is expected to help ratify this issue: 86% of CISOs believe generative AI will alleviate existing security team skills gaps and shortages.¹⁰

AI will also help elevate security staff's skill sets: Security leaders intend to upskill security teams through training on prompt engineering, training on generative AI threats and establishing protocols to determine the types of tasks appropriate for AI-powered bots.¹¹

How companies are using generative AI for cybersecurity¹²

35%

security hygiene and posture management analysis and performance

27%

data enrichment of alerts and incidents

26%

internal communications

26%

analyzing data sources

25%

malware analysis



CHAPTER 2

Best practice checklist for ransomware readiness

When it comes to security breaches, the question is when it will happen, not if it will happen. The most reliable way to fight AI-powered ransomware is to be prepared upfront for any eventuality.

Here are nine best practices for ransomware preparedness that will serve to strengthen your organization's security posture and improve your ability to not only detect and respond to ransomware, but also your ability to recover quickly and with minimal impact in case of an event.

Nine future-proof defense strategies



Patch management

Ensure software, drivers and firmware are kept up to date with new patch releases to reduce risk due to vulnerabilities and optimize performance. The three most common types of patches include security patches, bug fixes and feature updates — all of which play an important role in your cybersecurity posture.

- **Network scan:** Perform scans on a weekly basis to check for vulnerabilities and prioritize based on the criticality/CVSS score.
- **Security:** Patch management fixes vulnerabilities in your software and applications that are susceptible to cyberattacks, helping your organization reduce its security risk.
- **System uptime:** Patch management ensures that your software and applications are up to date and running smoothly, supporting continuous system uptime.
- **Compliance:** Given the increasing frequency of cyberattacks, organizations are often mandated by regulatory bodies to maintain a certain level of compliance. Patch management is a crucial component of adhering to these compliance standards.
- **Feature improvements:** Patch management can extend beyond software bug fixes to also include updates to features and functionalities. Patches can be critical in ensuring that you have access to the latest and greatest offerings of a product.

2



Employee education

A concerning number of data breaches can be traced back to human error. Prioritize teamwide training as a critical component of your cybersecurity strategy. Training on cybersecurity hygiene and phishing attempts can help minimize the human element inherent in security risk.

- **Regularly train employees** on cybersecurity attack vectors.
- **Educate** on the safe use of removable media (e.g., USB).
- **Provide guidance** on recognizing phishing emails, text messages or social media messages.
- **Foster** a robust security culture within the organization.

3



Access control

Outdated or fragmented network infrastructure often lacks the built-in visibility and security controls necessary for adequate protection. Identify and implement best-fit access control frameworks for your organization such as the Principle of Least Privilege (POLP), Multi-Factor Authentication (MFA), Zero Trust Network Access (ZTNA) and advanced authentication strategies.

- **Implement** proper Role-Based Access Control (RBAC) and Privileged Identity Management (PIM) for resource access.
- **Apply** the POLP to vendor management.
- **Conduct** weekly audits of access controls to identify any unusual activity.





4



Network security

Networks offer a host of vulnerabilities. In addition to careful access control, network architecture should take into consideration strategies for network segmentation, the use of IDS/IPS and firewall integration to mitigate the spread of potential malware.

- **Deploy** next-gen centralized firewalls for internal and network edge, restrict outbound traffic and implement Geo-IP filtering.
- **Establish** proper network segmentation based on environment or workload (e.g., development, QA, testing, production).
- **Use proper network security group rules** to restrict both internal and external network flow.
- **Implement** network IPS and IDS to detect and lure malicious activity in the environment.
- **Block** known malicious IP addresses used by known bots and ransomware hosts.
- **Employ DDoS protection** to defend against bot-led attacks.

5



Email filtering

Sophisticated email filtering techniques can help prevent phishing attempts from reaching teammates' inboxes and stop malware from infiltrating your organization. Defense technologies for inbound emails should ensure that only emails from trusted sources are accepted, that domains are validated, and that spam and malicious content are filtered out.

This feature:

- **Scans email attachments** for both known and unknown malware signatures and blocks potentially harmful messages.
- **Detects and removes** unsolicited email messages, reducing the risk of phishing attacks.
- **Blocks email messages** from known malicious IP addresses.
- **Automatically encrypts** email messages that meet specific criteria, such as containing sensitive information or being sent to external recipients.
- **Uses DKIM, SPF and DMARC policies** to authenticate email senders by verifying that the email came from the stated domain.
- **Allows users to digitally sign and encrypt** email messages, ensuring the authenticity and confidentiality of the communication.

6 Know your vulnerabilities

Strengthening your vulnerabilities first requires knowing where your weaknesses lie. Partnering with an expert provider of cybersecurity consulting and services can help your organization take the critical step of identifying and addressing the vulnerabilities within your existing infrastructure and teams.

7 Secure your data

Data protection is paramount in safeguarding sensitive information and maintaining the trust of customers, partners and stakeholders. Many organizations mistakenly believe there is inherent data security in the cloud. However, this is not the case. The sole responsibility for total data protection falls upon the owner of that data. While some cloud providers may offer a level of data protection, it is your responsibility to seek out and adopt the necessary data protection measures for your organization, including third-party solutions.

- **Encrypt all data** in and out of the corporate network.
- **Use** encryption for data at rest.
- **Implement proper Data Loss Prevention (DLP) policies** for sharing data across users and clients: Use data labels on all documents being stored, sent out and archived to identify data leakage and exposure.
- **Encrypt all workstations and servers** using in-house encryption keys.
- **Utilize** automated threat detection tools.
- **Regularly analyze** security logs.

8 Back up your backups

In today's threatscape, backups are no longer safe. Many malicious actors have developed highly targeted programs designed to identify and seize an organization's backup files as the primary target. This has made reliable off-site backup strategies — including air-gapping solutions such as tape, which have previously been considered outmoded — more necessary than ever.

Follow the 3-2-1 rule: Try to keep three separate copies of your data on two different storage types, with one copy offline. You can also enhance this process by adding another copy to an immutable (can't be altered), indelible (can't be deleted) cloud storage server.

9 Have a plan

Why is it that so many organizations find themselves facing a security event with no predetermined plan of action in place? A disaster recovery plan should be nonnegotiable. From network security considerations to legal implications, evaluate all the potential impacts of a ransomware event and determine a customized, actionable incident response plan. Ensure the plan is well documented and extends to your entire organization. Test your plan in your current environment for any flaws, adjusting as necessary and practicing on a timely basis, continuing to revise as needed. This ensures internal teams are ready to respond quickly and effectively in case of an event and that your plan is up to date and optimally positioned for best results.

CHAPTER 3

Advanced defensive strategies

Incident response planning

Don't make the mistake of waiting for an incident to figure out your response strategy. Start creating and practicing your incident response strategy as soon as possible.

Key considerations for planning your strategy include:

- Storage of documentation and credentials
- Tabletop exercises
- Capacity planning
- Performance testing
- Backup vs. replication
- Communication management
- Administrative access
- Process automation
- Business Continuity/Disaster Recovery (BC/DR) tests
- Staffing and development
- Documentation of cyber event response



Incident Response Playbook: Empower Your Teams to Handle Modern Threats

Read this guide to uncover more details on the processes listed on the left and give your organization the starting point it needs to craft a strong incident response strategy.

[Read the ebook](#) →

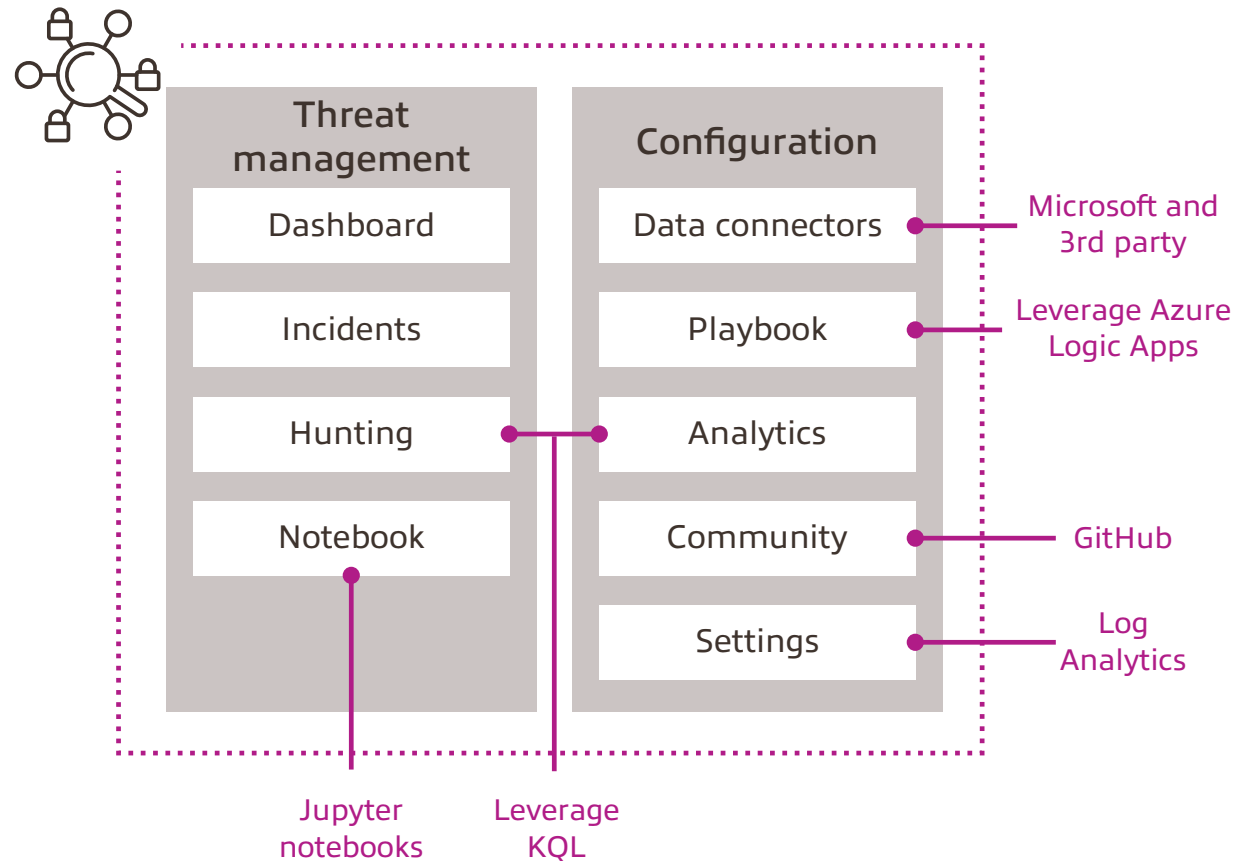
Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR)

Advanced SIEM/SOAR solutions help empower Security Operations Center (SOC) teams to detect and respond to cyberattacks and write and deploy automated response playbooks. Microsoft Sentinel™ is one such solution, offering users a cloud-native advantage with limitless scalability and seamless integration.

Microsoft Sentinel architecture

Microsoft® Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting and threat response.

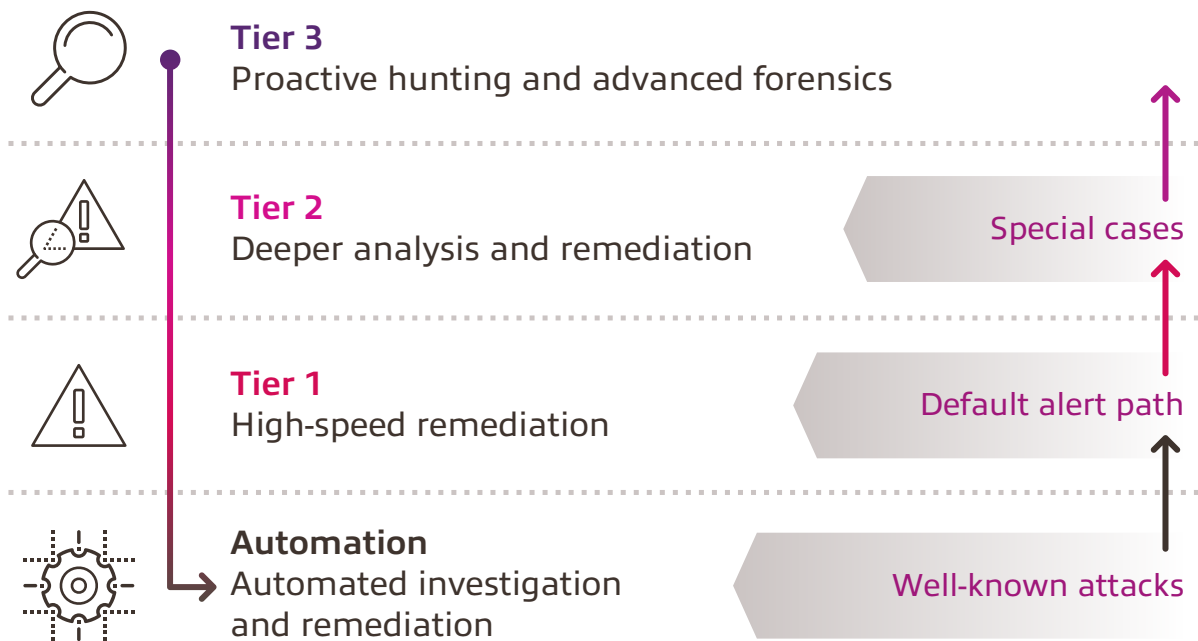
Sentinel natively incorporates proven foundation services from Azure®, such as Log Analytics and Logic Apps. Also, it enriches investigation and detection with AI in conjunction with Microsoft's threat intelligence stream. The below diagram depicts major Microsoft Sentinel components.



Threat hunting

Threat hunting is the process of iteratively searching through a variety of data to identify threats in the systems. Threat hunting involves creating hypotheses about the attackers' behavior and researching the hypotheses and techniques that were used to determine the artifacts that were left behind.

As you can see in the figure below, Tier 3 is responsible for performing proactive hunting and advanced forensics. The goal of this team is to perform an analysis to identify anomalies that may indicate advanced adversaries. While most incidents are remediated at Tiers 1 and 2, only unprecedented findings or deviations from the norm are escalated to Tier 3 teams.



Microsoft Sentinel has a dedicated threat hunting capability designed specifically for hunt teams and Tier 3 analysts, and ships with built-in hunting queries that have been written and tested by Microsoft security researchers and engineers. Within Sentinel, an analyst can create a new query, modify existing queries, bookmark, annotate and tag interesting findings, and launch a more detailed investigation.

Endpoint security

The average workplace uses many more endpoints now than in the past. The number of devices in play in any given organization is constantly in flux, and constantly growing. And each endpoint represents a potential avenue for risk. Thus, endpoint security is another critical part of a strong defensive strategy against ransomware.

There are three main types of endpoint security:



Endpoint Protection Platform (EPP)

EPP works to prevent attacks from threats such as malware through using databases of known signatures to identify threats, blocking or allowing certain applications, URLs, etc., and providing a sandbox to test suspected threats.



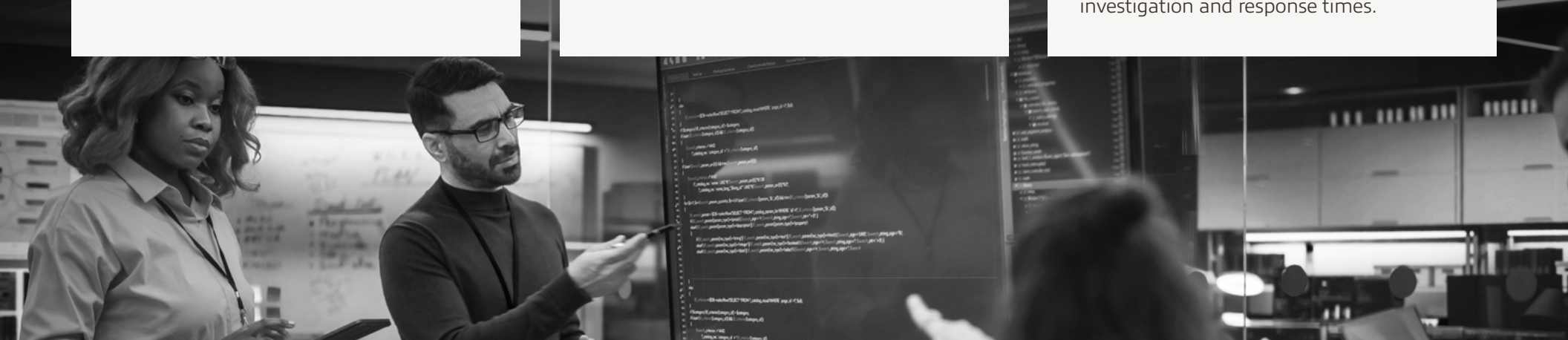
Endpoint Detection and Response (EDR)

EDR is used to examine and respond to incidents after they have happened. Functions include identifying indicators of compromise, providing real-time alerts and executing automated remediation through actions such as wiping or reimaging affected endpoints.



Extended Detection and Response (XDR)

XDR integrates security and incident response, combining security data from tools like SIEM, EDR, and Identity and Access Management (IAM) to provide an overview of the environment in its entirety. This helps security teams improve productivity with faster, more effective investigation and response times.





Post-attack recovery

Effective recovery planning and asset restoration post-attack are crucial aspects of cybersecurity management.

Here are some insights:

- **Comprehensive incident response plan:** Develop a detailed incident response plan that outlines roles and responsibilities, escalation procedures, and steps for mitigating and recovering from cybersecurity incidents. Ensure that all relevant stakeholders are aware of their roles and are trained on the procedures.
- **Testing and validation:** Regularly test and validate your backup and recovery processes to ensure they are effective and up to date. Conduct simulated attack scenarios to assess the readiness of your team and the effectiveness of your recovery plan.
- **Prioritize restoration:** Identify critical assets and systems that need to be restored first to minimize downtime and disruption to operations. Develop prioritization criteria based on the impact of the attack on business operations and customer service.
- **Communications plan:** Develop a communications plan to keep stakeholders informed about the incident, recovery efforts and any impact on operations. Provide regular updates on the progress of recovery efforts and steps being taken to prevent future incidents.
- **Continuous improvement:** After the recovery process is complete, conduct a post-incident review to identify lessons learned and areas for improvement. Use this feedback to update and enhance your incident response plan and recovery procedures for future incidents.

By implementing these strategies, organizations can effectively plan for and recover from cybersecurity incidents, minimizing the impact on operations and restoring normal business functions in a timely manner.

CHAPTER 4

Implementing AI for proactive defenses

Attackers are adopting AI at incredible speed. The only way to stay ahead is to move faster. If your organization hasn't already integrated AI for enhanced ransomware prevention, detection and response, now is the time.

AI plays a pivotal role in bolstering cybersecurity, particularly in the realms of ransomware detection, user behavior monitoring and MFA:

- **AI-driven SIEM solutions** facilitate initial detection by employing pattern recognition and correlation techniques within logs. They scrutinize activities associated with known attack vectors, such as Windows® behavior monitoring disablement, ransomware extension files, privilege escalation, data exfiltration and deletion of volume shadow copies.
- **Enhanced monitoring** of traffic parameters, including communication with malicious IP addresses, URLs, domains and suspicious geographic locations, is made possible through advanced analysis of firewall logs.
- **AI-powered tools** monitor user behavior, such as lateral movement within the environment, using services like Defender for Identity. These systems leverage AI to forecast compromised user accounts and potential account takeovers.
- **MFA** provides an additional layer of security for end users. Authentication methods such as authentication applications and FIDO keys help mitigate the risk of user compromise, thereby reducing the likelihood of further attacks on the environment.



Fortifying web applications against ransomware

Web applications serve as common entry points for ransomware attacks due to various vulnerabilities that can be exploited by attackers.

These vulnerabilities include:

- **SQL injection:** This vulnerability arises when attackers inject malicious SQL code into web applications, allowing them to extract data from SQL Server® devices.
- **Cross-Site Scripting (XSS):** Attackers inject malicious code into web applications, enabling them to steal user data or execute commands on users' browsers.
- **File inclusion:** This vulnerability occurs when a web application allows users to include files from external sources, such as uploading a file.
- **Remote code execution:** Attackers exploit this vulnerability to execute arbitrary code on a web server.

Securing web applications is crucial to prevent ransomware attacks and protect against unauthorized access, data breaches and other security incidents.

Key measures to consider include:

- **Using Web Application Firewalls (WAFs):** WAFs can help protect web applications from attacks by filtering out malicious traffic.
- **Implementing secure coding practices:** Developers should adhere to secure coding practices, such as input validation and output sanitization, to prevent injection attacks.

Safeguarding web applications against ransomware is imperative in today's threat landscape. By addressing these vulnerabilities and prioritizing security measures, organizations can fortify their defenses against malicious attacks and ensure the integrity and safety of their web applications.

Conclusion

Fight fire with fire. With an AI-equipped ransomware readiness strategy and a tried-and-tested data protection approach, your organization can be equipped to face ransomware attempts with confidence — even as the incidence of AI-supported attacks increases.

Strengthen your ransomware readiness today with Insight.

[Contact us to get started.](#)

Ready to fortify your defenses against ransomware threats?

Take action with [Insight's Ransomware Readiness Scorecard](#) and test and maintain your defense strategies to keep in step with ever-evolving technologies and threat vectors.

Security unmanageable? Discover Managed Security.

For organizations that need a more hands-off way to ensure proactive security, [Insight's Managed Security Services](#) offer a complete solution to address security challenges and protect against threats.

Explore these related resources for further reading on ransomware readiness.



Managed Services

Client story: [State Government Improves Safety & Service for Millions](#)

Video: [Scalability & Recoverability With Insight Managed Security](#)

Webinar: [Gain 24/7 Security Support With Managed XDR](#)

Webinar: [Maximize Your Cloud Security](#)

Solution brief: [Managed Security](#)



Data protection

Webinar: [Defend, Detect, Recover: Three Essential Steps to Protecting Data](#)

Webinar: [Guide to Cloud Security and Data Protection](#)

Infographic: [CISO's Checklist: 5 Attack Surfaces to Prioritize Now](#)

Infographic: [Streamline Network Security With SASE](#)

Infographic: [Long Live Tape — And Other Data Protection Trends for a New Threatscape](#)

eBook: [Securing Your Business Assets With Zero Trust Architecture](#)



Ransomware, incident response, disaster recovery & more

eBook: [Ransomware Readiness Best Practices](#)

eBook: [Elevate & Innovate: The CISO's Guide to Overcoming Cybersecurity Challenges](#)

eBook: [Incident Response Playbook: Empower Your Teams to Handle Modern Threats](#)

Infographic: [Back to Basics: Baseline Considerations for Ransomware Recoverability](#)

Infographic: [Your 2024 Security Checklist](#)

Solution brief: [Vulnerability Management Program Review](#)

Solution brief: [Identity and Access Management Advisory Assessment](#)

Solution brief: [Ransomware Prevention and Recovery](#)

About Insight

Insight Enterprises, Inc., is a Fortune 500 Solutions Integrator with 13,000 teammates worldwide helping organizations accelerate their digital journey to modernize their business and maximize the value of technology. We enable secure end-to-end transformation and meet the needs of our clients through a comprehensive portfolio of solutions, far-reaching partnerships and 35 years of broad IT expertise. Rated as a Forbes World's Best Employer and certified as a Great Place to Work, we amplify our solutions and services with global scale, local expertise and a world-class eCommerce experience, realizing the digital ambitions of our clients at every opportunity.

[Discover more at insight.com.](https://www.insight.com)



Sources:

- ¹ Petrosyan, A. (2023, Nov. 15). Estimated cost of cybercrime worldwide 2017-2028. Statista.
- ² Petrosyan, A. (2023, Sept. 1). Average amount of cyber ransom payments at organizations worldwide from 1st quarter 2022 to 2nd quarter 2023. Statista.
- ³ Irei, A. (2024, Jan. 31). Top 13 ransomware targets in 2024 and beyond. TechTarget.
- ⁴ Petrosyan, A. (2023, Aug. 28). Average duration of downtime after a ransomware attack at organizations worldwide from 1st quarter 2020 to 2nd quarter 2022. Statista.
- ⁵ Petrosyan, A. (2023, Aug. 31). Annual share of companies worldwide that paid ransom and recovered data from 2018 to 2023. Statista.
- ⁶ Kovar, R. and Paine, K. (2023). The CISO Report. Splunk.
- ⁷ National Cyber Security Centre. (2024, Jan. 24). The near-term impact of AI on the cyber threat.
- ⁸ Voice of SecOps 4th Edition. (2023). Generative AI and Cybersecurity: Bright Future or Business Battleground? Sapio Research sponsored by Deep Instinct.
- ⁹ Ibid.
- ¹⁰ Kovar, R. and Paine, K. (2023). The CISO Report. Splunk.
- ¹¹ Ibid.
- ¹² Ibid.