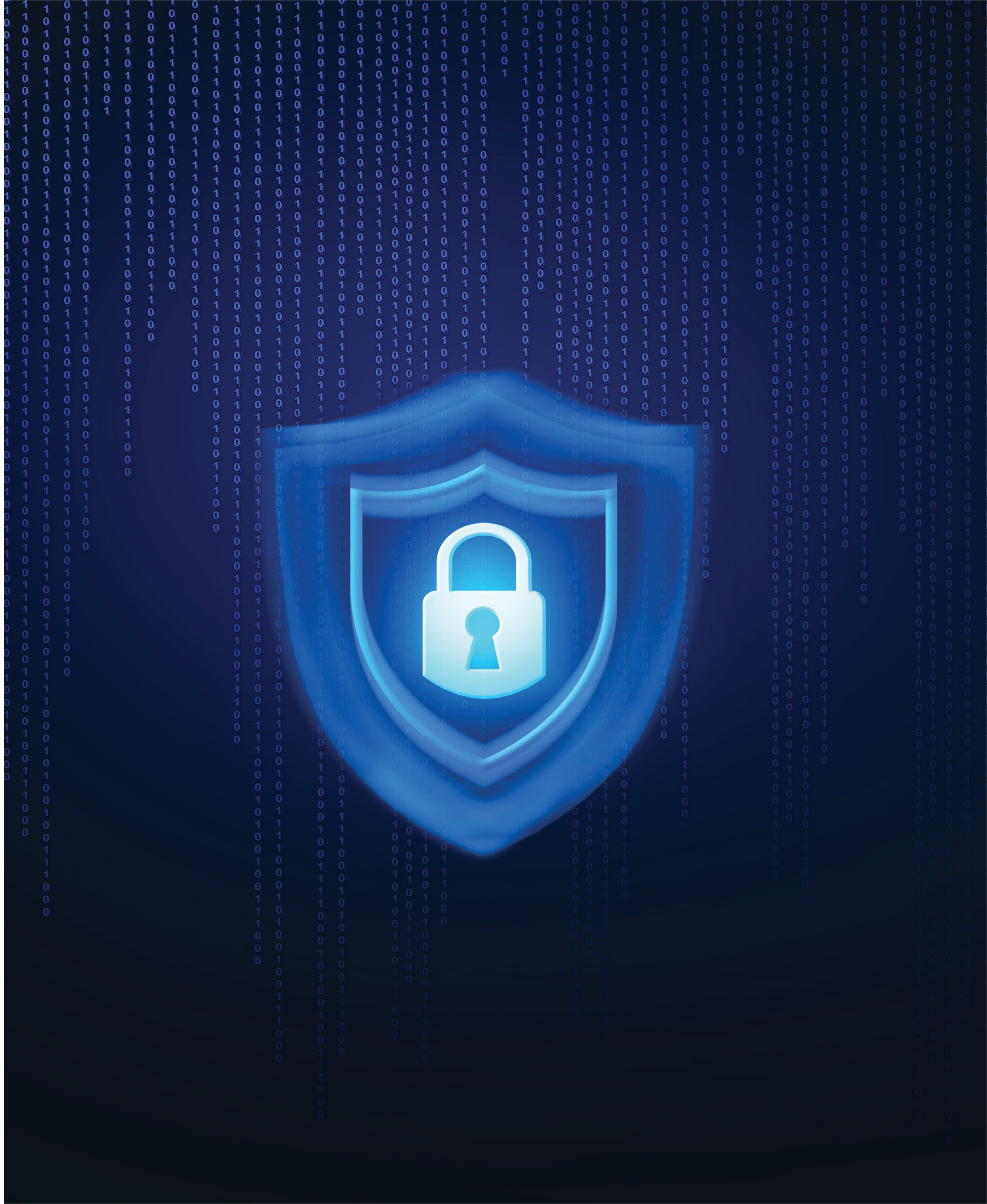
Recorded Future®

Proactive Ransomware Mitigation

Elevating Security Defenses with Threat Intelligence



Recorded Future®

Executive Summary

What’s the cost to your business if you can’t ship products or provide services or access to your platform for days or weeks? What would be the impact if your customers’ personal information was stolen, your stock price declined, or you lost market share? These are just some of the possible outcomes of a ransomware attack. Such devastating consequences have fundamentally changed the way organizations should think about **ransomware**: it is no longer just a security problem; it is now a business problem.

Gartner warns that ransomware is

> “one of the key external threats facing organizations today.” [1]

These attacks are soaring at a staggering rate, up **70% year over year from 2022 to 2023**[2], shutting down utilities, banks, hospitals, schools, governments, media outlets, airlines, hotels, and more. No organization is immune from this threat, with 66% of organizations reporting they’ve already been hit by ransomware.[3] Because the business impacts are now so severe, preventing ransomware should be considered a high priority at every level within your organization, including the executive team and board.

How can you fortify your business and proactively prevent these attacks?

Utilizing threat intelligence for proactive ransomware mitigation arms your organization with real-time, actionable insights so you can:

- Identify, investigate, and prioritize cyber threats
- Prioritize and mitigate vulnerabilities based on risk
- Discover and protect the expanding attack surface
- Prevent misuse of compromised credentials and identities
- Protect the business value chain including vendors, partners, and contractors

The following eBook will explore the current state of ransomware and why it has become a fundamental business problem. You’ll learn how to create your own approach to ransomware prevention and the key components of an effective threat intelligence solution for ransomware mitigation. Finally, you will hear how other organizations have implemented an “intelligence-centric” approach to proactively protect their business.

⚠ **66%** of organizations have been hit by ransomware.

⚠ **84%** of those lost business or revenue.

Recorded Future®

The Threat is Growing and Evolving

Attacks are on the rise

Ransomware attacks accounted for nearly one-quarter of all breaches in 2023, affecting nearly all types of businesses and industries.

66%

of organizations experienced a **ransomware attack over the past year**[4]

43%

of organizations had their data or systems held hostage[8]

84%

reported lost business or revenue. [9]

Threat actors are growing more sophisticated

Hackers now tailor attacks to specific organizations to yield greater ROI. They also subject their victims to 'triple extortion,' in which organizations pay the initial ransom, are attacked again through vulnerabilities hackers discovered during the first attack, and may suffer future attacks when their information is sold as part of the Ransomware-as-a-Service (RaaS) economy to another hacker.

Breaches are direct and indirect

Ransomware is often introduced through phishing attacks with the intent to trick individuals into revealing personal information, like passwords. 78% of organizations have experienced email-based ransomware attacks[10]. Hackers also gain access to corporate systems via supply chain ecosystems. Enterprises connect with an average of 173 third parties[11]–each a potential gateway into their network. Consequently, 93% of companies have suffered a cybersecurity breach because of weaknesses in their supply chain.[12]

Attack on MGM Resorts International

In 2023, hackers obtained credentials from MGM's IT Help Desk by impersonating an employee to access, infect, and lock their systems. MGM refused to pay the ransom, and it took 10 days for most systems to be brought back online. 10.6 million guests had personal information stolen and published on a hacking forum.[13]

Business impact

$ 100 million loss due to

- Lost revenue
- Business disruption: Room digital keys and slot machines stopped working, websites for many properties went offline, and guests waited hours to check into the hotel and for handwritten receipts for casino winnings
- Technology consulting services, legal fees, and expenses of other third-party advisors
- Free credit monitoring services for affected guests

Ransomware is a Business Problem

A ransomware attack has a direct impact on a business's bottom line.

Ransomware payments nearly doubled from 2022 to 2023 to $1.5 million[14], and the average total cost of a data breach disclosed by the attacker has risen to $5.2 million[15]. However, costs can be significantly higher, with Caesars Entertainment making a $15 million ransomware payment in 2023 and MGM spending a $100 million to deal with the total cost of their breach that same year–without paying the ransom.

Ironically, the ransom payment is least of an organization's concerns, says Gartner: "The real threat is not ransomware itself, but the impact on the business from the sudden elimination or interruption of services or processes.[16] The cost of recovery and the resulting downtime in the aftermath of a ransomware attack, as well as the reputational damage, can be 10 to 15 times more than the ransom."[17]

Aside from paying a ransom, financial outcomes can include loss of revenue, business, and market share, with 84% of ransomware victims reporting business and/or revenue loss due to an attack.[18] Public companies reported suffering a 7.5% decline in their stock values after a data breach, combined with a mean market cap loss of $5.4 billion.[19] Indirect costs can be even more damaging, from reputation damage and customer attrition to massive fines and lawsuits.

Attack on Loan Depot

LoanDepot, the fifth-largest retail mortgage lender in the U.S., disclosed that on January 6, 2024, ransomware hackers accessed company systems and encrypted data.

The company shut down several systems to contain the incident. 16.6 million customers had their sensitive personal information stolen.

Business impact

- Customers were unable to make mortgage payments or access their online accounts.
- The financial impact has not yet been disclosed, but it will likely be in the tens of millions of dollars or more due to regulatory fines, business disruption, the cost of working with forensic, security and legal services, and providing affected customers with credit monitoring services.

Recorded Future®

How to Plan Your Defense

Before looking for a threat intelligence solution for ransomware mitigation, ask and answer critical questions to develop the best approach to preventing attacks aimed at your organization.

Where do we focus?

96% of security decision makers believe it is important to understand which threats could be targeting their organization.[20] However, with 2,200 cyberattacks occurring daily[21] and hundreds of ransomware groups and initial access brokers operating–all with different motives, organizations are feeling overwhelmed and vulnerable.

The key to prevention is focusing on those threat actors with a high intent to target your organization, due to either financial gains or for ideological purposes. Intent, though, is nothing without an opportunity to target your organization.

Do you still have the MOVEit file transfer vulnerability unpatched? Unpatched software and exposed credentials provide the chance for a threat actor to target your organization. By focusing in on individual threat actor groups, using comprehensive threat intelligence tools, you can be more prescriptive with how you implement controls that are truly effective.

What's exposed?

Digital integration has led to an explosion of assets on the public internet due to an uptick in the remote workforce, cloud sprawl, hybrid environments, merger and acquisition events, and more – making it increasingly harder for organizations to maintain a persistent view of their internet-facing assets. To compound this problem, assets move, change, and are added constantly, and this dynamic nature means traditional asset inventory processes cannot keep up. Your external attack surface is in a constant state of change and growth–increasing 18% per year. [22] This can lead to dozens or hundreds of unknown or unprotected assets, greatly increasing the risk of a cyberattack.

76% of organizations have experienced a cyberattack due to an unknown or mismanaged asset. [23] Because you can't secure what you can't see, it's critical that you uncover blind spots and gain visibility into all assets along your external attack surface. Technology can help you understand what common vulnerabilities, exposures and misconfigurations are active for your company, as well as which internet-facing assets might be out-of-policy, so your team can be more proactive, strengthening your security posture.

Recorded Future®

How to Plan Your Defense

What’s vulnerable?

60% of breaches are tied to unpatched vulnerabilities,[24] and threat actors are exploiting these vulnerabilities faster than ever. 47% of security practitioners agree the inability to prioritize what needs to be fixed is the primary reason for their vulnerability backlog.[25]

But vulnerability management is overwhelming: patching is resource-intensive, and there are simply too many vulnerabilities to address. Common Vulnerability Scoring Systems (CVSS) prioritization isn’t sufficient, and organizations lack visibility into vulnerability exploitation.

The best way to protect your organization is to understand your attack surface, what vulnerabilities you are susceptible to, and which vulnerabilities are being actively exploited by ransomware groups or other threat actors.

Using threat intelligence, organizations can improve vulnerability management to help security teams track vulnerabilities being exploited in the wild and CVEs that could be weaponized in the future.

What’s stolen?

86% of beaches involve the use of stolen credentials.[26] Your dynamic ecosystem of employees, partners, supply chain vendors, and customers is facing a sharp increase in account takeovers. Adversaries are looking to steal credentials so they can access and initiate fraudulent activities. In addition, there is a lucrative market for initial access brokers selling credentials on dark web channels, which organizations are unable to monitor on their own.

Actionable and timely intelligence on novel compromised credentials sold on dark web channels helps security teams be more proactive with getting ahead of risks, which can include issuing a password reset or placing the account under stricter controls. With the proliferation of infostealer malware being used by threat actors, multi-factor authentication is no longer enough to reduce the risk of an account compromise.

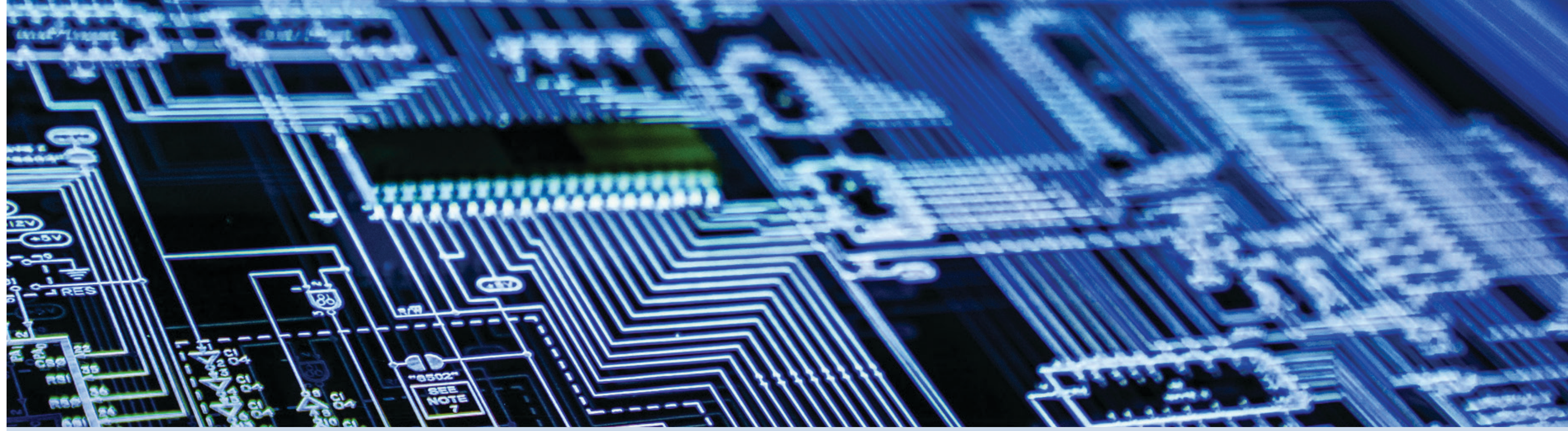
Recorded Future®

Preventing Ransomware Requires Proactive Insights

Threat Intelligence: Identify, investigate, and prioritize cyber threats

When you're dealing with thousands of alerts daily, it's difficult to identify which threats are relevant to your organization. Threat Intelligence can quickly provide detailed profiles of the threat actors targeting organizations like yours and the techniques and tools they are using. This information enables your threat hunters to work smarter and faster by prioritizing searches for the most dangerous threats to your organization.

Some solutions provide context like Indicators of Compromise (IOCs), sandbox analysis, and hunting packages to give you the information you need to take action, power remediation, mitigate threats directly, and integrate the intelligence into your existing security tools.



> "**To support our proactive approach to security,** we needed to invest in threat intelligence to prepare us for cyberattacks before they happen. Recorded Future's wide coverage and volume of information led to our initial evaluation of their intelligence, and later to choosing Recorded Future as our intelligence provider."

Takashi Amano, General Manager
Cyber Security Technology Center, Toshiba

Toshiba Shifts from Reactive to Proactive Security with Recorded Future

Using Recorded Future, Toshiba has established an "intelligence-centric" approach to security, powering proactive protection of their business through a wide breadth of coverage and proactive alerting capabilities.

Recorded Future®

Preventing Ransomware Requires Proactive Insights

Vulnerability Intelligence: Prioritize and mitigate your vulnerabilities based on risk

With thousands of new critical vulnerabilities disclosed each year, security operations teams are increasingly overwhelmed trying to prioritize vulnerabilities using traditional asset criticality and severity inputs. Vulnerability Intelligence prioritizes threats based on risk, allowing security teams to focus on critical vulnerabilities that pose a real risk to the organization's sensitive data and overall security posture.

By automatically collecting, structuring, and analyzing billions of indexed facts from a massive volume of open, dark, and technical sources, Vulnerability Intelligence can alert your teams to newly disclosed vulnerabilities days before they're published in the U.S. National Vulnerability Database (NVD), and give them the comprehensive intelligence needed to make fast, confident prioritization decisions.

Attack Surface Intelligence: Discover and protect your expanding attack surface

Many of your internet-facing assets may be forgotten and unsecured while new assets are added every day. Because organizations often rely on manual or ad-hoc processes and inefficient technologies to discover and track these assets, security teams are operating with limited visibility into their attack surface, causing delayed responses to critical vulnerabilities, a backlog of exposures to remediate, and an unclear picture of what to prioritize.

Attack Surface Intelligence reduces risk by improving asset visibility, prioritizing exposures to remediate, and enforcing security controls. It automatically and continuously discovers and tracks internet-facing assets associated with your organization, as soon as they surface on the internet, including high-risk CVEs, misconfigurations, exposed administrative panels, assets that fall out of policy compliance, and more. Armed with actionable exposure scoring and a real-time inventory, security teams can prioritize and remediate risky assets.

Recorded Future®

Preventing Ransomware Requires Proactive Insights

Identity Intelligence: Prevent misuse and protect compromised credentials and identities

Unable to keep up with the growing onslaught of attacks and continuous monitoring of the dark web for compromised credentials on their own, organizations are not able to be proactive and are left exposed to financial, legal, and reputational consequences.

Identity Intelligence enables users to monitor for compromises in real time, and access critical details, such as password length, complexity, and whether the leak was novel or recycled. Armed with this real-time evidence, security and IT teams can quickly prioritize identity threats and initiate downstream response workflows, integrated directly into their existing security and identity tools.

Third-Party Intelligence: Protect your business value chain

While your vendors, suppliers, partners, contractors, and resellers all add value to the business, they also introduce risk. Third-Party Intelligence uses machine learning and natural language processing to monitor in real time for key indicators that a member of your ecosystem has been compromised.

These indicators include evidence of ransomware extortion, security incidents, malicious network activity, credentials leakage, domain abuse, vulnerable infrastructure, web application security, and more. By receiving risk-prioritized alerts in real time, your security team will immediately know about new risks and their severity, and have the context and evidence required to address threats quickly and confidently.

Recorded Future®

Proactively Protect Against Ransomware Attacks with Recorded Future

Recorded Future's Intelligence Cloud empowers organizations with the tools and insights needed to stay ahead of threats. By using the Recorded Future Intelligence Cloud as part of your defensive toolkit against ransomware attacks, you'll gain comprehensive visibility into your attack surface, prioritize alerts for accelerated detection and response, and stay informed about the evolving ransomware threat landscape.

Gain visibility into your attack surface exposures

Detect high risk CVEs, misconfigurations, end-of-life software, and additional types of exposed assets that could be exploited by attackers.

90% of our clients have a better understanding of their threat landscape now by using Recorded Future.

Prioritize the alerts that matter

Reduce alert noise and prioritize the alerts that matter with risk scoring and evidence. Recorded Future identifies patterns across multiple IOCs and automates remediation through integrations with your existing security workflows and tools.

Recorded Future clients save an average of 6.5 hours per user per week on threat mitigation efforts using our solution.

Get in-depth insights on adversaries

Gain comprehensive and real-time visibility into your relevant ransomware landscape including bad actors, their tactics, techniques, and procedures (TTPs), targets, and intent so you can focus mitigation efforts, stay ahead of threats, and protect your organization.

Our clients are 48% faster at identifying a new threat than prior to using Recorded Future.

Recorded Future®

Cummins Gains Asset Visibility and Exposure Prioritization

Challenge:

Spent ~80 hours a week trying to map their changing attack surface

Unable to prioritize risks due to manual processes and labor intensive workflows

Solution:

Alerted to newly-discovered assets and exposures

Continuously identifies and prioritizes key areas of risk to help secure their business

Views external assets with the same perspective as an attacker

Business Impact:

163%	decrease in risk from vulnerabilities
51%	decrease in overall vulnerable attack surface
32%	decrease in cyber insurance premium year on year

> “Recorded Future shows us how we can take action and takes our risk assessments to the next level.”

Mattheus Bittick, Attack Surface Reduction Analyst at Cummins

Recorded Future®

Strengthen Your Defenses with Threat Intelligence

By 2031, experts predict ransomware threat actors will attack a business, consumer, or device every two seconds and will collectively cost victims $265 billion annually. [27] Automation and intelligence will be essential to preventing these attacks and protecting your business.

Recorded Future is the most comprehensive and independent threat intelligence cloud platform on the market, named a leader in The Forrester Wave™ External Threat Intelligence Service Providers, Q3 2023 report.

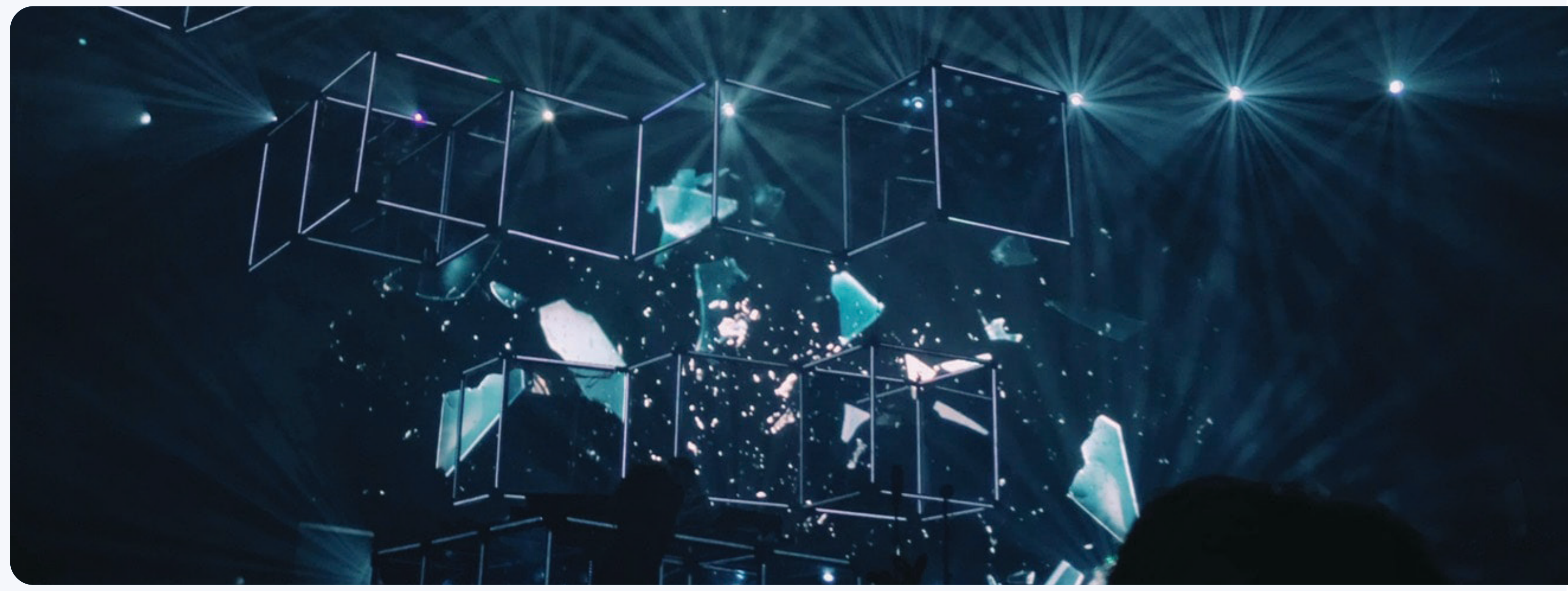
With Recorded Future, you are better prepared to detect ransomware attacks in their early stages, establish relevant controls, mitigate risk, and protect your organization.

Multinational energy organization NOV protects its business investments, and reputation with Recorded Future

Using Recorded Future, NOV's CISO reports he and his team have:

- Automated intelligence into day-to-day tasks they'd otherwise perform manually
- Access to critical intelligence to analyze and prioritize threats
- Confidence about what's high risk vs. low or no priority
- Insights needed to report up to senior leadership and deliver a quarterly board presentation about evolving threats
- Intelligence to guide future investments in cybersecurity defense and keep leaders from missing threats that could damage the company's reputation with potential investors and customers

FORRESTER®
WAVE
LEADER 2023
External Threat
Intelligence Service
Providers



To learn more about the Recorded Future Intelligence Cloud and how we can help you protect your organization from ransomware, request a demo or talk to your customer success representative.

Endnotes

[1] https://www.gartner.com/en/doc/how-to-prepare-for-ransomware-attacks

[2] https://www.darkreading.com/cyberattacks-data-breaches/2023-ransomware-attacks-up-more-than-95-over-2022-according-to-corvus-insurance-q3-report

[3] https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

[4] https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

[5] https://assets.sophos.com/X24WTUEQ/at/h48bjq7fqnqp3n5thwxtg4q/sophos-the-state-ransomware-2023-infographic-1200-1200px_2x.png

[6] https://www.verizon.com/business/resources/reports/dbir/s

[7] https://assets.sophos.com/X24WTUEQ/at/h48bjq7fqnqp3n5thwxtg4q/sophos-the-state-ransomware-2023-infographic-1200-1200px_2x.png

[8] https://www.splunk.com/en_us/pdfs/gated/ebooks/state-of-security-2023.pdf

[9] https://assets.sophos.com/X24WTUEQ/at/h48bjq7fqnqp3n5thwxtg4q/sophos-the-state-ransomware-2023-infographic-1200-1200px_2x.png

[10] https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[11] https://www.auditboard.com/blog/murky-visibility-across-the-supply-chain-how-organizations-are-overcoming-tprm-roadblocks/

[12] https://www.wsj.com/articles/third-party-cyber-risk-management-primer-aug-2023-update-797c7377

[13] https://www.techtarget.com/searchsecurity/news/366554695/MGM-faces-100M-loss-from-ransomware-attack

[14] https://www.weforum.org/agenda/2023/09/next-international-ransomware-attacks/

[15] https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700077724064000&p5=e&g

[16] https://www.gartner.com/en/documents/4022384

[17] https://www.gartner.com/en/doc/how-to-prepare-for-ransomware-attacks

[18] https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

[19] https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

[20] https://www.mandiant.com/resources/blog/requirements-driven-approach-cti

[21] https://connect.comptia.org/blog/cyber-security-stats-facts

[22] Recorded Future

[23] https://www.techtarget.com/searchsecurity/feature/Security-posture-management-a-huge-challenge-for-IT-pros

[24] https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf

[25] https://ponemonsullivanreport.com/2022/11/if-time-is-money-vulnerability-backlog-is-really-expensive/

[26] https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf

[27] https://cybersecurityventures.com/ransomware-will-strike-every-2-seconds-by-2031/clid=Cj0KCQjwqP2pBhDMARIsAJQ0CzqoPoV7a2rv87tyeQUaOtatmfCAOKU5zJo6YHhYCWy3n4mWzGu23rsaApNiEALw_wcB&gclsrc=aw

Recorded Future®

About Recorded Future

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com