REPORT

The 2023 Global Ransomware Report

Executive Summary

While 78% of organizations believe they are "very" or "extremely" prepared to mitigate an attack, 50% still fell victim to ransomware last year.

Fortinet recently surveyed 569 cybersecurity leaders and decision-makers from organizations of all sizes and industries around the globe to understand their perspectives on ransomware, how it has impacted their organizations, and what strategies they have in place to mitigate a potential attack. In this year's survey, more than 80% of respondents say they are "very" or "extremely" concerned about the threat of ransomware, yet a similar number (78%) of organizations surveyed also believe they are "very" or "extremely" prepared to thwart a breach. Despite those concerns and feelings of preparedness, half of the organizations surveyed still fell victim to ransomware last year.

Of the organizations that experienced a ransomware incident, 71% said they paid at least a portion of the demanded ransom, even though 72% indicated they detected the incident within hours (often within minutes). And while nearly all respondents had cyber insurance, this didn't guarantee that all costs would be covered, or data restored. In fact, only 35% of those affected by ransomware recovered all their data after the incident.

It's not all bad news, though. In fact, despite economic uncertainty, nearly all leaders surveyed (91%) expect increased security budgets in the coming year to invest in technologies and services that further safeguard their networks from a potential ransomware attack. In general, security leaders' top priority is to implement advanced technologies such as artificial intelligence (AI) and machine learning (ML) that enable faster threat detection, followed by central monitoring to speed response. And specifically, Internet-of-Things (IoT) security and next-generation firewalls (NGFWs) topped the list of areas and products that leaders planned to invest in, with the greatest increase in plans to implement endpoint detection and response (EDR) and secure email gateway (SEG) solutions. This is a promising plan, as phishing emails were the number one method respondents reported ransomware actors used to gain entry. And of course, the endpoint is the ultimate destination of ransomware.

Interestingly, while many security leaders have traditionally believed that buying the best individual product for a project will yield the strongest cybersecurity posture, this year's survey data indicates that those organizations that reported taking a point product approach were the most likely to become a victim of ransomware. However, technology is only part of the solution. The survey found that four out of the top five challenges in preventing ransomware were related to people and processes.

As ransomware proliferates and attacker methods grow in sophistication, organizations of all shapes and sizes are a target, making it crucial that security leaders invest in the right technologies, people, and processes now to prevent a ransomware incident in the future.

The Growing Sophistication of Ransomware Makes Every Organization a Target

While ransomware has existed for decades, the global threat remains at peak levels. It also continues to become more sophisticated, causing increasing harm to organizations worldwide. According to observations from the FortiGuard Labs Incident Response (IR) team, financially motivated cybercrime accounted for the highest volume of incidents (74%) in 2022, with 82% of financially motivated cybercrimes involving the deployment of ransomware or malicious scripts.[1]

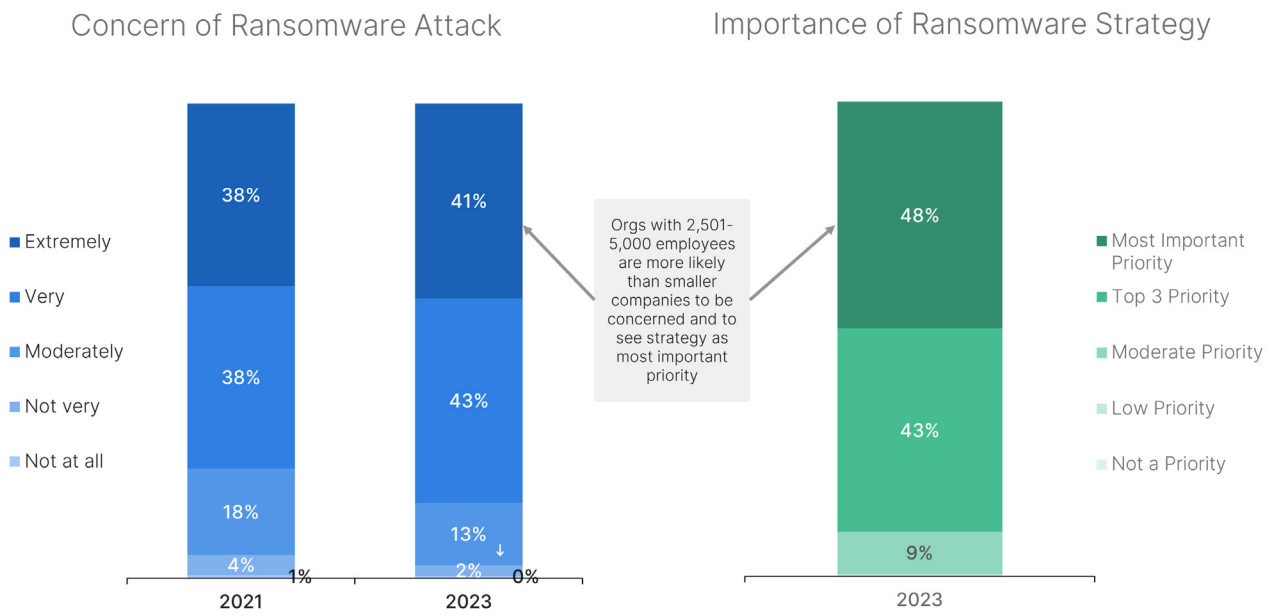
While year-over-year ransomware growth has slowed in 2022—following the explosion of this attack method in 2021—the frequency of it is still increasing. For example, in the first half of 2022, FortiGuard Labs observed the introduction of 10,666 new variants—that's double the number seen in the six months prior.[2] The likely reason for the change is that Ransomware-as-a-Service (RaaS) operations are maturing, enabling cybercriminals to successfully introduce new, more sophisticated, and aggressive variants than ever before. And they are also being more selective, specifically targeting organizations able to provide a large payout. In contrast to the early success of RaaS, which initially relied on volume—more affiliates meant more opportunities to infiltrate networks and launch attacks—RaaS operators are increasingly becoming more selective regarding the associates they allow to join their operations.

This more systematic approach to executing ransomware attacks is yielding greater success. For starters, they're spending more time conducting reconnaissance to identify lucrative targets, meaning that many ransom demands now reach well into the tens of millions of dollars. Additionally, the ransoms these groups are demanding from their targets now tend to be commensurate with the organization's size and industry. Many cybercriminal organizations use a formula to determine what amount to ask for so that a victim is more likely to pay.

This growing maturity of ransomware operations is to be expected, given that RaaS is a significant driver of Crime-as-a-Service (CaaS). Yet, as RaaS operators become more aggressive with their playbooks and incorporate increasingly destructive elements into attacks—such as the growing use of wipers—organizations of all shapes and sizes must implement appropriate security strategies to mitigate potential breaches.

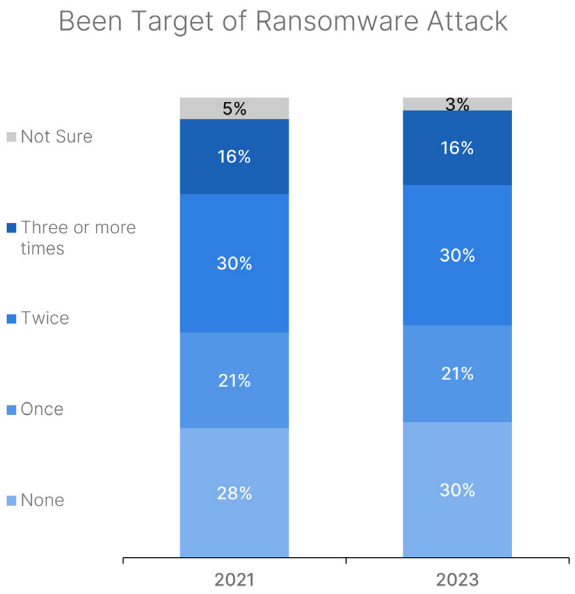
Ransomware Attacks Are Common and Costly

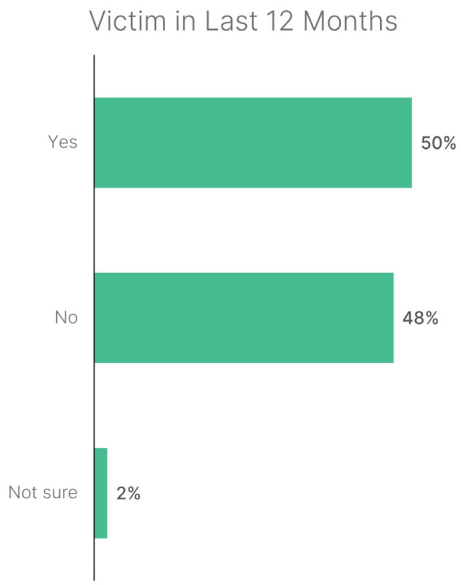
Given the evolution and growing sophistication of ransomware operations, it's not surprising that 84% of organizations represented in this year's survey remain "very" or "extremely" concerned about this threat, which is even higher than the 76% of respondents that expressed the same level of worry when surveyed in 2021. However, despite these concerns, 78% also believe they are "very" or "extremely" prepared to prevent or mitigate a ransomware attack (up significantly from the 63% who felt that way in the prior survey). In fact, more than 90% of those surveyed said that having a ransomware strategy in place is either their team's most important or one of their top three priorities. And 88% include cyber insurance as part of their preparedness strategy.



Unfortunately, the reality is that a disconnect remains between respondents' perceptions of their organization's preparedness and their ability to prevent a ransomware incident. Of those surveyed this year, half of enterprises fell victim to a ransomware attack in the last 12 months, and 46% were targeted by ransomware two or more times.

Of those organizations surveyed that fell victim to a ransomware attack in 2022, phishing—targeting an individual or group through malicious emails—remained the top tactic (56%) yet again. This was followed by access via vulnerable ports (54%) and remote desktop protocol exploits (51%) taking the second and third spots on the list. With multiple methods reported by more than 50% of respondents, it seems ransomware operators either seek multiple ways in as part of the same or subsequent attacks.





Most respondents whose enterprises experienced a ransomware attack have a policy that dictates they pay the ransom requested. Of note, despite most (72%) detecting the incident within hours, sometimes minutes, more than 70% said they paid at least a portion of the ransom that attackers demanded, despite guidance from the FBI that paying ransom only fuels the problem and doesn't guarantee that organizations will recover their data.[3]

Interestingly, organizations in certain industries were more likely to pay the ransom than others. For example, organizations in the manufacturing sector paid the requested ransom more often than those in other industries. And the amount requested was also typically higher—in fact, in 25% of breaches among manufacturing companies, the demanded ransom was $1M or higher. The industry's willingness to pay is understandable given that their cost of downtime is so high. And adversaries demand more from these enterprises because they know the companies can pay.

That said, neither paying the ransom nor hoping cyber insurance will cover losses is an effective strategy for mitigating an attack. In fact, 65% of respondents were not able to recover all their data post-attack. Further, almost half (41%) of organizations with cyber insurance didn't receive as much coverage as expected and, in some cases, didn't receive any because of an exception from the insurer.

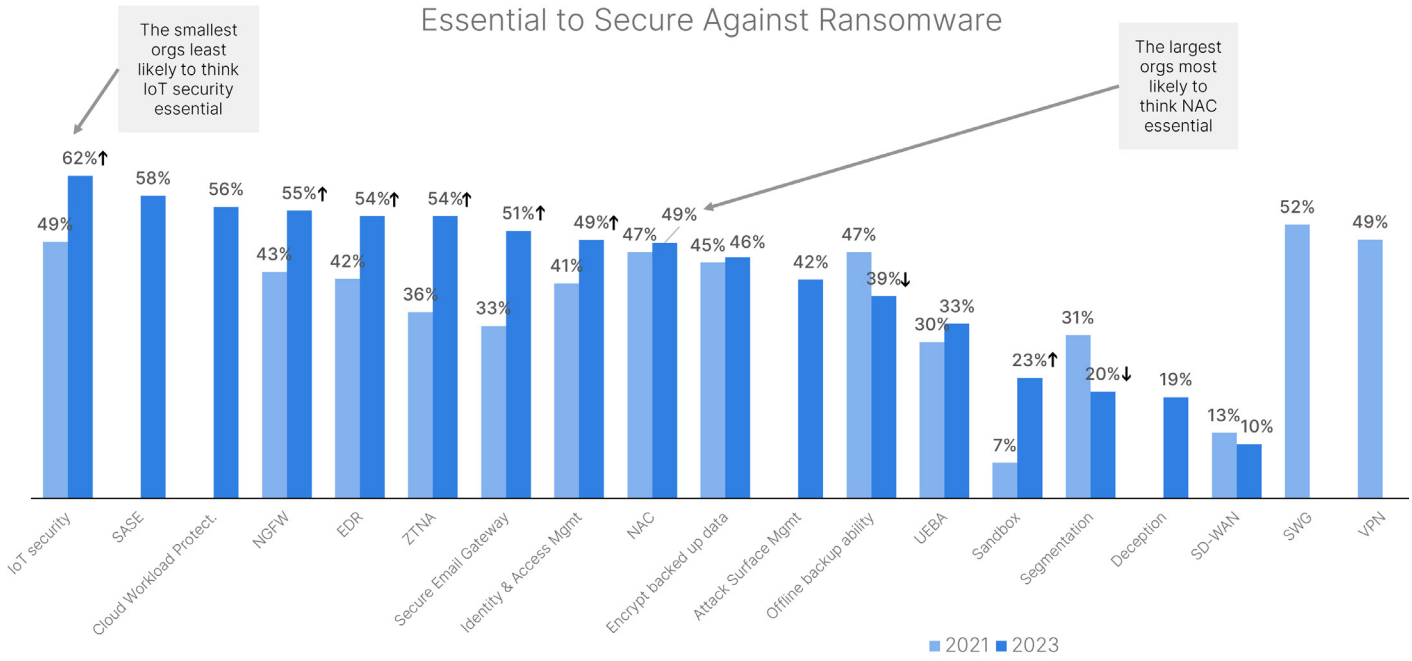
Organizations Are Actively Working to Guard Against Ransomware, Yet Many Aren't Prioritizing Essential Protections

For the second time in a row, respondents said their top challenge in preventing attacks was the growing sophistication of the threat landscape; something outside of their control. However, the next four challenges—a lack of clarity on properly securing their networks against a ransomware attack, a lack of cybersecurity awareness among end-users, no clear chain of command, and difficulty stopping employees from being fooled by social engineering—were related to people and processes, which seems to contradict their sense of being prepared for a ransomware attack. On the bright side, it's encouraging to see that some worries that topped the list in 2021—such as the complexities of securing an increasingly remote workforce—were less concerning to respondents this year.

It's also promising that despite the general economic environment, 91% of organizations expect their security budgets to increase—and of that group, many (42%) expect their budgets to increase by more than 10%—in the coming year, allowing them to make investments to address these ransomware challenges. To safeguard their respective enterprises, security teams also said they are investing in additional cybersecurity technology, reporting attacks more frequently to law enforcement, and leveraging their cyber insurance when needed.

No single investment stood out as the perceived answer to mitigating ransomware, which is a good sign. Instead, a range of solutions was cited as essential to secure against ransomware attacks. Half or more of those surveyed cited each of the following security technologies as crucial to their strategies: IoT security, SASE, cloud workload protection, NGFWs, EDR, zero-trust network access (ZTNA), and SEG. Compared to the 2021 survey, the number of respondents citing both ZTNA and SEG technologies as critical tools jumped by nearly 20%. This change in perception is good news, given that phishing remains the most common attack vector for gaining access to an organization's network and putting granular controls in place to govern application and data use is an important best practice.

However, while it's great to see enterprises embracing these security technologies, it's also interesting that they aren't recognizing other essential protections, such as sandboxing, network segmentation, and storing data off-site, which are table stakes in defending against ransomware.



Beyond what's viewed as important, we also asked what organizations plan to invest in next. As teams evaluate new tools to protect against ransomware, understanding the enterprise's current security posture and identifying gaps is a crucial first step before making additional investments. Organizations can do this by mapping current defenses to the attack chain using tools like the MITRE ATT&CK framework. Such an approach will help teams understand if they've taken the most effective steps to defend against ransomware and what potential security gaps they need to address.

The top three investments respondents planned to make were in IoT security (57%), NGFWs (53%), and EDR (51%). One of the most surprising findings from Fortinet's previous survey was that the top method of entry in 2021 was email phishing, yet only a third of organizations reported plans to improve that defense. Email phishing remained the number one method of entry for the second time in 2022, something that will hopefully decline if organizations now follow through on plans (47% of respondents in 2022, up from 31% in 2021) to invest in this area.

The Need for Consolidation and Integration

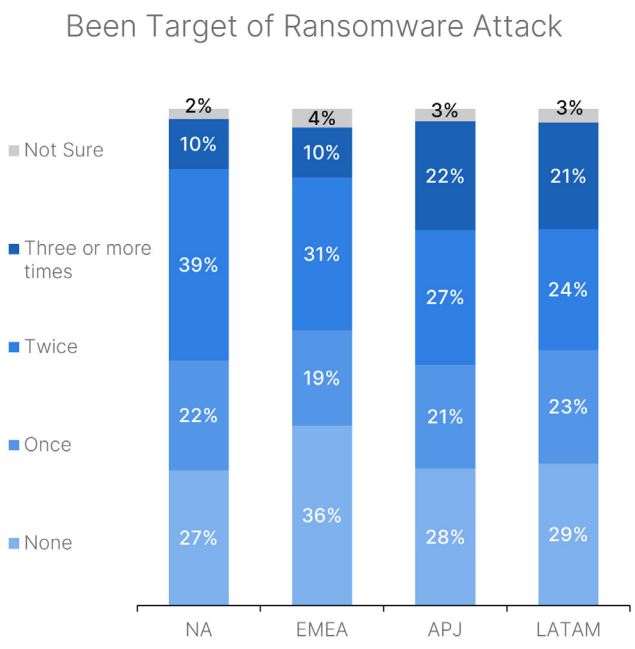
But while it's encouraging to see enterprises investing in additional technologies to guard against ransomware, the reality is that simply adding tools to an already overloaded toolbox often isn't enough to lower an organization's risk of being attacked. An increasing number of respondents (45%) say they're using a mix of security platforms and point products, but 36% continue to buy only "best-of-breed" point products. As a result, many security teams end up spending a great deal of time managing individual products deployed over time and struggling to get their collection of technology to operate together effectively. And such manual processes can hinder a security team's ability to gather the right data and promptly respond to a ransomware incident.

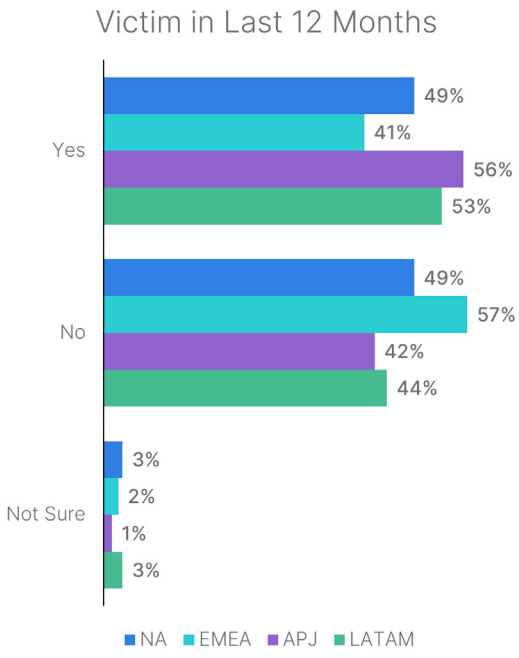
Interestingly, those that reported taking a best-of-breed approach were most likely (67%) to fall victim to a ransomware attack, while those who had reduced their vendor overhead by consolidating to a small number of platforms complemented by point products were the least likely (37%) to be impacted. We see more and more organizations consolidating the number of point products they use and instead leveraging a smaller number of strategic platforms. Our survey results reinforced this, with 99% of respondents viewing integrated solutions or a platform as essential to preventing ransomware attacks. And again, it's not just about technology, but also the people and processes to use these platforms to their best effect.

A Look at Ransomware Attacks and Organizational Preparedness Around the World

Organizations' perspectives on ransomware and their respective levels of concern, preparedness, and top challenges have largely normalized across all regions, with nearly all respondents around the globe indicating that having a ransomware strategy was either the most important priority or one of their top priorities. Similarly, regions consistently implement many early detection and response tools, most purchase best-of-breed products, and nearly all have cyber insurance.

However, we did see a variation in the percentage of enterprises across regions that experienced a ransomware attack in the last 12 months, with Asia Pacific/Japan (APJ) experiencing the most ransomware incidents (56%) and Europe, the Middle East and Africa (EMEA) experiencing the least (41%).





Not only that, but there are differences in their response efforts, like the speed of detecting attacks and whether organizations feel compelled to pay the requested ransom. For example, Latin America (LATAM) tended to detect attacks more quickly and was less prone to social engineering tactics than other regions. Regarding the implementation of security tools, respondents from North America (NA) and EMEA plan to invest more heavily in ZTNA than APJ and LATAM. As for ransom demands, respondents in EMEA saw smaller ransom amounts than other regions, and nearly half of the respondents didn't pay the requested ransom. Organizations in APJ saw higher ransom demands, and 44% said they paid the total amount.

Looking Ahead: Enhancing Security Strategies

Finally, we asked respondents about the general types of security technologies they plan to invest in moving forward to guard against ransomware. Of note, the number one area, reported by 50% of respondents, said that adopting advanced technologies powered by AI and ML ranked among their top three priorities. Security leaders are also prioritizing centralized monitoring tools like security information and event management (SIEM) and security orchestration, automation, and response (SOAR) to speed detection and response efforts. Respondents also ranked the following attributes as "extremely important" as they evaluate new technologies: solutions that include actionable threat intelligence (50%), have AI-driven behavioral detection capabilities (48%), and are designed to work together (45%).

This gives us reason for optimism, as organizations are recognizing that even with seasoned security professionals on staff, additional measures are needed to thwart mature cybercrime ecosystems on their own. Deploying more early detection technologies along the cyber kill chain of attacks is critical to halt ransomware attempts.

Organizations that reported taking a best-of-breed point product approach to security were the most likely (67%) to fall victim to ransomware, while those that consolidated technologies to take a platform-driven approach were least likely (37%) to be breached.

However, keep in mind that "more" doesn't always mean "better" when it comes to security technology. Teams typically spend an excessive amount of time tuning and stitching together disparate point products, which often places unnecessary strain on the analysts tasked with safeguarding the enterprise. By pursuing a security mesh architecture approach—a collaborative ecosystem of security technology designed to work together, such as the Fortinet Security Fabric—security teams can reduce complexities, enhance detection efforts, and reduce the burden on security operations center (SOC) professionals. Embracing services like managed detection and response (MDR) and SOC-as-a-service (SOCaaS) can also help security teams that are stretched thin take full advantage of the advanced technologies they've implemented.

Beyond procuring technology, preparing your people and creating effective processes is crucial. You can do this yourself or take advantage of incident readiness and response services to help generate new or test existing plans and identify any areas for enhancement through activities such as conducting a gap analysis, running tabletop exercises, and developing playbooks and IR plans.

While you and your analysts are ultimately responsible for securing your organization, remember that all employees have a role to play in fending off attackers. An enterprise's employees are often the first line of defense when preventing an attack, making ongoing cybersecurity awareness education and training programs a critical part of your risk management strategy.

Ransomware isn't slowing anytime soon. However, security leaders can take numerous actions to better protect their organization's data and networks. They just need to ensure those measures align with the risks and strategies of a ransomware attack. Taking a consolidated platform approach to safeguard your enterprise, incorporating AI-driven tools and automation, testing (and retesting) plans and processes, proactively monitoring external vulnerabilities, and educating your broader employee base on how to spot a potential cyberattack are all essential steps to take today to decrease the chances you'll fall victim to a ransomware attack tomorrow.

[1] "FortiGuard Labs Reports Destructive Wiper Malware Increases Over 50%," Fortinet, February 22, 2023.

[2] "1H 2022 FortiGuard Labs Global Threat Landscape Report," Fortinet, August 17, 2022.

[3] "How We Can Help You: Common Scams and Crimes," FBI.gov.

April 20, 2023 2:41 PM

2051666-0-0-EN