REPORT

The 2021 Ransomware Survey Report

TABLE OF CONTENTS

Executive Overview

Fortinet recently surveyed 455 business leaders and cybersecurity professionals worldwide to gauge their state of readiness to defend against the growing challenge of ransomware. Most are very or extremely concerned about the threat of a ransomware attack, with many seeing those attacks as a more significant challenge than other cyber threats. The majority feel prepared and report having a strategy that includes employee cyber training, risk assessment plans, offline backups, and cybersecurity/ransomware insurance. But despite these plans, two-thirds also claim to have been the victim of at least one ransomware attack.

The majority of respondents feel prepared and report having a strategy that includes employee cyber training, risk assessment plans, offline backups, and cybersecurity/ransomware insurance. But despite these plans, two-thirds also claim to have been the victim of at least one ransomware attack.

As we dig deeper, this high incidence of ransomware is perhaps not so surprising as there seems to be a gap between the strategies and tools many respondents see as necessary to protect against the threat of ransomware and what's needed to guard against the most commonly reported methods used to gain entry to their organizations. Common investment plans include Secure Web Gateways and IoT security, which most reported as essential for securing themselves against ransomware. But a Secure Email Gateway, for example, was at the bottom of their list—and at the same time, they indicated that phishing employees via email is the most common vector for gaining access. Similarly, tools like sandboxes and segmentation are also at the bottom of the list, even though ransomware attacks generally include malware variants that a sandbox is best equipped to detect, and lateral movement is an essential tactic after a remote endpoint device has been compromised.

It is perhaps no surprise then that most believe that a ransomware attack is inevitable. Most even have a ransom payment policy in place that includes paying a ransom—even though though the FBI has reminded organizations that paying a ransom doesn't guarantee that an organization will get any data back.[1] Or that paying a ransom "encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."

The State of Ransomware

The prevalence of ransomware continues to grow, reaching new highs. According to the 2021 1H Global Threat Landscape Report from FortiGuard Labs, ransomware grew 1,070% between July 2020 and June of 2021.[2] While numerous high-profile incidents have grabbed international headlines, the real impact is felt by tens of thousands of organizations, from enterprises to small businesses and from federal agencies to local governments.

Two things are fueling the staggering growth of ransomware. First, tools like Ransomware-as-a-Service and selling the names of companies that have already been compromised have commoditized the process. Novice criminals, acting as a sort of franchisee for a cyber-criminal organization, can now successfully target organizations with little or no technical skills. All the back-end processes, from target acquisition to pricing to collecting funds, are offered as a service—for a fee—by sophisticated criminal enterprises that even provide help desk services for their customers. The second is that the enormous paydays that ransomware delivers have been broadly discussed in the news and online forums and have triggered nothing short of a feeding frenzy.

Fortunately, organizations around the world have begun to organize. The White House has formed a cross-government task force to develop and coordinate defensive and offensive measures against ransomware in the U.S. Solutions being discussed range from revising cybersecurity regulations to updating the security infrastructure to offering rewards for identifying threat actors. The World Economic Forum's Center for Cybersecurity and Interpol are likewise engaged, holding international conferences and outlining strategies for combating this scourge. But for now, this is a pressing problem that every organization should be prepared to address.

Ransomware Survey Overview

Fortinet recently surveyed 455 business leaders worldwide, mostly cybersecurity professionals, to learn how ransomware has impacted them, as well as what strategies they have in place and how they intend to combat it. The survey is designed to better understand the following:

- How concerned are security leaders about the threat of ransomware attacks?
- How did the pivot to remote work and learning from home affect their cybersecurity posture?
- How confident are they in their existing countermeasures, and what else do they plan to deploy?

Top Ransomware Concerns

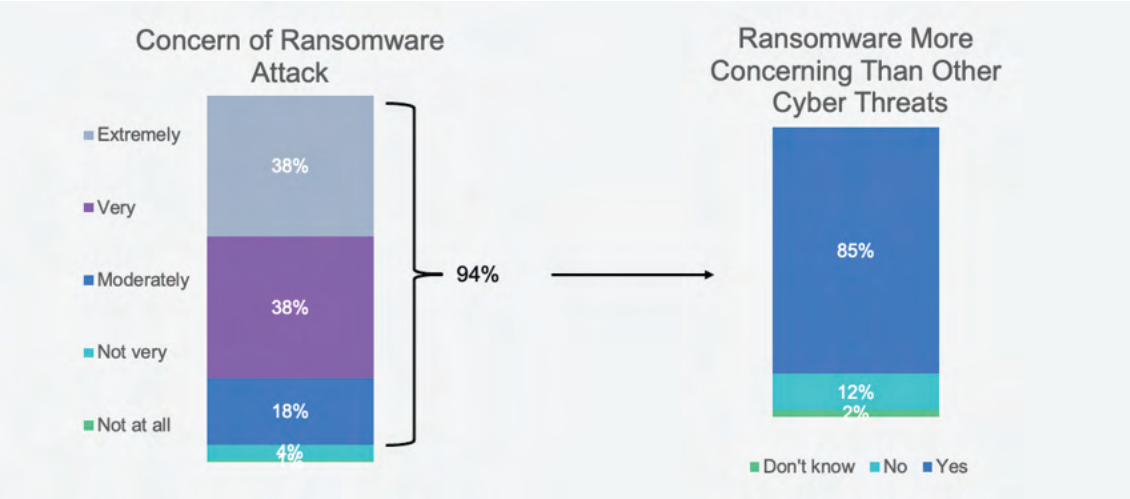

Figure 1: Q. How concerned are you about the threat of a ransomware attack on your organization? Base: Total Completes n=455 Q. Is the risk of a ransomware attack more of a concern than other perceived cyber threats you face? Base: Moderately, Very, or Extremely Concerned n=428

94% of those surveyed indicated that they are concerned about the threat of a ransomware attack, with 76% being very or extremely concerned. Of those, 85% are more worried about a ransomware attack than any other cyber threats.

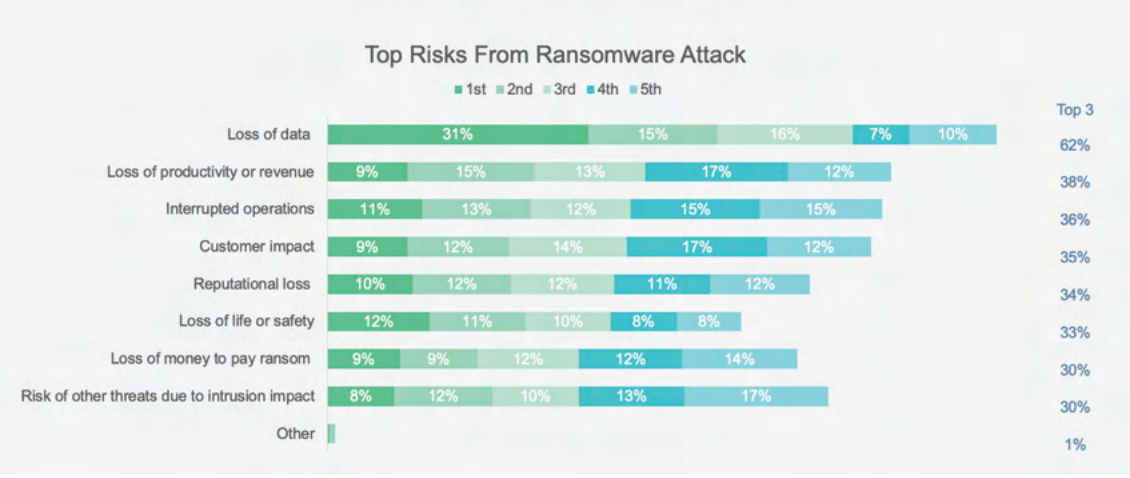

Figure 2: Q. Please rank the top 5 risks to your organization from a potential ransomware attack, where 1 is the most significant risk. Base: Total Completes n=455

It probably comes as no surprise that the top concern of organizations concerning ransomware (62%) is the risk of losing data. Today's businesses run on data, so while loss of productivity (38%) and the interruption of operations (36%) are still top concerns, they can be recovered from much more quickly than a significant loss of data.

Ransomware developers are continually adding advanced features and functions designed to thwart existing security systems and evade detection. That's why 36% of respondents identify the growing sophistication of the threat landscape as being among their top five challenges in preventing ransomware. Following closely is a lack of user awareness and training about cybersecurity hygiene (32%) and the difficulties of securing "work from anywhere" employees (31%). And taking the fourth and fifth place slots are "lack of actionable threat intelligence" (29%) and "no clear chain-of-command strategy to deal with attacks" (27%).

Interestingly, 27% of respondents report that a "lack of visibility across the distributed network" is a top five challenge. This is often due to deploying point solutions in different parts of the network that were not designed to interoperate, as well as issues arising from the lack of visibility into the home networks of remote workers. Vendor and solution sprawl, usually the result of an ad hoc approach to securing new network edges and technologies, can undermine visibility and control. This is especially critical for ransomware attacks that seek to move laterally across the network, looking for data to harvest and encrypt. Fractured visibility makes it easier for IT teams to miss an attack or fail to recognize a threat approaching from another segment of the network.

Preparedness

Despite 67% of organizations reporting that they have been a ransomware target (16% say they were attacked three or more times), 96% feel they are at least moderately prepared. That said, less than half of respondents have a strategy that includes such things as network segmentation (48%), business continuity measures (41%), a remediation plan (39%), testing of ransomware recovery methods (28%), or red team/blue team exercises (13%) to identify weaknesses in security systems.

And while 84% also report having an incident response plan in place, what comprises that incident response plan is important to unpack.

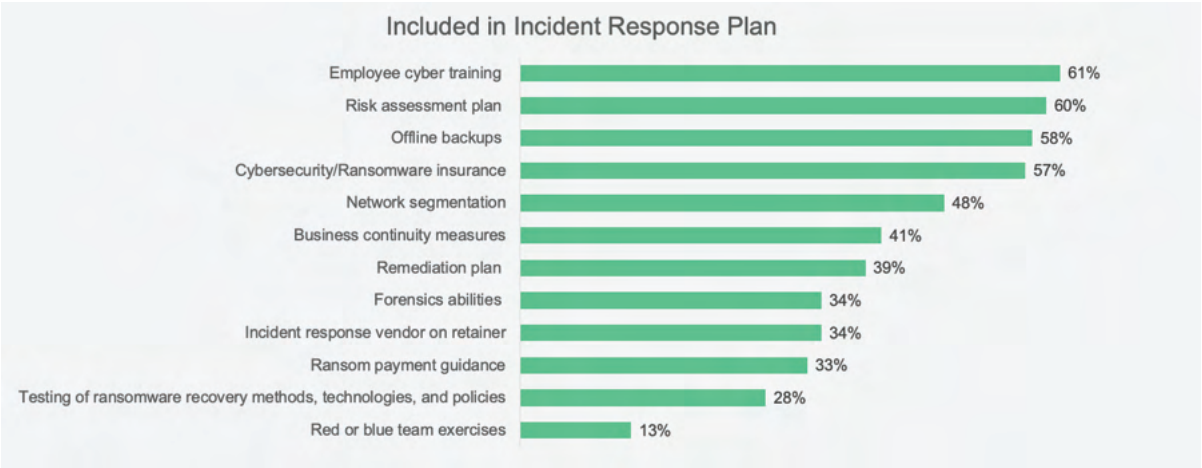

Figure 3: Q. Which of the following are part of that plan? Base: Have incident response plan n=378

A common element is employee cyber training (61%). The message that end-users are the primary target of ransomware attacks, and are therefore the first line of defense against phishing attacks, has clearly gotten through. Risk assessment plans (60%), offline backups (58%), and cybersecurity/ransomware insurance (57%) round out the elements included in the majority of incident response plans.

Of those without an incident response plan, the number one reason cited (54%) was a lack of skilled internal resources for developing a plan.

Paying a ransom is a hot-button issue for many organizations, especially among cybersecurity professionals and law enforcement. 72% of respondents claim they have a ransom policy in place. Interestingly, the procedure for 49% of them was to pay the ransom outright, and for another 25%, it depends on how expensive the ransom is. This is why more sophisticated cyber criminals conduct a financial survey of potential victims along with their search for exploitable vulnerabilities.[3] Rather than impose a random fee, experts on the dark web help attackers set a ransom fee based on an organization's ability to pay. Others specialize in negotiating a price for those who resist paying.

Protection and Defensive Measures

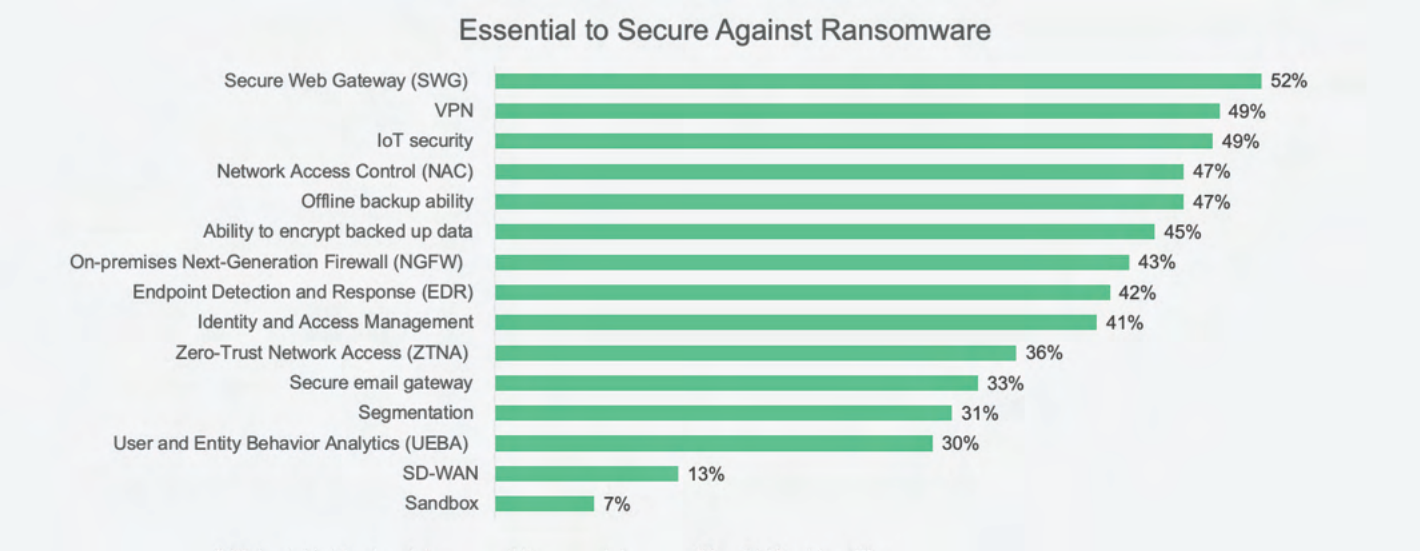

Figure 4: Q. What products/solutions do you believe are essential to secure against ransomware? Base: Total Completes n=455

In addition to readiness, a broad spectrum of protection tools was selected as being essential to combat ransomware. Respondents could choose as many as they thought were essential. And while there was no clear winner (with many clustered within 10% of each other), their choices indicate that their top concern was remote workers and devices. Secure Web Gateway (52%), VPN (49%), and Network Access Control (47%) are three of the top five choices. Offline backup (47%) and encrypting backed-up data (45%) are also top selections.

What's more interesting are the technologies at the bottom of the list. Zero-Trust Network Access (ZTNA) is a relative newcomer, so it only being selected by 36% of respondents may be understandable. But any strategy involving secure remote access should be seriously considering ZTNA as a replacement for aging VPN technology. However, the relatively low placement of segmentation (31%) is a surprise, as a critical characteristic of nearly all ransomware attacks is to move laterally across the network, looking for additional data to encrypt. Likewise, UEBA and sandboxing play a crucial role in identifying intruders, compromised systems, and new ransomware variants but were also relatively low on the list of tools deemed essential (30% and 7%, respectively).

The most surprising finding was how few respondents selected Secure Email Gateway (33%), given that they also reported phishing as the most common method (55%) used to gain access to their organizations. Arguably, the first line of defense, even before a trained end-user, is a modern secure email gateway capable of detecting and disabling malicious attachments and links before they ever reach the user's inbox.

SD-WAN is interesting for a different reason. Traditional WAN connections are rapidly being replaced with SD-WAN because it is inherently smarter and more agile. But not necessarily more secure, which is why every organization with an SD-WAN strategy needs to be considering a secure SD-WAN solution (SD-WAN built on a security-based platform, like an NGFW) as their primary approach for upgrading legacy remote connectivity to cloud and data center resources by branch offices and certain superusers.

Plans for investing in security technologies map closely to those identified as essential, with no technology being selected by more than half of respondents. However, 91% plan to invest in more employee cyber awareness training, which is an excellent first line of defense.

The Need for Integration and Intelligence

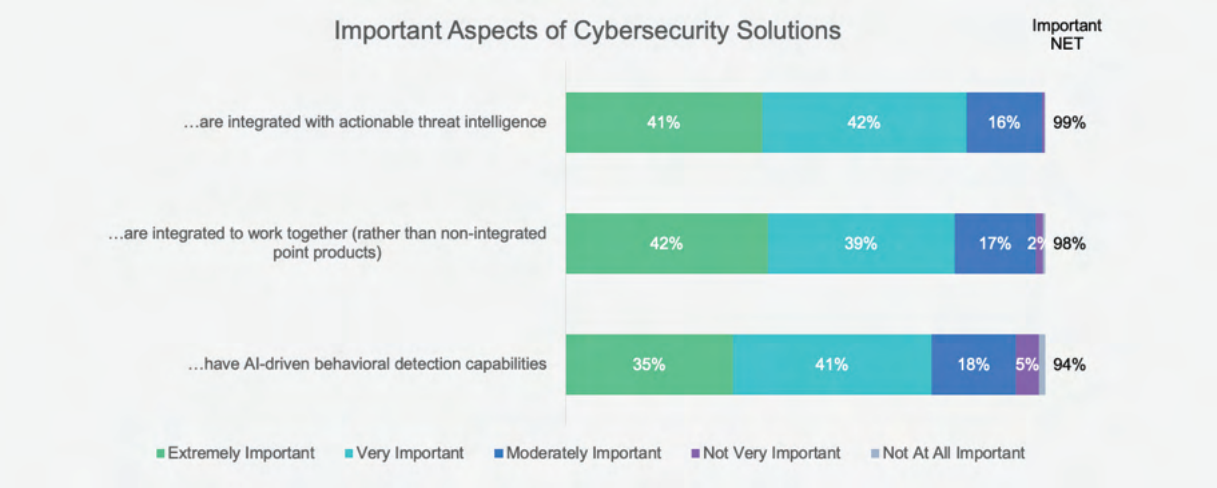

Figure 5: Q. How important is it that a ransomware strategy consists of cybersecurity solutions that... Base: Total Completes n=455

One critical question asked of respondents was how important it was for cybersecurity solutions to provide the required set of functions individually and whether they needed to work together in an integrated fashion. And 83% of respondents said that being combined with actionable threat intelligence is a very or extremely important criterion for selecting cybersecurity solutions. Similarly, they identified tools integrated to work together (rather than non-integrated point products) to be nearly as crucial, at 98%. And 94% want solutions embedded with artificial intelligence (AI)-driven behavioral detection capabilities.

Regional Variations

While concerns about ransomware were reasonably consistent across the board, respondents in EMEA (95%), Latin America (98%), and APJ (Asia-Pacific/Japan) (98%) were slightly more concerned about ransomware attacks than their peers in North America (92%). But despite these differences, all regions except for APJ perceive the loss of data as the top risk associated with a ransomware attack, along with the worry that they will be unable to keep up with an increasingly sophisticated threat landscape. APJ, uniquely, lists the lack of user awareness and training as their top concern.

Interestingly, respondents in APJ and Latin America were far more likely to have been victims of a ransomware attack in the past (78% compared to 59% in North America and 58% in Latin America). And concerning the types of attacks they experienced, organizations in APJ (65%) and Latin America (67%) are more likely to be the victims of a targeted attack. In comparison, North America (58%) is more likely to be part of a broader campaign. Ransomware attacks in EMEA are pretty evenly split between the two.

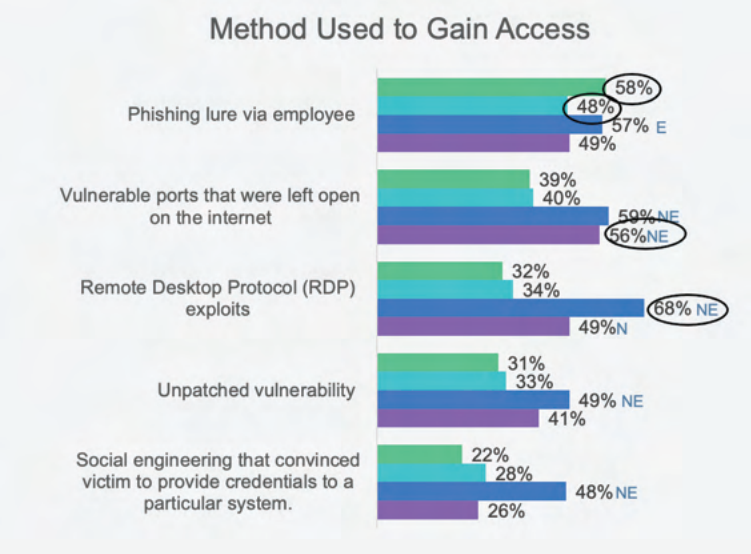

Figure 6: Q. What was the method to gain access to your network to launch the ransomware for this attack?
Base: Been target of attack NA=88; EMEA=58; APJ=118; LatAm=39

Attack techniques also vary between regions. For those respondents that said they had been a victim of a ransomware attack, phishing lures were the primary attack vector for North America (58%). APJ was primarily targeted using Remote Desktop Protocol (RDP) exploits (68%) and vulnerable, open ports (59%). The top attack vector for Latin America was open vulnerable ports (56%), but other attack strategies were consistent across the rest of the methods. And for EMEA, as with the type of attack being used, no one exploit method was dominant.

Conclusion

Many of the key takeaways from this report should come as no surprise. Ransomware is ubiquitous, everyone is a target, and it is driving investments in strategies, training, and technologies because no one expects it to go away anytime soon. But the most interesting data comes from the seeming disconnect between the concerns and experiences of organizations compared to the defensive technologies and strategies they have identified as their top priorities. More needs to be done to educate organizations about the critical value of advanced email security, segmentation, sandboxing, and similar tools and strategies to detect, prevent, and limit ransomware.

Not only that, but most organizations recognize that today's security tools need to provide core capabilities and be fully integrated with actionable threat intelligence. They must also be designed to interoperate as a unified system and be enhanced with AI and machine learning to better detect and respond to ransomware threats.

[1] FBI article on ransomware

[2] "2021 Global Threat Landscape Report," Fortinet, August 2021.

[3] Val Saengphaibul, "The Affiliate's Cookbook - A Firsthand Peek into the Operations and Tradecraft of Conti," FortiGuard Labs, August 10, 2021.

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

September 29, 2021 8:29 AM

1290667-0-0-EN