White Paper: **September 2022**

IT and Security Leaders Turn to Lateral Security to Mitigate Ransomware

vmware®

Introduction

As ransomware gangs continue to refine and intensify their attacks, IT and security leaders must find a way to stay ahead of adversaries. The rising number of successful attacks proves that security at the endpoint and the perimeter is not enough to protect the enterprise.

Instead, organizations need a lateral security approach made up of systematic, omnipresent tools deployed between the perimeter and endpoints. This combination of tools—including network segmentation, micro-segmentation, and advanced threat prevention capabilities such as intrusion detection/prevention systems (IDS/IPS), network sandboxes, network traffic analysis/network detection and response (NTA/NDR), and others—is the only way to effectively detect, prevent, and remediate ransomware and other advanced threats.

Results of two eye-opening surveys from VMware show that ransomware remains a top concern for enterprises worldwide. Additionally, IT and security leaders and chief information security officers (CISOs) believe that deeper deployment and investment in lateral security tools is the answer to protecting their companies from successful attacks.

The Growing Threat of Ransomware Attacks

Ransomware is a pervasive, constantly evolving form of malware that encrypts files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption, knowing that most organizations cannot function without access to their systems and data. They may also resort to extortion—threatening to release sensitive information publicly if the victim organization does not comply. A successful attack's economic, operational, and reputational impact can be devastating for companies, especially given the extensive containment and recovery actions necessary to restore systems and data.

The number of ransomware attacks continues to grow unabated, with a 13% increase from 2020 to 2021—a larger increase than the previous five years combined.[1] This trend was echoed in a 2022 VMware survey of 200 IT and security leaders who manage networking or security in enterprise organizations in North America, Europe, the Middle East, and Africa. Approximately one-third of the survey respondents work for a company with 1,001 to 5,000 employees, one-third represent companies with 5,001 to 10,000 employees, and one-third represent companies with more than 10,000 employees.

More than two-thirds (68%) of the respondents report that their organization has experienced at least one ransomware incident (whether successful or not) in the previous 24 months, see Figure 1. Of those reporting attacks, 42% say they suffered at least three incidents (whether successful or not). In addition to attacks on their own organizations, 55% of respondents are aware of three to six peer organizations that have suffered at least one ransomware attack in the last 24 months.[2]

1. "2022 Data Breach Investigations Report," Verizon, May 2022
2. "Private Cloud Security in the Face of Ransomware Onslaught," VMware survey, 2022

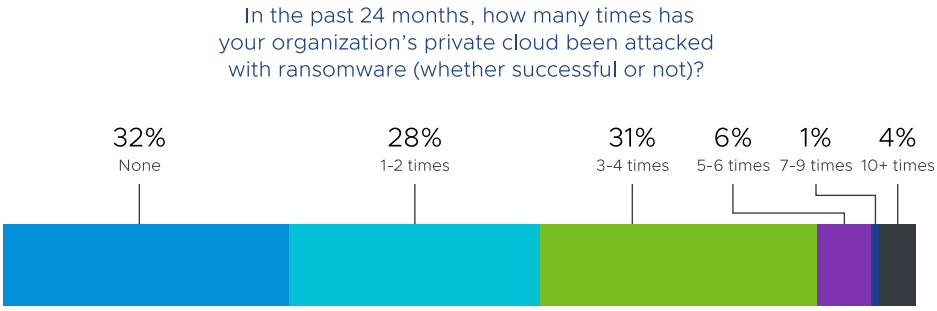

Figure 1: The number of ransomware attacks experienced in the previous 24 months[2]

Because attackers use everything from social engineering to brute-force attacks to gain entry into corporate networks and then move laterally, survey respondents say that network segmentation, micro-segmentation, and IDS/IPS are the top three technologies to protect their organizations from ransomware, see Figure 2.

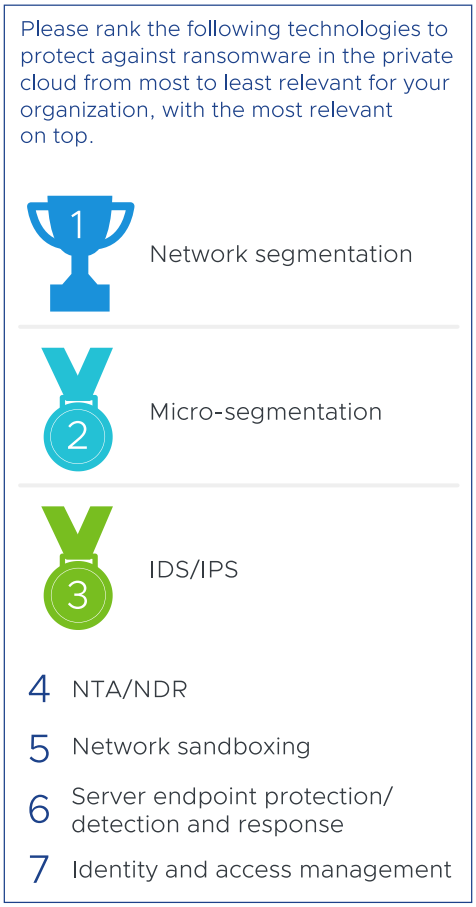

Figure 2: Top technologies to protect against ransomware[2]

The People, Processes, and Technology for Securing the Enterprise

As a follow-up to the first survey that focused on IT and security leaders, VMware decided to explore how security professionals whose organization has experienced a ransomware incident in the last three years responded to the attack and what they changed in the aftermath. The follow-up survey represents 200 respondents from enterprises with more than 1,000 employees, with approximately the same company size representation and geographies as the first survey. Respondents included vice presidents, directors, and managers responsible for information security in their organization.[3]

By focusing the follow-up survey on three core areas—people, process, and technology—involved in securing the enterprise against ransomware attacks, the findings shed light on where security leaders believe they were underprepared for an attack and what steps they planned to take to address their gaps.

3. "Ransomware Incident Response," VMware survey, 2022

Companies think that security team staffing is adequate

Having the right staffing for the security team is a key component of effective threat detection and response. In the survey, just over two-thirds (68%) of respondents said they felt their security team was adequately staffed at the time of the event. Overall, 39% of respondents reported the size of their security team did not change within six months as a direct result of the attack. These results imply that staffing-level was unrelated to the likelihood of a successful ransomware attack in most organizations.

Incident response plans are in place and effective

The majority of respondents (70%) say they had a ransomware incident response plan in place before their most recent ransomware incident, and of those who had one, 87% report that the plan was followed. Not only was the plan followed, but 81% of those organizations utilizing an incident response plan say the plan was adequate or mostly adequate for handling the ransomware incident. Overall, security leaders did not seem to believe that process and planning were lacking in response to successful incidents.

Gaps exist in the deployment of important security technologies

While most respondents report their organizations had identity and access management and server endpoint protection/detection and response technologies in place before the ransomware incident, fewer had segmentation and advanced threat prevention tools deployed. For example, only 58% had network segmentation implemented before the attack, less than half (48%) used micro-segmentation, and only one-third (35%) took advantage of network sandboxing. IDS/IPS and NTA/NDR were the least deployed at 25% and 15%, respectively.

We interpret the findings on segmentation technologies to mean that a significant portion of the networks within respondents' organizations was flat—including the area of the network that was hit by the ransomware. Flat networks provide no barrier against attackers that first compromise a lightly defended low-value system and then move laterally to infiltrate higher-value systems.

The bottom line is that network segmentation, micro-segmentation, and other essential lateral security tools were not deployed pervasively, leaving gaps in protection that attackers could exploit. It's no surprise then that those organizations report an increase in interest in these types of tools after the ransomware incident. Lateral security tools getting increased investment after a ransomware incident include micro-segmentation (46% of organizations), network sandboxing (41% of organizations), network segmentation (39% of organizations), and NTA/NDR (29% of organizations), see Figure 3.

Interestingly enough, IDS/IPS was the more popular choice for investment among the IT professional respondents in the first survey (relative to other technologies) than the security professionals in the second survey. This is even though only 25% of the respondents had IDS/IPS capabilities in place at the time of a successful ransomware attack. Perhaps staffing and/or budget constraints

forced respondents' organizations to deprioritize advanced threat prevention tools such as IDS/IPS relative to access control tools such as network segmentation and micro-segmentation.

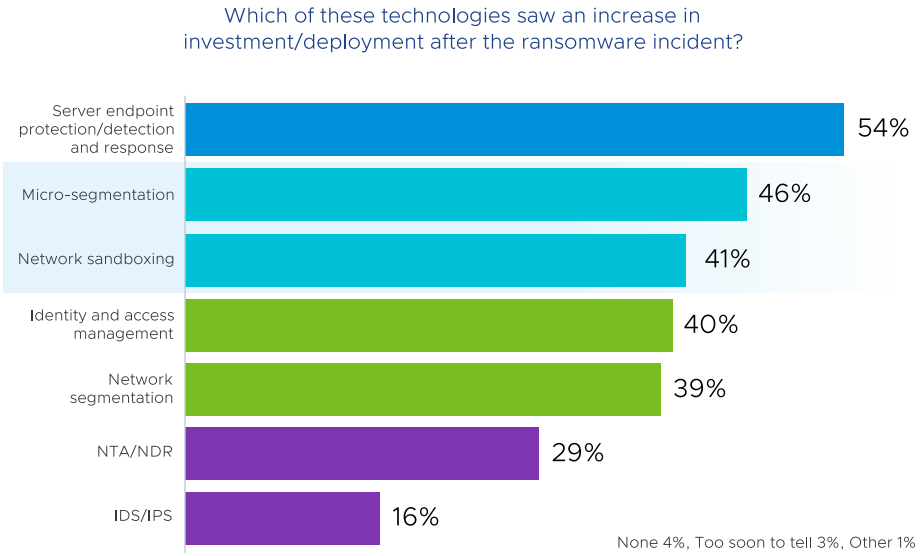

Figure 3: Lateral security technologies that saw an increase in investment/deployment after the ransomware incident[3]

Many organizations in the survey would like to deploy lateral security tools even more deeply, with 40% saying that micro-segmentation should see a further increase in investment/deployment and 36% saying that network segmentation should be increased as well, see Figure 4. To be fair, despite adequate staffing, some organizations may not have enough security professionals with the right skills or tenure to deploy the needed technology as broadly, deeply, and quickly as needed. These security teams may be temporarily hindered in their ability to see faster improvements in protection against successful ransomware attacks.

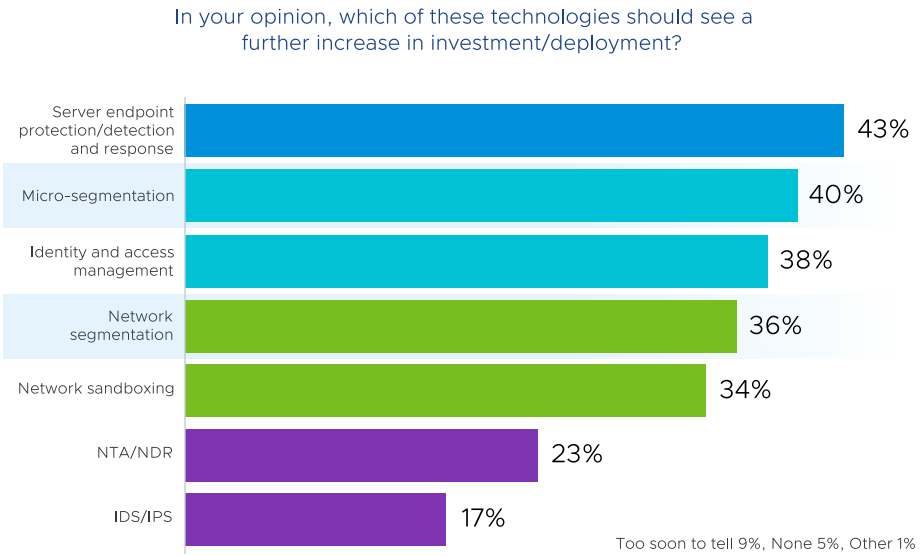

Figure 4: Lateral security technologies that should see an additional increase in investment/deployment[3]

Lateral Security Tools Top the List of CISO Investments

Security teams aren't the only ones that recognize the need for better lateral security in their battle against ransomware. Chief information security officers (CISOs) are also connecting ransomware attacks and lateral security tools' deployment.

A survey sponsored by VMware and other technology companies of 411 CISOs or CISO-equivalents in North America, Europe, and the Asia Pacific regions shows that ransomware once again tops the list of the most worrying cyber threats.[4] This says a great deal about the perception of ransomware risk at the security executive level and the understanding of how a successful attack can cause significant damage.

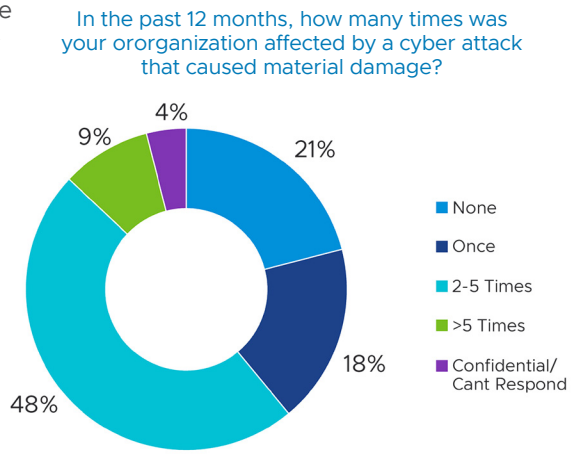

Figure 5: Number of cyber attacks causing material damage[4]

At the same time, CISOs face the constant challenge of trying to keep their organizations safe against all types of advanced threats. The majority (67%) of CISOs in the survey see the threat landscape as worse than the previous year. In fact, 75% confirm being affected by a cyber attack that caused material damage during the previous 12 months at least once and as many as five times, see Figure 5.

In response, the CISOs in the survey plan to deepen investment in lateral security tools, with the top technology for investment (either planning to add or upgrade) being network segmentation and micro-segmentation at 64.8%. At the same time, respondents cited the lack of skilled personnel as the top challenge that inhibits the organization's ability to establish effective cybersecurity defenses, which could impact plans for increasing deployment of lateral security—something these organizations can ill afford.

The Role of Lateral Security Tools

As organizations look to improve their defenses against ransomware attacks, the set of tools that make up a lateral security approach has come into sharper focus. That's because these technologies, when used in concert with each other, can eliminate the blind spots that prevent organizations from detecting threats as they move laterally through the infrastructure.

Lateral security involves a two-pronged approach to preventing successful ransomware attacks: access control and advanced threat prevention. Let's explore how the lateral security tools and capabilities cited by respondents in the surveys fit into these two aspects of securing the enterprise against attack.

4. "The CISOs Report: Perspectives, Challenges and Plans for 2022 and Beyond," AimPoint Group, CISOs CONNECT, and W2Communications, 2022

Further Reading

To learn more about micro-segmentation, read "Internal Firewall: The Best Way to Protect East-West Traffic."

For more information on advanced threat prevention, download "Advanced Threat Prevention with VMware NSX Distributed Firewall."

Access control using network segmentation and micro-segmentation

As the perimeter becomes diffused and, modern workloads become increasingly distributed, internal private cloud traffic (that is, east-west traffic) is left unprotected and vulnerable to lateral movements by bad actors. Network segmentation and micro-segmentation address this by dividing private cloud infrastructure into smaller security zones and inspecting the traffic within those zones. Both methods rely on internal firewalls to establish network segments, control and protect east-west traffic and prevent lateral movement.

Network segmentation splits networks into subnetworks, reducing the attack surface and isolating breaches to prevent them from spreading across the enterprise. The segmentation can be by function; for example, finance and accounting systems can be segmented from human resources applications. Organizations can also segment specific environments such as production and development, partner environments, business units, etc.

Micro-segmentation takes network segmentation further to isolate workloads from each other, securing each individually. A core concept within the zero trust model, micro-segmentation allows fine-grain control of traffic flows between every workload to protect all east-west communication.

Advanced threat prevention

Advanced threat prevention tools use multiple detection technologies (such as IDS/IPS, network sandboxing, and NTA) combined with NDR capabilities to identify and block threats that attempt to blend in with normal east-west traffic.

The IDS/IPS capabilities examine live traffic for known attacks as the traffic passes through the network, the network sandbox detonates suspicious objects (such as files) in a safe environment, and the NTA analyzes traffic to detect anomalies. NDR capabilities then aggregate, correlate, and add context to signals from the detection technologies to reach a verdict (malicious or benign) on network activities. This comprehensive approach is essential to effectively detect, prevent, and remediate advanced threats such as ransomware.

Conclusion

Ransomware is a serious threat to all organizations across all industries. While there will always be constraints such as budget, staffing, and skills that can impact the effectiveness of an organization's security strategy, investing in lateral security tools is the best approach for enterprises to protect themselves against successful ransomware attacks.

VMware provides a full suite of lateral security tools to help organizations achieve strong security against sophisticated threats such as ransomware. Only VMware sees every process running in an endpoint, every packet crossing the network, every access point, and the inner workings of both traditional and modern apps to identify and stop threats others can't.

Item No: IT and Security Leaders Turn to Lateral Security to Mitigate Ransomware_JR2 9/22