FORTINET

Protecting the Endpoint To Work From Anywhere

Table of Contents

Executive Summary

With many of us still working from home and in various other places, the threat landscape continues to evolve and expand with more sophisticated attacks and evasive techniques that are easier to execute when people are not operating within the traditional perimeter. Forrester recently cited that 74% of organizations have indicated that they have suffered a business-impacting cyberattack attributed to remote work vulnerabilities.[1] Ransomware is one of the most chilling forms of cyber crime organizations face today, and it's not going away. FortiGuard Labs reports a sevenfold increase in ransomware activity in December compared to July 2020.[2] A global ransomware survey also showed that 67% of organizations have been a ransomware target—with nearly half saying they had been targeted more than once.[3]

These days, malware can gain access to a system in a number of ways, often with a simple click or even no click at all. After it lands, the attacker tries to spread their malware laterally to gain a foothold in every network they can, even from roaming endpoints. Because attacks are so prevalent, organizations need to be prepared—they need to have strategies in place to address issues before, during, and after an attack, especially in the face of ransomware. Many mature enterprises already have incident response plans built into their security strategies. Organizations can take steps to reduce the risk and scope of potential incidents and secure roaming endpoints, no matter if they are at home or the airport.

A global ransomware survey also showed that 67% of organizations have been a ransomware target—with nearly half saying they had been targeted more than once.[4]

Introduction

As attacks increase, they tend to come through multiple vectors utilizing various techniques, from Trojans to fileless scripts. Workers often fail to recognize phishing attempts, traverse unsafe non-work sites, spend time on social media, and download music and videos throughout the week, whether at home or in the office. These are all opportunities to infect the device even when they are not the intended target of an attack.

Additionally, attackers take the time to do reconnaissance on specific job roles to infiltrate the larger networks (when workers reconnect). Once they get in, they may lurk in the environment for weeks at a time, mapping it out and circumventing security controls. This time gives them the opportunity to drop ransomware payloads and figure out ways to exfiltrate data, and then hold that information hostage as well. The longer attackers lurk, the more damage they can eventually do. Organizations need comprehensive prevention, detection, response, and remediation strategies in place so critical systems can be protected and restored as quickly as possible.

Pre-incident Strategy

Strong endpoint security is a must because endpoints are the ultimate destination for most attacks like ransomware. This process starts with reducing the attack surface of each endpoint by closing off unnecessary ports and peripherals, controlling the communications from vulnerable applications installed on the system, shielding vulnerabilities from exploit, and maintaining this secure configuration.

From there, it is critical to use robust static analysis that combines threat intelligence with machine learning (ML). The analysis should be performed on all code added to the devices and complemented by dynamic behavior-based inspection of all runtime activity to detect threats. It is essential to have the ability to take action in real time and contain attacks in progress without waiting on manual alert triage and response.

As well as endpoint security, organizations often need to make foundational changes to the frequency, location, and security of their data backups. When coupled with digital supply chain compromise and a workforce telecommuting into the network, there is a real risk that attacks can come from anywhere. Cloud-based security solutions, such as secure access service edge (SASE), protect off-network devices, and zero-trust network access (ZTNA) and network segmentation strategies restrict access to applications and resources based on policy and context. Finally, the human element in securing an organization remains as important as technology. It's essential to continually educate employees on new social engineering tactics to know what to look for and how to respond to it.

Ransomware Protection

Over the last half of a decade or more, ransomware has become one of the most popular forms of malware and one of the most advanced and developed. Attackers in 2022 and beyond will continue to look for any way into the organization, and the more connected an endpoint is to multiple networks, the more delectable the target.

In the face of this daily reality, endpoint security needs to monitor the system for malicious encryption continuously and use file access monitoring (FAM) and file integrity monitoring (FIM). The goal for any endpoint security solution should be to prevent as much malware from executing as possible.

URL Filtering

The web continues to be one of the top attack vectors for delivering today's rapidly evolving, sophisticated attacks, including ransomware, phishing, command-and-control (C2) backdoors, and more. Through encryption, many attacks coming from the web will land directly on the endpoint. Additionally, organizations struggle to enforce acceptable use policies and, therefore, often do nothing despite having access to the technology through various security offerings like firewalls and endpoint security.

URL filtering via endpoint security can block access to known malicious sites and C2 servers. This action can stop phishing attacks, credential harvesting, ransomware, and a litany of other forms of malware or beacons being installed on the endpoint to exfiltrate data or establish the device as part of a larger botnet or cryptomining pool (cryptojacking).

Attackers in 2022 and beyond will continue to look for any way into the organization, and the more connected an endpoint is to multiple networks, the more delectable the target.

Continuous Monitoring Strategy

A recent report from Aberdeen has established a baseline of security effectiveness from traditional signature-based endpoint protection at 91.5% (leaving a 7.5% risk of compromise). The report also showed the incremental value of attack surface reduction at 4.7%, bringing effectiveness to 96%. It calculated that behavior-based endpoint security could raise effectiveness to 99.6% (or just 0.4% risk exposure).[5]

For all the prevention measures, organizations with a security operations center (SOC) with 8×5 or 24×7 coverage would still benefit from having a service arrangement with an endpoint security vendor or managed security services partner for after-hours coverage and escalation support. These services focus on monitoring alerts and suspicious threats, providing guidance and next steps to incident responders, including proactive threat hunting (including searching for indicators of compromise, identifying potential vulnerable and unauthorized programs, and retrieving and analyzing forensic artifacts). Once the event is analyzed, an incident notification explains the threat and recommendations for review and remediation steps.

Incident Response

Despite the merits of endpoint security, no solution or even layered solution set is perfect. Bad actors do get through for one reason or another. As much as it is imperative to block ransomware and other attacks before they execute, having a plan to fail, mitigate, and remediate the damage caused by an attack is just as important. When a security incident is discovered, it's imperative to respond immediately to minimize potential damage, even with containment in place. Specialized skills, tools, and repeatable processes are required for effective threat mitigation. These can be used to assess the situation and determine how to contain the threat and recover operations.

A robust endpoint security platform needs to be the first and last line of defense as people work from anywhere in the world. Today, a modern platform should automatically detect when a malicious action has occurred, such as the unapproved encryption of a file or a connection to a C2 server, for instance, and follow a preplanned set of measures to eliminate the threat and heal the endpoint. First-generation endpoint detection and response (EDR) tools were great to handle an attack based on artificial intelligence (AI) and ML algorithms. Still, they damaged SOC staff because they were soon inundated with alerts that led to their burnout. The more customized one can design their automated incident response playbooks, the less manual remediation has to occur.

A robust endpoint security platform needs to be the first and last line of defense as people work from anywhere in the world.

Summary

The walls between the home and the corporate office eroded significantly during the COVID-19 pandemic, giving adversaries a lucrative foothold into the corporate network. With remote work, the desktops secured behind corporate firewalls became home laptops operating outside the corporate perimeter, significantly increasing the attack surface. Many of these devices are also used as workers travel, where they often connect with corporate resources through public access points. Furthermore, the same device used to access the corporate network may be used to surf the web outside the corporate firewall, exposing connected resources to malicious content.

Organizations need an endpoint security platform that will be the first and last line of defense. They need to be able to handle the world's most aggressive and well-designed forms of attacks while protecting people and communications coming from the endpoint from connecting to malicious sites and C2 servers, among others. They need to block nearly everything before malware executes and remediate the problems on the endpoint if they ever do.

[1] "Beyond Boundaries: The Future Of Cybersecurity In The New World Of Work," Forrester, September 2021

[2] "Global Threat Landscape Report: A Semiannual Report," FortiGuard Labs, August 2021.

[3] "The 2021 Ransomware Survey Report," Fortinet, September 28, 2021.

[4] Ibid.

[5] "Quantifying the Risk Reduction of Evolving Endpoint Security Technologies," Aberdeen Strategy and Research, July 2021.

www.fortinet.com

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.

December 23, 2021 10:53 AM

1384378-0-0-EN