Setting Up Endpoint Strategies, Processes, and Technology To Address Ransomware
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Pre-incident Strategy</td>
<td>6</td>
</tr>
<tr>
<td>Continuous Monitoring Strategy</td>
<td>7</td>
</tr>
<tr>
<td>Response Strategy</td>
<td>9</td>
</tr>
<tr>
<td>Summary</td>
<td>10</td>
</tr>
</tbody>
</table>
Executive Summary

The threat landscape continues to evolve with more sophisticated attacks and evasive techniques. Ransomware is one of the most chilling forms of cyber crime that organizations face today, and it’s not going away. FortiGuard Labs reports that there was a sevenfold increase in ransomware activity in December compared to July 2020.¹ 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.²

Ransomware can gain access to a system in a number of ways, often with a simple click or even no click at all. And because ransomware is so prevalent, organizations need to be prepared. They need to have strategies in place so they are prepared before, during, and after a ransomware attack. Many mature enterprises already have incident response plans, which should be used. But to reduce the risk and scope of potential incidents, many things also should be done in advance to lower the risk of an incident and to understand what to do when in the midst of an attack.
The continued evolution of Ransomware-as-a-Service (RaaS), an emphasis on “Big Game Hunting” (big ransoms for big targets), and the threat of disclosing compromised data if demands weren’t met created a market for massive growth that cyber criminals turned into big profits.\(^3\)
Introduction

Ransomware attacks are increasing and they tend to be extremely thorough. Attackers are taking the time to do reconnaissance to target specific victims and may lurk in the environment for weeks at a time, mapping it out and circumventing security controls. The longer attackers lurk, the more damage they can do. This time gives them the opportunity to not only drop the ransomware payload but also to figure out ways to exfiltrate your data and then hold that information hostage as well. Organizations need comprehensive prevention, detection, response, and remediation strategies in place so critical systems can be restored as quickly as possible.
Pre-incident Strategy

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), to protect off-network devices; advanced endpoint security, including endpoint detection and response (EDR) solutions that can disrupt malware mid-attack; and zero-trust access and network segmentation strategies that restrict access to applications and resources based on policy and context, should all be considered to minimize risk and to reduce the impact of a successful ransomware attack. Finally, the human element remains as important as technology. It’s important to continuously give employees updates on new social engineering attack methodologies so they know what they should and shouldn’t do.

That said, because endpoints are the ultimate destination of ransomware, you need to focus on strong endpoint security. This process starts with reducing the attack surface of each endpoint by closing off unnecessary ports and peripherals, controlling the 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. The analysis should be performed on all code that is being 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.
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 7.5% risk of compromise). The report also established the incremental value of attack surface reduction at 4.7%, bringing effectiveness to 96%. It calculated that behavior-based endpoint security can actually raise effectiveness to 99.6% (or just 0.4% risk exposure).4

For all the prevention measures, organizations that do have a security operations center (SOC) with 8×5 or 24×7 coverage, it is a good idea to have a service arrangement with your 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, which may include proactive threat hunting that includes 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/or remediation steps.
Ransomware is involved in 27 percent of malware security incidents.\textsuperscript{5}
Response Strategy

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.

Even with the people tools and process in place, further preparation and practice remain essential to smooth response actions in the midst of an emerging cyber incident. These activities include:

- Incident response readiness assessment to evaluate an organization’s current security posture through the review of the network architecture, security controls, and staff roles and responsibilities. The objective is to identify technology, people, and processes
- Incident response playbook review to determine sufficiency and areas for improvement of the step-by-step process in the event of a major cybersecurity incident such as a ransomware attack
- Incident response tabletop exercises to simulate incident types and test the organization’s actual incident response plan and execution, with the goal of practicing and improving the response processes
Summary

When an organization is in the midst of a ransomware attack, it’s too late to put the strategies, processes, and technology in place to stop the damage. Planning and preparation before an attack occurs is key. To help security teams mitigate the damage from threats and minimize the time it takes to respond, organizations should invest in solutions that cover all the stages of attack surface reduction, threat prevention and detection, containment, and response.