INDUSTRY TRENDS

How to Prevent Ransomware Attacks: 9 Best Practices

By Renee Tarun | December 06, 2021

Ransomware attacks have become a massive problem for almost every industry and every organization size. In the U.S., federal officials have called it one of the biggest threats currently facing the nation. Criminals are attacking schools, shipping agencies, healthcare organizations, medical trials, and more. Given the impact these attacks can have on organizations everywhere, security professionals need to secure their systems, networks, and software in new ways.

What is a Ransomware Attack?

Ransomware is a specific type of malware that holds data hostage in exchange for a ransom. As an attack methodology, it has the potential to cause severe damage. Phishing emails are a common delivery method, but ransomware can also be spread through drive-by downloading, which is when a user visits a website that's infected. Advanced attacks take seconds to compromise endpoints, and ransomware attacks take seconds to damage your systems and infrastructure. That's why it's critical to ensure your organization is prepared. As attacks grow in sophistication, the impact of ransomware goes beyond financial losses and the productivity loss associated with systems going down.

What Can You Do to Prevent Ransomware Attacks?

Attempted attacks and data breaches are inevitable, and no organization wants to be forced to decide between paying a ransom payment or settlement and losing important data. Fortunately, those aren't the only two options. The best option is to keep from being forced into that decision in the first place. This approach requires a layered security model that includes network, endpoint, edge, application, and data-center controls powered by actionable threat intelligence.

9 Ways to Prevent Ransomware Attacks and Limit Their Impact

With that in mind, here are nine things to consider to give your organization the best chance of avoiding ransomware attacks.

1. Email Gateway Security and Sandboxing

Email is one of the most popular attack vectors for threat actors. A secure email gateway solution provides advanced multilayered protection against the full spectrum of email-borne threats, and sandboxing provides an added layer of protection. Any email that passes the email filter and still contains unknown links, senders, or file types can be tested before it reaches your network or mail server.

2. Web Application Security/Firewall Technology

A web application firewall (WAF) helps protect web applications by filtering and monitoring HTTP traffic to and from a web service. It's a key security element because it acts as the first line of defense against cyberattacks. As organizations execute new digital initiatives, they often expand the attack surface at the same time. New web applications and application programming interfaces (APIs) can be exposed to dangerous traffic because of web server vulnerabilities, server plugins, or other issues. A WAF prevents ransomware attacks by keeping helps keep these applications and the content they access secure.

3. Threat Intelligence Sharing

Organizations must have real-time actionable intelligence to help mitigate unseen ransomware threats, such as what is offered through FortiGuard Labs. Information must be shared between the different security layers and products within your environment to provide a proactive defense. In addition, this information sharing should extend to the broader cybersecurity community outside of your organization, such as Computer Emergency Response Teams (CERTs), Information Sharing and Analysis Centers (ISACs), and industry coalitions like the Cyber Threat Alliance (CTA). Rapid sharing is the best way to respond quickly to attacks and break the cyber kill chain before it mutates or spreads to other systems or organizations.

4. Protecting Endpoint Devices

Traditional antivirus technologies don't always do a good job of preventing ransomware attacks, and as threats continue to evolve, they typically can't keep up. Organizations need to make sure they are appropriately protecting endpoint devices using an endpoint discovery and response (EDR) solution and other technologies.

In the current threat environment, advanced attacks can take minutes or seconds to compromise endpoints. First-generation EDR tools simply can't keep up because they require manual triage and responses. Not only are they too slow for today's lightning-fast threats, but they also generate a massive volume of alarms that burden already overworked cybersecurity teams. Additionally, legacy EDR security tools can drive up the cost of security operations and slow network processes and capabilities, which can have a negative impact on the business.

In contrast, next-generation EDR solutions deliver advanced, real-time threat intelligence, visibility, analysis, management, and protection for endpoints – both pre- and post-infection to protect against ransomware. These EDR solutions can detect and defuse potential ransomware threats in real-time to proactively reduce the attack surface and help prevent malware infection and automate response and remediation procedures with customizable playbooks.

5. Data Backups and Incident Response

Your organization should be able to perform backups of all your systems and data and store it off the network. These backups should also be tested to ensure you can properly recover.

Every organization should have an incident response plan in place, to ensure your business is prepared if you're hit by a successful ransomware attack. People should have specific tasks assigned ahead of time. For instance, who will you contact for help with forensic analysis? Do you have experts readily available to help you restore systems? You also should be running exercises on a regular basis, with a focus on how you would recover from a ransomware attack.

6. Zero-trust Implementation

The zero-trust security model assumes that anyone or anything that attempts to connect to the network is a potential threat. This network security philosophy states that no one inside or outside the network should be trusted unless their identification has been thoroughly checked. Zero-trust recognizes that threats both outside and inside the network are an omnipresent factor. These assumptions inform the thinking of network administrators, compelling them to design stringent, trustless security measures.

With a zero-trust approach, every individual or device that attempts to access the network or application must undergo strict identity verification before access is granted. This verification uses multi-factor authentication (MFA), which requires users to provide multiple credentials before they are granted access. Zero-trust also includes Network Access Control (NAC), which is used to restrict unauthorized users and devices from gaining access to a corporate or private network. It ensures that only users who are authenticated and only devices that are authorized and compliant with security policies can enter the network, helping to detect and prevent ransomware threats.

7. Firewalls and Network Segmentation

Network segmentation is increasingly important as cloud adoption increases, especially in multi-cloud and hybrid cloud environments. With network segmentation, organizations partition their network according to business needs and grant access according to role and current trust status. Every network request is inspected according to the requestor's current trust status. This is extremely beneficial to prevent lateral movement of threats within the network if they do in fact get inside the network.

8. User Training and Good Cyber Hygiene Are Key

Humans need to be at the heart of any cybersecurity strategy. According to the 2021 Verizon Data Breach Investigations Report, 85% of data breaches involve human interaction. You can have all the security solutions in the world, but if you've overlooked training your employees in cyber awareness, you'll never be truly secure. Make sure all your employees receive substantial training on spotting and reporting suspicious cyber activity, maintaining cyber hygiene, and securing their personal devices and home networks. Employees should take training when they are hired and periodically throughout their tenure, so the information stays current and top of mind. To help prevent ransomware and decrease the severity of attacks, training also should be kept updated and include any new security protocols that may need to be implemented.

Educating individuals, especially remote workers, on how to maintain cyber distance, stay wary of suspicious requests, and implement basic security tools and protocols can help CISOs build a baseline of defense at the most vulnerable edge of their network and help keep critical digital resources secure.

Organizations must also practice good basic cyber hygiene to ensure all systems are properly updated and patched.

9. Deception Technology

Organizations should also be aware of deception technology. Although it's not a primary cybersecurity strategy, deception solutions can help protect systems if, despite all the other cybersecurity strategies you have in place, the bad actors still find a way in.

With deception technology, decoys mimic the actual servers, applications, and data so that bad actors are tricked into believing they have infiltrated and gained access to the enterprise's most important assets when in reality, they haven't. This approach can be used to minimize damage and protect an organization's true assets. In addition, deception technology can accelerate the average time to discover and address threats.

Prevent Ransomware Attacks and Keep Your Data Safe

Ransomware attacks are everywhere. Company size and industry no longer matter as criminals search for an easy entry point into the network. What's more, the global shift to remote work has created an increased risk for bad actors to exploit, and they are making the most of their moment. According to the Fortinet Global Threat Landscape Report, by the end of 2020, there were as many as 17,200 devices reporting ransomware each day.

Despite all of this, organizations are hardly helpless. They may need to do some rethinking and reorganizing, but tools are available that can provide significant protection against ransomware attacks. Evaluate these nine recommendations and consider what you might need to do differently to give your organization the best possible chance of preventing ransomware attacks.

Learn how the Fortinet Security Fabric can help prevent ransomware across all points of entry and combat today's most advanced threats. Understand the scope, risks, and prevention techniques of ransomware.

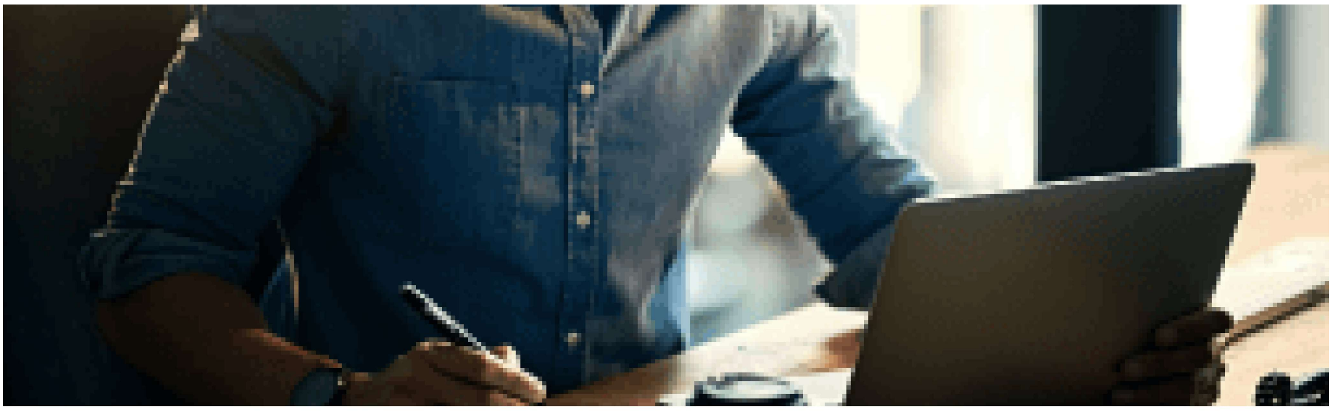
Related Posts

INDUSTRY TRENDS

How to Prevent Evolving Ransomware Attacks

INDUSTRY TRENDS

Analyzing the History of Ransomware Across Industries



INDUSTRY TRENDS

FORTINET

News & Articles

News Releases

News Articles

Security Research

Threat Research

FortiGuard Labs

Threat Map

Ransomware Prevention

Connect With Us

Fortinet Community

Partner Portal

Investor Relations

Product Certifications

Company

About Us

Exec Mgmt

Careers

Training

Events

Industry Awards

Social Responsibility

CyberGlossary

Sitemap

Blog Sitemap

Contact Us

(866) 868-3678

Also of Interest:

DOJ & Top Security Threats
Pay Ransomware Settlements?
Survey Reveals Challenges of Zero Trust Implementation
Types of Ransomware Attacks and Cyber-Hygiene...