SOLUTION BRIEF

Preventing Ransomware in Small Businesses

Protection Begins by Knowing How It Works

Executive Summary

Ransomware is a threat to all organizations, but small and midsize businesses (SMBs) are particularly vulnerable to this type of attack. Seventy-one percent of ransomware attacks in 2018 targeted small businesses[1] and piecemeal security solutions might not be enough to protect against more sophisticated threats. In addition, SMBs might not have the internal resources, knowledge, or security budget to confidently prevent ransomware and deal with the ramifications of a successful attack. To fight ransomware, businesses need a comprehensive solution that is simple, straightforward, and affordable, so that they can focus on growing the business while knowing their users and data are protected.

Hackers Are Attacking Small Businesses with Ransomware

Ransomware is when hackers gain access into an organization's network, usually via malicious email, and demand payment of the organization to get its data back. Larger businesses can sometimes absorb ransom demands, but for SMBs, a ransomware attack is potentially catastrophic. For many organizations, the loss of critical business cycles and revenues from systems that are grounded far outweigh the price of the ransom itself.

Gaps in Security Threaten Smaller Businesses

The pressing need for speed and agility across businesses of all sizes has led to the rapid adoption of new technologies such as Software-as-a-Service (SaaS), public cloud, and other omnichannel customer engagement tools that bring convenience and flexibility, and help overall customer and user experiences. But these innovations also create security vulnerabilities when administrators are unable to understand how applications are using data and how users are accessing it—making it easier for even basic threats to get past defenses when those defenses aren't effectively communicating.

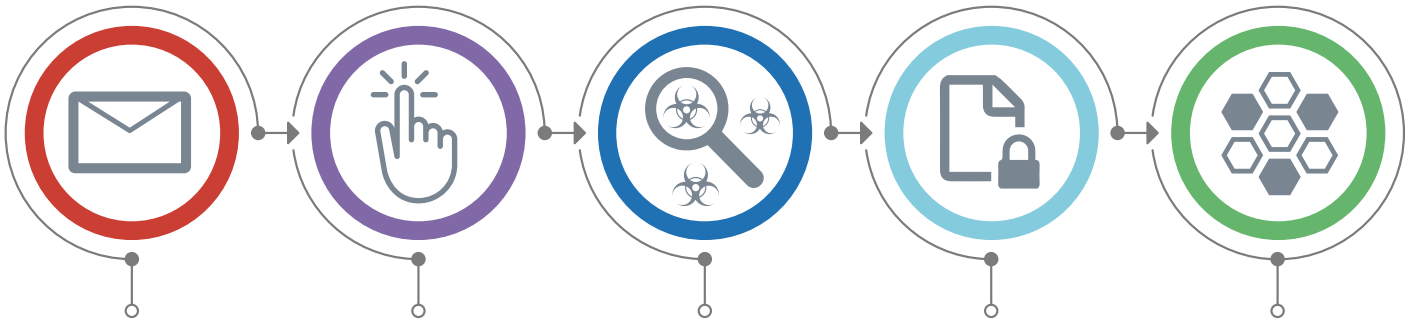
For many organizations, security is a mishmash of different solutions. Each product has its own version of policies and rules that don't mesh with other products without customization or additional third-party technology to translate from one device to the other. This makes it easy for bad actors to exploit gaping security gaps. And as the world shifts to more users engaging outside the traditional perimeter, businesses can't expect ransomware attacks to wane; the vulnerability factors, relative ease of implementation, and high-profit potential for bad actors mean the frequency of attacks only continues to increase.

By 2021, there will be a ransomware attack every 11 seconds.[2]

How Malicious Emails Circumvent Security

- **Email attachments:** Attackers use advanced technology that's designed to evade security. Without a way to analyze the attachment, organizations have no indication of the threat.
- **URLs embedded in email:** Sites that look legitimate are often blindly clicked. Many organizations are unable to analyze embedded links, nor can they identify known malicious sites.

How Ransomware Attacks



Step 01
Email

A user receives a malicious email that appears to be legitimate, enticing the user to click a link or download an attachment that delivers the malware.

Step 02
User Clicks and Attack Begins

Once a user clicks an attachment or URL, the attack is launched. Without effective network security or endpoint protection there's not much an organization can do to stop the attack.

Step 03
Hunts Network

Once the malware is unleashed, it hunts for key data and folders, and can disable backup and recovery mechanisms.

Step 04
Encrypts

Within the network, the malware establishes command and control to communicate back to the attacker and begins to encrypt files.

Step 05
Lateral Movement

Without network segmentation, the malware spreads laterally and automatically hunts for other connected networks to infect.

SMBs Need a New Approach in the Fight Against Ransomware

SMBs need to be ahead of the curve when it comes to taking precautions against ransomware threats. In this fight, prevention is the best defense. When considering an approach to protecting against ransomware, SMBs should make sure their solution is:

Effective and Comprehensive: Many security providers say their solution will work, but for a solution to be truly effective, it must provide broad coverage. Ransomware only needs a small opening to be effective, so it's critical to plug every hole in security coverage. Only comprehensive security coverage that's been validated provides that.

94%
of cyberattacks in general leverage email to begin their attack.[3]

Easy to Use and Affordable: Many SMB security teams are focused on many tasks, perhaps lacking specific malware prevention expertise. A solution needs to be simple, straightforward, and affordable, one that gives the organization the level of protection they need without the burden of overstretched resources and/or budgets.

Reputable and Lasting: SMBs must be smart about their investments. Buying something only to throw it away along with the solution experience when its capabilities can't scale as they mature just isn't a smart option. Hackers are continuously evolving, so should cybersecurity capabilities of SMBs. Their security providers should be able to show long-term ROI as part of the proposed investment.

Fortinet Delivers Comprehensive Protection Against Ransomware

Few security vendors offer solutions to protect their clients across multiple attack vectors, specializing in one area but not another and forcing their customers to build and manage custom integrations or invest in additional third-party tools. Only Fortinet is engineered to bring a broad, integrated, and automated Security Fabric approach to security across network, email, and endpoint security along with Cyber Threat Assessment Programs (CTAPs) to help businesses identify potential risks and solidify their defenses.

FortiMail Prevents Phishing and Other Email-initiated Attacks

FortiMail is available as a SaaS offering or on-premises device and brings powerful anti-spam and anti-malware capabilities to organizations to stop unwanted bulk emails, phishing attempts, and other business email compromise techniques. Complemented by technology designed to prevent outbreaks, automatically remove harmful active content embedded in messages and impersonation, FortiMail is a strong first step to protecting the business from ransomware.

Security-driven Networking Prevents Malicious Files and Communications on the Network

The Fortinet FortiGate next-generation firewall (NGFW) is the most widely deployed NGFW on the market and ensures malicious actions and communications crossing the perimeter are blocked, such as when a user accidentally arrives at a malicious website and a drive-by download attack ensues. Administrators gain visibility over how applications are interacting with data, users, and the devices with out-of-the-box reporting and the ability to easily control these activities to better protect the business. With plug-and-play ease, businesses can effortlessly extend this security to wireless (FortiAP) and wired (FortiSwitch) devices to harden their infrastructure.

Mature organizations looking to add segmentation can also institute the FortiGate to monitor east-west traffic as well as deploy the FortiGate virtually in public clouds for a seamless security experience.

FortiClient and FortiEDR Stop Attacks at the Endpoint

FortiClient strengthens endpoint security through integrated visibility, control, and proactive defense. With the ability to discover, monitor, and assess endpoint risks, IT teams can ensure endpoint compliance, mitigate risks, and reduce exposure. FortiEDR provides additional protection by detecting and defusing potential threats in real time and can automate response and remediation with customizable playbooks.

FortiSandbox Cloud Prevents Advanced Threats and Automates Threat-intelligence Sharing

When security solutions aren't designed to work together, the burden of creating automation and scaling to address the endless number of alerts from disjointed products falls on the business. The Fortinet Security Fabric answers this challenge with FortiSandbox Cloud. As a licensing option for the above solutions, FortiSandbox Cloud creates a central point for products to send unknown files. Advanced analysis determines their threat level and communicates this information across the Fabric. Threat intelligence is gathered from Fortinet customers around the world and shared, ensuring no matter where a threat was first encountered, the entire community has actionable intelligence.

Helping SMBs Put Ransomware in Its Place

As long as smaller businesses present an easy target for cyber criminals, the threat of ransomware will not go away on its own. The Fortinet Security Fabric architecture offers SMBs advanced capabilities and threat-intelligence sharing to help them prevent, detect, and remediate ransomware and other sophisticated modes of attack.

[1] "Beazley Breach Briefing – 2019," Beazley, March 21, 2019.

[2] "Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021," Cybersecurity Ventures, October 21, 2019.

[3] "2019 Data Breach Investigations Report," Verizon, 2019.

FORTINET

www.fortinet.com

May 26, 2020 2:58 PM

677787-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2020:SB-Preventing-Ransomware-SMB:sb-preventing-ransomware-smb-052620-258pm