SOLUTION BRIEF

Repel Ransomware Attacks With Fortinet Proactive, Reactive, and Managed Services

Executive Summary

Today's organizations are changing rapidly to meet the needs of the times, including Software-as-a-Service (SaaS) apps and cloud adoption, remote users, increased business collaboration tools, new acquisitions, and employee and security staff changes. Change is constant, whether digital transformation or pandemic adaptations in the enterprise. At the same time, ransomware continues to evolve and remains as pervasive as ever. With regular changes in tactics, techniques, and procedures (TTPs), security teams and the broader organization must stay alert to reconnaissance-stage tactics to early footholds and, ultimately, ransomware.

Fortunately, Fortinet provides proactive, reactive, and managed services that help enterprises detect, prevent, and respond to ransomware attacks. Our expert teams work with security leaders, architects, and other team members to prepare incident-response plans, exercise their teams, manage endpoint detection and response (EDR) and the Fortinet Security Fabric, and respond to incidents. With this diversity of services to prepare, maintain, and respond, we can augment enterprise security teams and help security leaders assess and improve their state of readiness for such attacks.

Don't Overlook the Planning

Regardless of the specific number of ransomware attacks, variants, or Ransomware-as-a-Service (RaaS) groups, the prevalence and potential impact of this category of malware is an ongoing enterprise reality and significant concern. Meanwhile, organizations are dynamic, living entities—full of employee turnover, shortfalls in security staff resources and skill sets, and many other challenges. From cloud and new business software adoption to digital transformation initiatives to mergers, acquisitions, and other organizational changes, the technology evolutions alone make it difficult for security leaders to maintain a consistent and high level of security.

Fortinet Services

PREPARE

- Ransomware Assessment Service
- Ransomware playbook development
- Ransomware tabletop exercises
- Incident Readiness Subscription Service

MAINTAIN

- SOCaaS
- Managed detection and response
- Security awareness and training
- Cybersecurity certification

RESPOND

- Incident response

Meanwhile, most security teams are so stretched attending to their necessary daily operations that it can be easy to overlook the planning for a preemptive, proactive stance against ransomware or other threats. Add to that a lack of the right skills to be proactive, and it's no surprise that the number one reason organizations don't have an incident response plan is attributed to a lack of skilled internal resources.[1] So, what can security leaders do to keep their organization's risk level low?

Prepare, Maintain, and Respond

Fortinet provides services that help organizations by:

- **Preparing** with regularly updated assessments and processes for ransomware attacks
- **Maintaining** the security of their networks against ransomware, and the skills and awareness of their security staff and employees
- **Responding** to a ransomware attack if needed

Security Experts With Practical Experience

Preparing security organizations to address the constant threat of ransomware requires security experts with practical "on the ground" experience. Ideally, they will have:

- Dealt with the latest attacks
- Access to real-time threat intelligence of the latest attacker TTPs, malware families and variants, and other threat insights
- Security expertise in the people, processes, and technology necessary to maintain the security of today's changing enterprise

Fortinet proactive, reactive, and managed services bring this level of expertise to every organization we support. Backed by FortiGuard Labs experience and expertise, our facilitators, trainers, practitioners, and responders have spent decades threat hunting, analyzing malware and attacks, conducting forensics investigations, and responding to incidents.

Prepare

FortiGuard Incident Readiness Services can provide organizations with preparation for ransomware—with the expertise and experience of a team of "first responders" to cyberattacks. Firsthand experience of attacks means firsthand knowledge of the recurring gaps in cybersecurity planning, operations, and processes that let such attacks happen.

Our facilitators, playbook developers, and assessors are skilled not only with years of cybersecurity expertise but also backed by the threat insights and analysis of FortiGuard Labs. Together, they assess, test, and strengthen an organization's incident-response plan before a security incident occurs, with:

- Ransomware Assessment Service
- Ransomware playbook development
- Ransomware tabletop exercises
- Incident Readiness Subscription Service

Maintain

In ransomware attack investigations, several key themes prevail, such as missed alerts and warnings, product misconfigurations, absent security best practices—often from staff and skill-set shortages—and inadequate employee awareness. In fact, across 1,200 organizations surveyed globally, 60% of leaders struggle to recruit cybersecurity talent, while 52% struggle to retain it.[2] And 52% believe their employees lack the necessary knowledge.[3]

Fortinet provides several options for augmenting understaffed security teams—monitoring customer environments and threat hunting, triage and response to incidents, and working with and on behalf of security teams with the following services:

- SOC-as-a-Service (SOCaaS) 24/7 log-based monitoring, triage, and incident escalation service for FortiGates and the Fortinet Security Fabric
- Managed detection and response 24/7 monitoring, threat hunting, analysis, and response to malicious activity detected on endpoints based on FortiEDR and FortiXDR

To help address skill sets within the existing staff and overall employee awareness, Fortinet offers employee awareness training with **timely and current awareness of today's cybersecurity threats**, as well as cyber-professional training and certification through the following services:

- Security Awareness and Training to help IT, security, and compliance leaders build a cyber-aware culture
- Fortinet Network Security Expert (NSE) training and certification program

Respond

Utilizing cutting-edge incident response and forensics technology and practices to assist customers with the detection, analysis, containment, and remediation of security incidents, these first responders reduce the time to resolution, limiting the overall impact on the organization from the incident.

Backed by FortiGuard experience and expertise, our incident response team calls upon decades of experience in threat hunting, analyzing malware and attacks, conducting forensics investigations, and incident response to act swiftly on incidents. With a one-hour response time,[4] our team provides critical services during and after a ransomware incident.

A Comprehensive Approach to Ransomware Preparedness

For a more comprehensive approach to ransomware preparedness, our services help guide and prescribe, rather than overwhelm security leaders, to make prioritized, impactful decisions that can mean the difference in their business operations continuity.

Essential preparation to effectively handle security incidents. FortiGuard experts work with organizations to proactively assess their security—with options to test and build incident response processes, increasing the readiness to appropriately respond to an attack.

“41% of enterprises surveyed conduct cyber-risk assessments annually.… Conducting cyber-risk assessments is critical to effective monitoring of risk factors and to improving response capabilities.”[5]

Rapid response to reduce business disruption. Our incident response teams draw from decades of firsthand investigatory experience to respond immediately. Our teams immediately stop additional damage, contain the impact, and help minimize business disruption and recover operations from a ransomware attack.

Expert assistance to scale, reduce burnout. Augment existing staff 24/7 with the resources, skills, and time. Giving you the power to catch and take an appropriate response to issues 24/7, with the right skill set, our teams help you do what’s necessary to protect your enterprise.

Increased user awareness, protected data, stopped breaches. The Fortinet Security Awareness and Training service helps create a security-compliant culture where employees are trained to be more aware and knowledgeable of potential security threats. They will feel empowered to report threats when they see them.

Prepared cyber professionals. The Fortinet NSE program of eight-level training and our certification program provide self-paced and instructor-led courses and practical, experiential exercises to demonstrate mastery and give independent validation of network security skills and experience.

Conclusion

Fortinet proactive, reactive, and managed services can help organizations prepare and respond to ever-evolving ransomware threats and maintain the resilience of their ever-changing networks. Providing security leaders with insights into their current gaps and domain-level knowledge of relevant practices that inform their ongoing cybersecurity strategies, our services and expertise can augment security teams 24/7, globally, if and as needed.

[1] Fortinet, 2021 Ransomware Survey Report, September 2021.

[2] Fortinet, 2022 Global Cybersecurity Skills Gap Research Report, April 2022.

[3] Ibid.

[4] Requires Incident Response Retainer Service for a one-hour response time.

[5] ISACA State of Cybersecurity 2022, Global Update on Workforce Efforts, Resources, and Cyberoperations, page 35, 2022.

www.fortinet.com

September 1, 2022 4:07 PM

1696133-0-0-EN