We’re With You on the Journey
Services to Support Your Ransomware Readiness

The journey to ransomware readiness requires maintaining staff security skillsets and employee awareness, plus regularly updating network (virtual, physical, or cloud) defenses and processes. Turnover in staff and employees, network dynamics, and changes in ransomware tactics, techniques, and procedures (TTPs) all contribute to a change in the state of an organization’s readiness to withstand a ransomware attack. If your organization lacks the needed skillset, opt for a managed service to protect the network and endpoints.

Ongoing training and proactive measures, including regularly updated ransomware assessments, playbooks, and tabletop exercises, help in several ways. You can understand your state of readiness, identify and address specific gaps, and update your readiness to withstand ransomware attacks. These measures, for ransomware and overall threat readiness, are an important part of good cyber hygiene.

Enterprise Evolution
• New tech, partners
• Digital transformation
• 41% executives don’t feel their security has kept up with digital transformation

Skillset Shortages
Lack of skilled personnel was the #1 factor preventing companies from defending against cyber threats.

Employee Turnover
In 2021, the overall turnover rate across industries was 57.3% (U.S.).

Ransomware Explosion
• Revenue increases
• TTPs ever-changing
• FBI’s Internet Crime Complaint Center reported a 62% year-over-year increase in ransomware complaints
• Has had >130 different strains since 2020

Ransomware Impact
• Doubled in frequency in 2021
• Took <4 hours to successfully infiltrate their target in ~97% of all attacks

NSE Training helps cybersecurity professionals maintain proficiency
Security and Awareness Training helps maintain employee awareness about security threats, including ransomware

SOCaaS and Managed EDR/XDR skillfully augment your teams to manage your network and endpoints

Ransomware playbooks provide set of new or refreshed prescriptive steps for ransomware attack
Ransomware TTXs evaluate a team’s adoption and ability to follow playbook

Incident Response helps teams investigate and recover from ransomware (and other) critical incidents

Did you know:
“A risk assessment can quickly identify and prioritize cyber vulnerabilities so that you can immediately... protect critical assets...while immediately improving overall operational cybersecurity.”

“The number one reason organizations did not have an incident response plan was due to lack of skilled internal resources.”

Fortinet has expert resources available to help you address these common challenges.

---

8 Ibid.