FERTINET

SERVICE BRIEF

Prepare for and Respond to Incidents with the FortiGuard Incident Readiness Subscription Service

Executive Summary

Cyberattacks have become more sophisticated, widespread, and relentless as cybercriminals continue exploiting old and new vulnerabilities. To support organizational resilience and help organizations be better prepared in the event of an attack, Fortinet offers the FortiGuard Incident Readiness Subscription Service, which is a suite of services organizations can select from to prepare, rapidly respond to, and take the most effective actions against today's cyberthreats.

The Only Constant Is Change

Change is an ever-present part of today's functional environments. Organizations must change rapidly to keep up with evolving business and technology needs. And at the same time, threats such as ransomware continue to be pervasive and effective as they evolve to exploit those network and business changes.

Given this perpetual state of flux, preparation is not a one-time activity. Enterprises must vigilantly assess their security posture by examining past compromises and anticipating new events. This security assessment requires continuous updates to incident response plans and playbooks, so every team member is well-versed in established processes.

Organizations also must stay abreast of the evolving threat landscape by incorporating insights from penetration testing and vulnerability assessments into their security strategies. Because the attack surface has so many moving parts, it's increasingly important for security teams to regularly assess security. Security operations center (SOC) and Active Directory assessments from outside professionals can help organizations review processes, talent planning, infrastructure, and detection and response efficacy. These assessments should be performed regularly. Having a second set of eyes helps ensure the organization maintains its effectiveness over time against the backdrop of chronic enterprise change.

The FortiGuard Incident Readiness Subscription Service

The FortiGuard Incident Readiness Subscription Service is an annual subscription that provides options and flexibility, so enterprises can effectively expand and evolve their SOC strategies. With a comprehensive menu of service options, an annual subscription allows enterprises to focus on honing the elements they need and have prioritized in a given year.

Each annual subscription comes with:

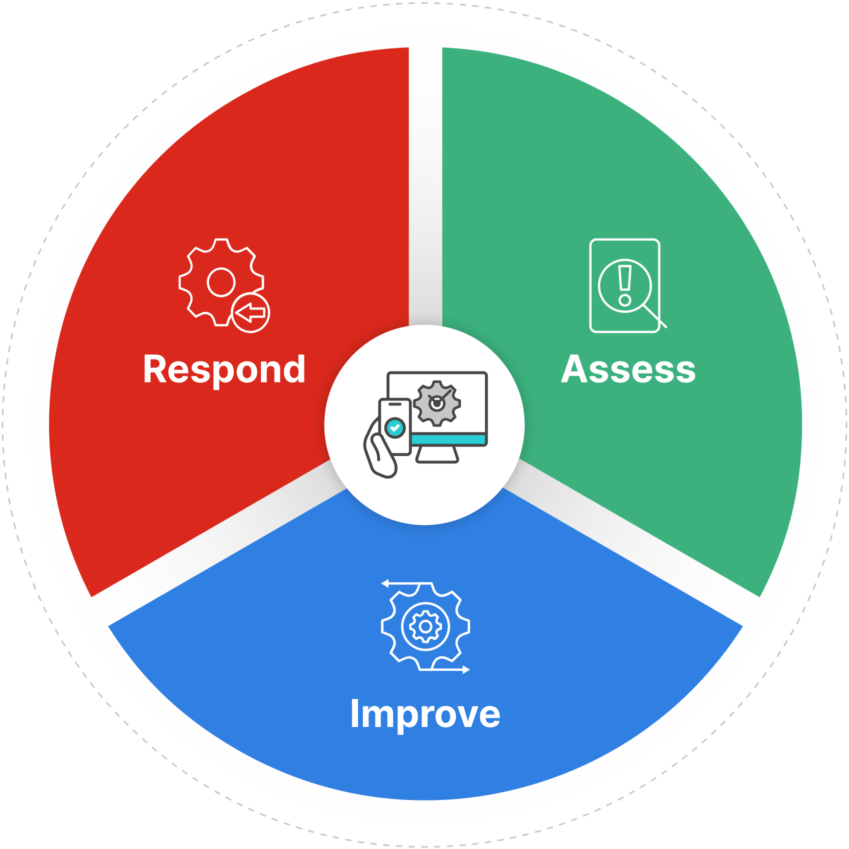
- An incident response readiness assessment
- Incident response retainer that includes a one-hour service level agreement
- Subscription points that can be used for incident readiness service offerings

"Conducting cyber-risk assessments remains a critical business activity for effectively monitoring risk factors and improving risk treatment options."[1]

"Time commitment was indicated as the primary barrier [for not conducting cyber-risk assessments] followed by a lack of personnel to perform assessments."[2]

Organizations can apply subscription points to help them assess and improve their current security posture while effectively responding to threats through advanced digital forensics and incident response capabilities.

Incident Readiness Subscription Service



Assess

- Incident Response Readiness Assessment
- Ransomware Readiness Assessment
- Security Operations Center (SOC) Assessment
- Active Directory Security Assessment
- Compromise Assessment
- Penetration Testing Services
- Vulnerability Assessment Services
- Red Team Assessment
- Countermeasure Assessment

Improve

- Incident Response Plan Development
- Incident Response Playbook Development
- Cybersecurity Tabletop Exercise
- SOC Development Service
- FortiGuard Incident Response Training Series

Respond

- Digital Forensics and Incident Response
- Ransomware
- Business Email Compromise (BEC)
- Web application attacks
- Advanced Persistent Threats (APTs)
- And more...

Figure 1. The FortiGuard Incident Readiness Subscription Service covers three key areas.

For detailed descriptions of each service, see the FortiGuard Security Advisory and Incident Response Services ordering guide.

Benefits of the Service

Organizations subscribe to the FortiGuard Incident Readiness Subscription Service to help them be prepared before an incident occurs and to be able to rapidly respond and remediate after an incident is detected. With the service, organizations benefit from:

- **Essential preparation to effectively handle security incidents.** FortiGuard experts work with organizations to proactively assess readiness with options to test and build incident response processes to increase their ability to appropriately respond to an attack.
- **Rapid response to reduce business disruption due to a cyberattack.** Predefined terms and conditions reduce the time to respond during urgent escalations, which helps minimize the impact of a cyberattack.
- **Expert assistance to the security team.** FortiGuard consultants have decades of first-hand investigatory experience. They also draw on the full support and resources of FortiGuard Labs, one of the world's largest threat intelligence and research organizations.
- **Powerful investigation tools.** FortiGuard experts use a variety of cutting-edge investigation tools, including FortiEDR endpoint detection and response technology. FortiEDR delivers real-time visibility, analysis, protection, and remediation for endpoints. It proactively prevents malware infections, detects and defuses potential unknown threats, and can automate response and remediation procedures.

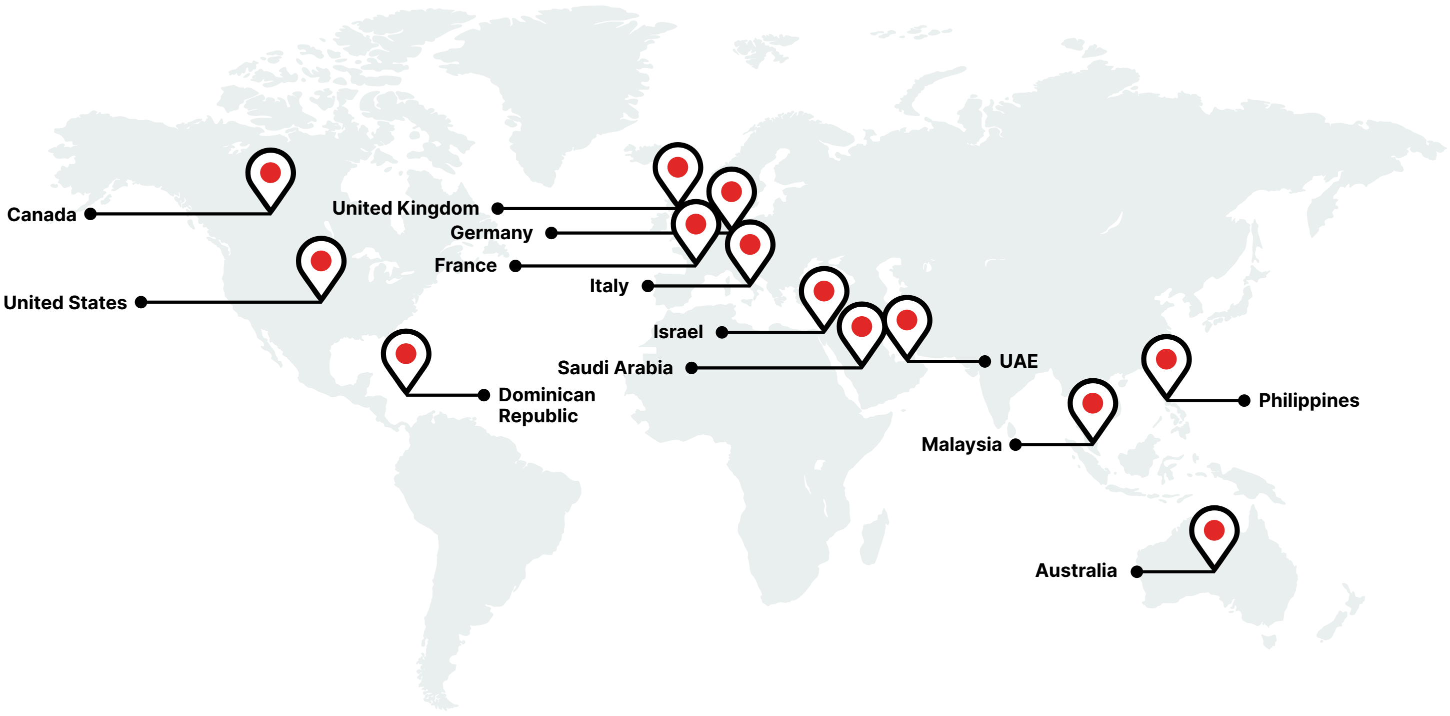


Figure 2: The FortiGuard global security operations center operates 24×7×365.

Why Fortinet?

Security leaders can take advantage of FortiGuard consultants' expertise, bringing top talent with extensive security experience and expertise into their teams. Fortinet offers:

- **Expertise.** The Fortinet Digital Forensics and Incident Response (DFIR) team leverages the experience of FortiGuard Labs. With more than 215 expert researchers, engineers, and analysts worldwide, Fortinet has one of the industry's largest and most successful security research and analyst teams.
- **Technology.** Fortinet uses cutting-edge incident response/forensics technology to help customers detect, analyze, contain, and remediate security incidents. The deployment of FortiEDR endpoint detection and response helps reduce the time to resolution and limits the overall impact on an organization.
- **Reactive and proactive services.** Organizations can choose reactive and proactive services that deliver a mix of incident response support and security services that assess, test, and strengthen the incident response plan before a security incident occurs.
- **Flexibility.** Fortinet has multiple incident response solutions designed to help companies of any size, no matter their unique needs.

The Time Is Now

Cyberattacks are getting increasingly difficult to stop, but the good news is it's possible to minimize or prevent damage, even after a breach is detected. However, doing so requires having the resources and knowledge to plan ahead to enable effective and rapid response. The FortiGuard Incident Readiness Subscription Service helps enterprise IT and security teams of all sizes navigate through high-pressure, high-stakes cybersecurity incidents.

[1] ISACA, Adobe, State of Cybersecurity 2023 Global Update on Workforce Efforts, Resources and Cyberoperations, 2023.

[2] Ibid.

March 14, 2024 9:59 PM
132836-B-0-EN