SERVICE BRIEF

FortiGuard Incident Readiness Subscription Service

Critical Services To Help Prepare Before a Security Incident and Rapidly Respond After One Is Detected

Executive Summary

Today's threat actors are continuously innovating, creating more sophisticated attacks and methods of delivery. The reality is that security breaches are inevitable. At some point, every organization is faced with a security incident that needs fast investigation, fast response, and/or fast remediation.

Unfortunately, a large number of organizations may not have the skilled resources to properly prepare for and take care of a security incident when the time comes to act quickly. This typically results in more severe damage and higher business impact than when there is better preparation and an immediate expert response to a detected incident.

"The number one reason organizations did not have an incident response plan was due to lack of skilled internal resources."[1]

To fill this gap, Fortinet offers security leaders the ability to better prepare, rapidly respond, and take the most effective actions at every step, with FortiGuard Incident Readiness Subscription Service.

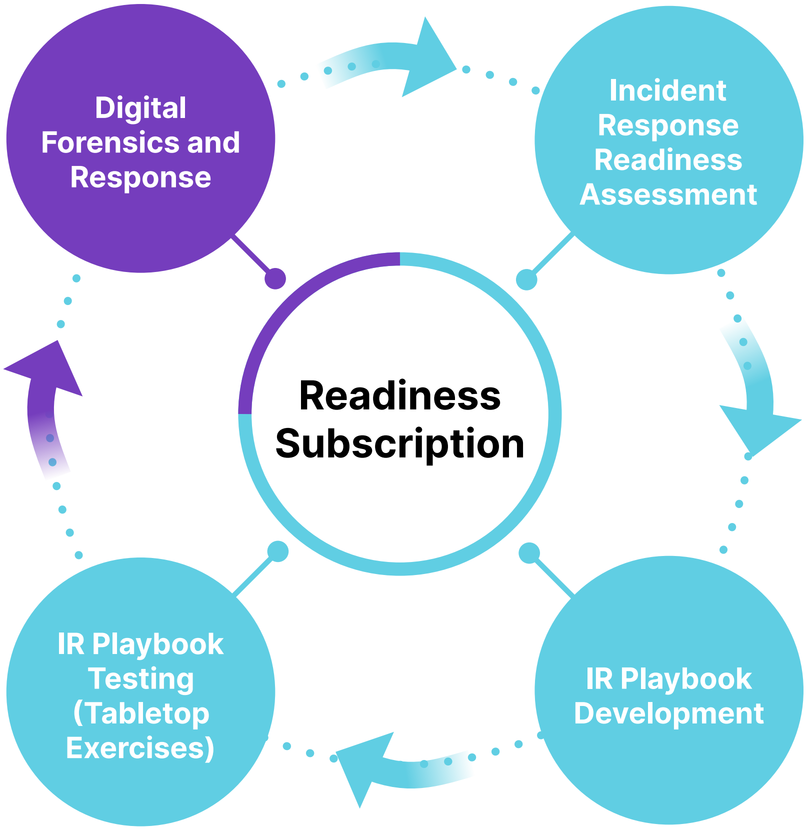
Expert Assistance With Assessment, Design, Testing, and Response

Through interviews with key stakeholders and document review, FortiGuard experts will first focus on assessing the organization's overall ability to respond efficiently and effectively to an unexpected cyber incident and provide a prioritized set of recommendations for further improvement. From there, security leaders have the flexibility to choose proactive services to implement and test their incident response playbooks and reactive services to help respond quickly to a security incident.

FortiGuard Incident Readiness Subscription Service includes:

- Incident Response Readiness Assessment (IRRA)
- 16 initial service points (64 hours) for:
  - Incident Response Playbook Development
  - Incident Response Playbook Testing (Tabletop Exercises)
  - Digital Forensics and Incident Response
- One-hour service-level Objective
- One-year subscription
- Additional hours may be added as needed

In addition, custom reactive and proactive solutions are available through a statement of work (SOW)-based SKU to fit most business needs.



"Ransomware increased by 10.7 times over the last 12 months! And not only has it gotten more prevalent, but it's also gotten even nastier."[3]

Incident Readiness Service Offerings

Incident Response Readiness Assessment: The assessment will be done through key stakeholder interviews and document review. The goal of this assessment is to strengthen the overall ability of an organization to respond efficiently and effectively to an unexpected cyber incident and help prioritize cybersecurity actions and investments. The final report will provide an overall maturity level index score, assessment findings, and a prioritized set of recommendations.

Incident Response Playbook Development: Assist with the development of Incident Response Playbooks. An Incident Response Playbook is a step-by-step guide organizations will use in the event of an impactful cybersecurity incident on the network, based on the most probable events. The playbook is part of an organization's larger incident response plan. Some current probable events include:

- A ransomware attack
- Spear-phishing email messages
- Compromised credentials
- Data loss
- Malware

The playbook will guide analysts in detection, containment, eradication, and recovery.

Incident Response Playbook Testing (Tabletop Exercises): The playbook testing will test the organization's incident response plan and assist in identifying security gaps in cybersecurity or processes. The testing is designed and delivered by the FortiGuard Incident Response Team based on experiences that they've encountered during various incident response engagements. The testing is then separated into several incident scenarios and delivered verbally during a roundtable discussion. There are many types of cybersecurity scenarios that can be used to assess an organization's readiness. Some scenario types could include:

- A ransomware attack
- Business email compromise (BEC)
- Unauthorized access
- Data theft/data loss

By the end of each testing scenario, each stakeholder should have a more in-depth understanding of what actions are taken, and by whom they are performed. The goal is to have a clear and concise incident response action plan.

Digital Forensics and Incident Response (DFIR): The DFIR provides help to organizations in the midst of a cybersecurity incident, including targeted ransomware attacks. Experienced staff, expert skills, powerful tools, and established process are used to efficiently assess the situation, its scope, and steps necessary to contain the impact and help recover operations.

Key Benefits

The primary drivers for subscribing to the FortiGuard Incident Readiness Subscription Service are to be prepared before an incident occurs and to be able to rapidly respond and remediate after it is detected. With the service, organizations will benefit from:

Essential preparation to effectively handle security incidents. FortiGuard experts work with organizations to proactively assess with options to test and build incident response processes, increasing the readiness 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. This results in minimized impact from a cyberattack.

Expert assistance to the security team. FortiGuard consultants have decades of first-hand investigatory experience and draw on the full support and resources of FortiGuard Labs, one of the largest threat intelligence and research organizations in the world.

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.

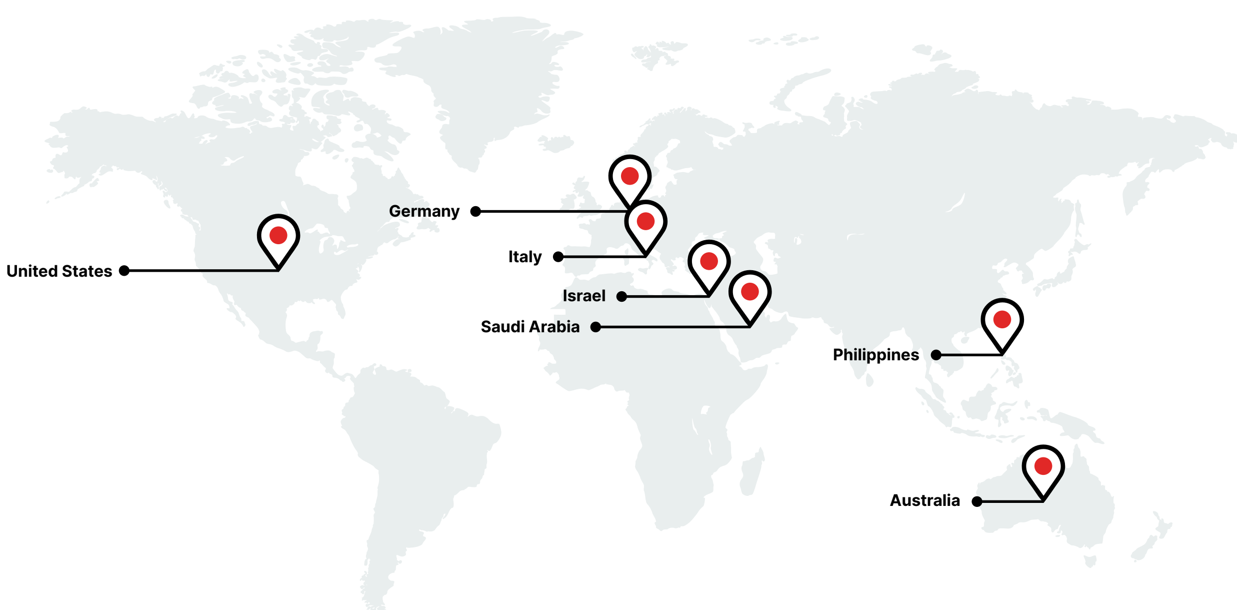


Figure 1: FortiGuard's global security operations center operates 24×7×365.

Why Fortinet Is the Best Choice

FortiGuard consultants give security leaders the opportunity to insert top talent with extensive security experience and expertise into their teams. Key differentiators include:

Expertise. Our Digital Forensics and Incident Response (DFIR) team leverages the experience from FortiGuard Labs. With over 215 expert researchers, engineers, and analysts around the world, we have one of the largest and most successful security research and analyst teams in the industry.

Technology. We utilize cutting-edge incident response/forensics technology to assist customers with the detection, analysis, containment, and remediation of security incidents. This reduces the time to resolution, limiting the overall impact to an organization, through the deployment of FortiEDR endpoint detection and response.

Reactive and proactive services. We provide the ability to choose both reactive and proactive services that deliver a mix of incident response support and security services that assess, test, and strengthen an organization's incident response plan before a security incident occurs.

Flexibility. Our multiple incident response solutions are created to help any size company 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 any damage, even after a breach is detected. This, however, requires having the resources and knowledge to plan ahead to enable effective and rapid response.

The FortiGuard Incident Readiness Subscription Service can help. It's the ideal choice to assist enterprise IT and security teams of all sizes navigate through high-pressure and high-stakes cybersecurity incidents.

Incident Readiness Retainer SKUs

FortiGuard Incident Readiness Subscription Service

FP-10-IR001-709-02-12: Incident Retainer Service (16 points)

FortiGuard Incident Response Emergency Service

FP-10-IR001-710-02-03: Emergency Service (25 points)

FortiGuard Incident Response SOW-based SKUs

FP-10-EDRFRNSCS: Digital Forensics and Incident Response

Service Point SKUs

LIC-IR-10: 10 Service Points for IR Services

[1] "The 2021 Ransomware Survey Report," Fortinet, September 28, 2021.

[2] "Cyturus Adaptive Risk Model (ARM)," Cyturus, accessed October 22, 2021.

[3] "Global Threat Landscape Report," FortiGuard Labs, August 2021.

October 28, 2021 11:32 PM
1328360-0-0-EN