**FORTINET FC-10-0051E-950-02-12**

# Fortinet FortiGuard Unified Threat Protection for FortiGate-51E

Model: FC-10-0051E-950-02-12

## 1. Introduction

The Fortinet FortiGuard Unified Threat Protection (UTP) service provides comprehensive cybersecurity protection for your FortiGate-51E firewall. This service bundle integrates multiple security features to defend against a wide range of cyber threats, ensuring the integrity and availability of your network.

This manual outlines the key features, activation process, operational aspects, and support information for the FortiGuard UTP service.

## 2. Service Overview

The FortiGuard Unified Threat Protection bundle enhances your FortiGate-51E with advanced web security services, building upon the Advanced Threat Protection (ATP) bundle. It is designed to protect organizations against web-borne threats, including sophisticated DNS-based attacks.

### Included Services:

- **Intrusion Prevention System (IPS):** Blocks vulnerabilities and exploits through network traffic inspection.
- **Advanced Malware Protection:** Blocks known malware, including ransomware, based on signature-based detection.
- **Application Control:** Manages and controls network application usage.
- **URL Filtering:** Prevents access to malicious websites and enforces web usage policies.
- **DNS Filtering:** Protects against DNS-based threats.
- **Video Filtering:** Filters video content based on policies.
- **Anti-Botnet and C2 Communications Services:** Detects and blocks communication with command-and-control servers.
- **Anti-Spam:** Filters unwanted email.
- **Sandboxing:** Executes suspicious files in an isolated environment to detect zero-day threats.
- **Web Application Firewall (WAF):** Protects web applications from attacks.
- **Data Loss Prevention (DLP):** Blocks data breaches and exfiltration.

- **Inline Malware Prevention:** Blocks unknown malware based on behavioral detection.


Figure 1: Overview of FortiGuard Security Services.

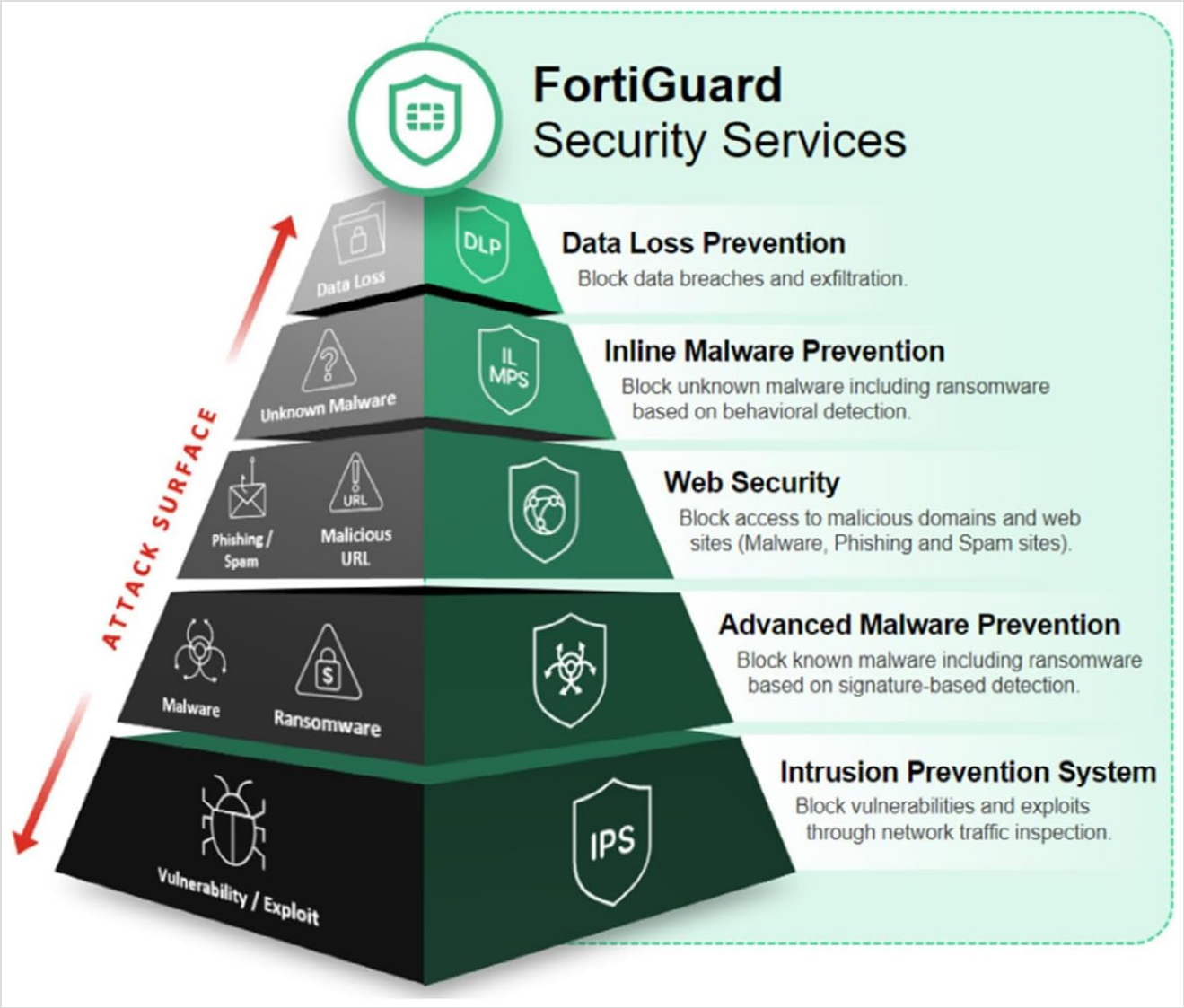


Figure 2: FortiGuard Security Services Attack Surface Protection.

## 3. Setup and Activation

The FortiGuard Unified Threat Protection is a subscription service designed for seamless integration with FortiGate firewalls. Activation typically involves applying the provided license key (FC-10-0051E-950-02-12) to your FortiGate-51E device through the Fortinet support portal or the FortiGate management interface.

### Activation Steps:

1. Ensure your FortiGate-51E is connected to the internet and has a valid FortiCloud account associated.
2. Log in to the Fortinet Support Portal (support.fortinet.com) with your credentials.
3. Navigate to the 'Asset Management' section and select your FortiGate-51E device.
4. Locate the option to 'Register Product' or 'Activate Services' and enter the provided FortiGuard license key (FC-10-0051E-950-02-12).
5. Follow the on-screen prompts to complete the activation. The FortiGuard services will then be synchronized with your FortiGate device.
6. Verify the activated services within your FortiGate-51E's management interface under the 'System' > 'FortiGuard' section.

No complex hardware configurations or additional installations are typically required for service activation, as it is a software-based subscription.

## 4. Operating the Services

Once activated, the FortiGuard UTP services operate continuously in the background, providing real-time threat intelligence and protection. Management and configuration of these services are performed directly through the FortiGate-51E's web-based management interface or FortiManager.

### Key Operational Aspects:

- **Policy Configuration:** Security policies on the FortiGate can be configured to leverage specific FortiGuard services (e.g., applying IPS profiles, web filtering profiles, application control policies to firewall rules).
- **Real-time Protection:** Services like IPS, Advanced Malware Protection, and URL/DNS Filtering actively inspect network traffic and block threats according to configured policies.
- **Reporting and Logging:** The FortiGate provides detailed logs and reports on detected threats, blocked attempts, and service usage, accessible via the FortiGate GUI or FortiAnalyzer.
- **Automated Updates:** FortiGuard services receive automated security updates from FortiGuard Labs, ensuring protection against the latest threats without manual intervention.

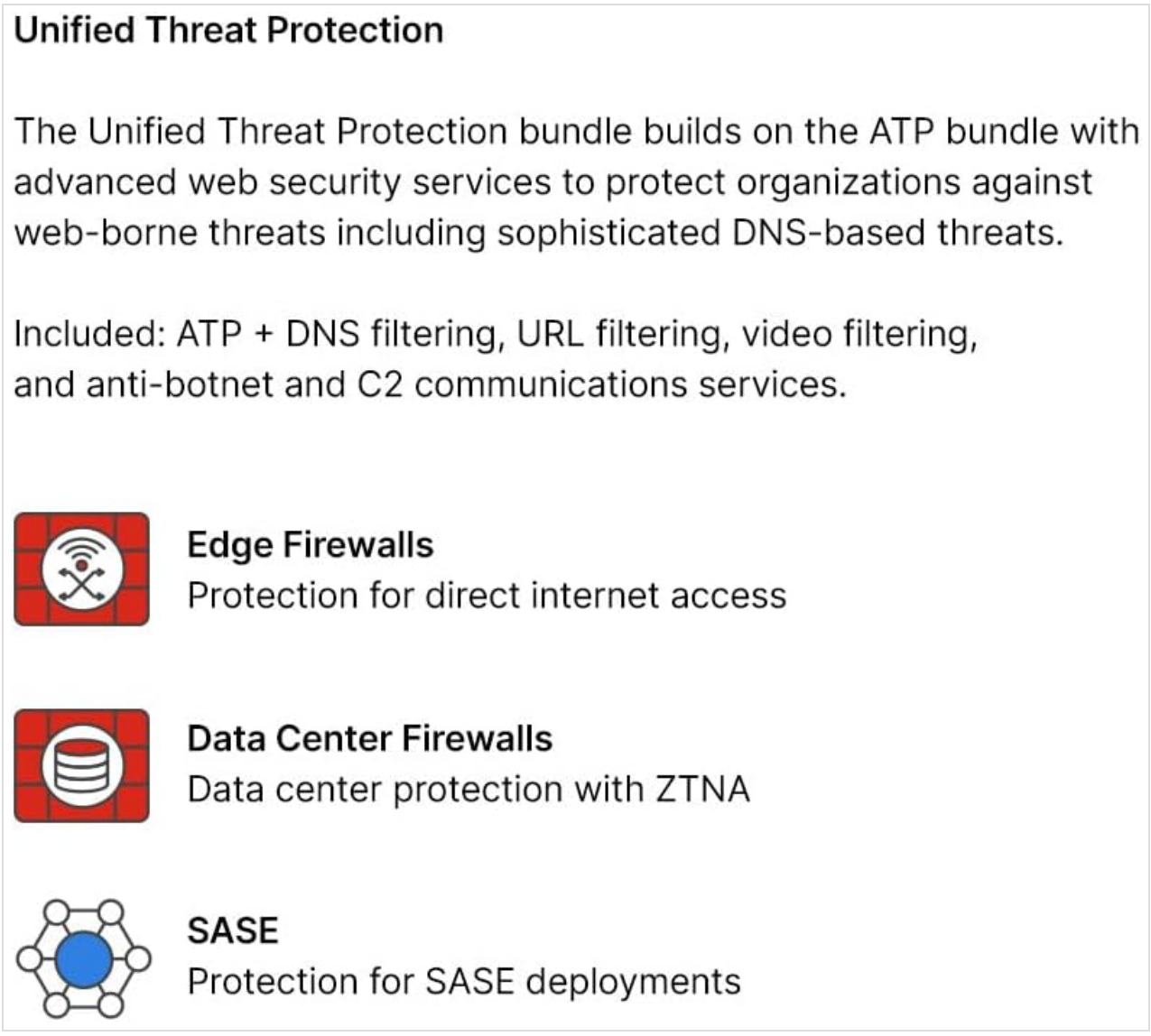


Figure 3: Unified Threat Protection Bundle Components.

## 5. Maintenance

FortiGuard services are designed for low maintenance, with most updates handled automatically by Fortinet's global threat intelligence network, FortiGuard Labs.

### Key Maintenance Activities:

- **Automated Security Updates:** FortiGuard services receive continuous, real-time updates for threat signatures, web filtering categories, and other intelligence to maintain up-to-date protection.
- **FortiGate Firmware Updates:** While FortiGuard services update independently, it is crucial to keep your FortiGate-51E's firmware updated to ensure compatibility and access to the latest security features and enhancements.
- **Policy Review:** Regularly review and adjust your FortiGate security policies to ensure they align with your organization's evolving security requirements and network usage patterns.
- **Monitoring:** Monitor FortiGate logs and reports for security events, performance metrics, and service status to identify and address potential issues proactively.

## 6. Troubleshooting

Should you encounter issues with your FortiGuard Unified Threat Protection services, consider the following troubleshooting steps:

- **Verify License Status:** Confirm that your FortiGuard UTP license is active and not expired on the Fortinet Support Portal and within your FortiGate-51E's management interface.
- **Check Network Connectivity:** Ensure your FortiGate-51E has stable internet connectivity to reach FortiGuard update servers.
- **Review FortiGate Logs:** Examine system and security logs on your FortiGate for error messages or indications of service failures.
- **Consult Fortinet Documentation:** Refer to the official Fortinet documentation and knowledge base for specific troubleshooting guides related to FortiGuard services and FortiGate devices.
- **Contact FortiCare Support:** If issues persist, contact FortiCare Premium Support for expert assistance. Refer to the 'Support' section for details.

## 7. Specifications

This section details the specific model and service duration for the FortiGuard Unified Threat Protection.

- **Product Model:** FC-10-0051E-950-02-12
- **Service Duration:** 1 Year
- **Associated Device:** FortiGate-51E
- **Included Bundles:** Unified Threat Protection (UTP)

## Subscriptions

| Service Category | Service Offering | A-la-carte | Bundles | | |
|---|---|---|---|---|---|
| | | | Enterprise Protection | Unified Threat Protection | Advanced Threat Protection |
| FortiGuard Security Services | IPS — IPS, Malicious/Botnet URLs | • | • | • | • |
| | Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct [3], AI-based Heurestic AV, FortiGate Cloud Sandbox | • | • | • | • |
| | URL, DNS and Video Filtering — URL, DNS and Video [3] Filtering, Malicious Certificate | • | • | • | |
| | Anti-Spam | | • | • | |
| | AI-based Inline Malware Prevention [3] | • | • | | |
| | Data Loss Prevention (DLP) [1] | • | • | | |
| | Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check | • | • | | |
| | OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS [1] | • | | | |
| | Application Control | | included with FortiCare Subscription | | |
| | Inline CASB [3] | | included with FortiCare Subscription | | |
| SD-WAN and SASE Services | SD-WAN Underlay Bandwidth and Quality Monitoring | • | | | |
| | SD-WAN Overlay-as-a-Service | • | | | |
| | SD-WAN Connector for FortiSASE Secure Private Access | • | | | |
| | SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth) [2] | • | | | |
| NOC and SOC Services | FortiConverter Service for one time configuration conversion | • | • | | |
| | Managed FortiGate Service—available 24×7, with Fortinet NOC experts performing device setup, network, and policy change management | • | | | |
| | FortiGate Cloud—Management, Analysis, and One Year Log Retention | • | | | |
| | FortiManager Cloud | • | | | |
| | FortiAnalyzer Cloud | • | | | |
| | FortiGuard SOCaaS—24×7 cloud-based managed log monitoring, incident triage, and SOC escalation service | • | | | |
| Hardware and Software Support | FortiCare Essentials [2] | • | | | |
| | FortiCare Premium | • | • | • | • |
| | FortiCare Elite | • | | | |
| Base Services | Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing | | included with FortiCare Subscription | | |

Figure 4: FortiGuard Subscription Bundles Comparison.

## 8. Support

The FortiGuard Unified Threat Protection bundle includes FortiCare Premium Support Services, ensuring you have access to expert assistance when needed.

### FortiCare Premium Support Services:

- **Availability:** 24x7x365 support via phone, chat, and web.
- **Response Times:** One-hour response times for Priority 1 and Priority 2 inquiries.
- **Firmware Upgrades:** Access to firmware upgrades.
- **Console Access:** Asset Management Portal.
- **RMA Support:** Return Merchandise Authorization (RMA) Replacement, eligible for Premium RMA Upgrade.

For most customers, FortiCare Premium provides the appropriate level of support for critical security needs.

| | FortiCare Premium (Included) | FortiCare Elite |
|---|---|---|
| **24×7 Support** | | |
| Telephone | ● | ● |
| Chat | ● | ● |
| Web | ● | ● |
| **Response** | | |
| P1 Inquiries | One Hour | 15 Minutes |
| P2 Inquiries | One Hour | 15 Minutes |
| P3 Inquiries | Next Business Day | Two Business Hours |
| P4 Inquiries | Two Business Days | Four Business Hours |
| **Firmware** | | |
| Firmware Upgrades | ● | ● |
| Long-Term Supported Firmware | | ● |
| **Console** | | |
| Asset Management Portal | ● | ● |
| FortiCare Elite Portal | | ● |
| **RMA Support (Appliances)** | | |
| Return Merchandise Authorization (RMA) Replacement | Advanced Replacement RMA (Eligible for Premium RMA Upgrade) | Advanced Replacement RMA (Eligible for Premium RMA Upgrade) |

### FortiCare Premium and FortiCare Elite

FortiCare Premium Support Services is included in all available bundles. FortiCare Premium provides 24×7×365 support (phone, chat, and web) with one-hour response times for Priority 1 and Priority 2 inquiries. For most customers, FortiCare Premium provides the right level of support.

For organizations with urgent or acute support needs, FortiCare Elite may be a stronger fit. With FortiCare Elite, customers receive 24×7×365 support with 15-minute response service-level agreements for Priority 1 and Priority 2 inquiries.

### Core Services Available with FortiCare

FortiGuard AI-Powered Security Bundles for FortiGate includes the following services as part of FortiCare Premium. The following is included with every bundle:

- Application control
- Inline CASB database
- Internet service (SaaS) database updates
- GeoIP database updates
- Device/OS detection signatures
- Trusted certificate database updates
- DDNS (v4/v6) service

Figure 5: FortiCare Premium vs. FortiCare Elite Support Comparison.