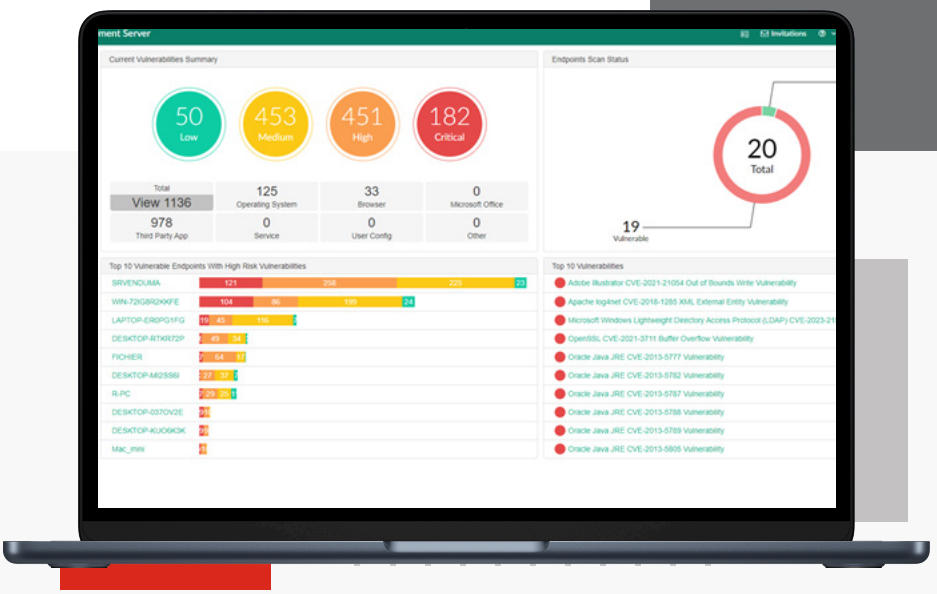
FortiEndpoint

The Fortinet Unified Agent



Highlights

- VPN/ZTNA Agent
- Vulnerability Assessment
- Sandboxing
- Device Control
- Endpoint Protection
- MITRE Tagging
- Threat Hunting
- Automated Response
- Advanced Forensics
- Extended Detection and Response (XDR)
- Cloud-based Management
- Managed Services

Gartner Peer Insights Customers' Choice 2024

AICPA SOC

Unified Agent for Secure Connectivity using ZTNA, Endpoint Protection, Extended Detection and Response

FortiEndpoint integrates with the Fortinet Security Fabric by combining FortiClient with multiple technologies including the power of FortiXDR into a single unified agent. It converges secure connectivity with advanced endpoint prevention, along with protection and response options to reduce the meantime to detect and repair without impact to your users.

Features

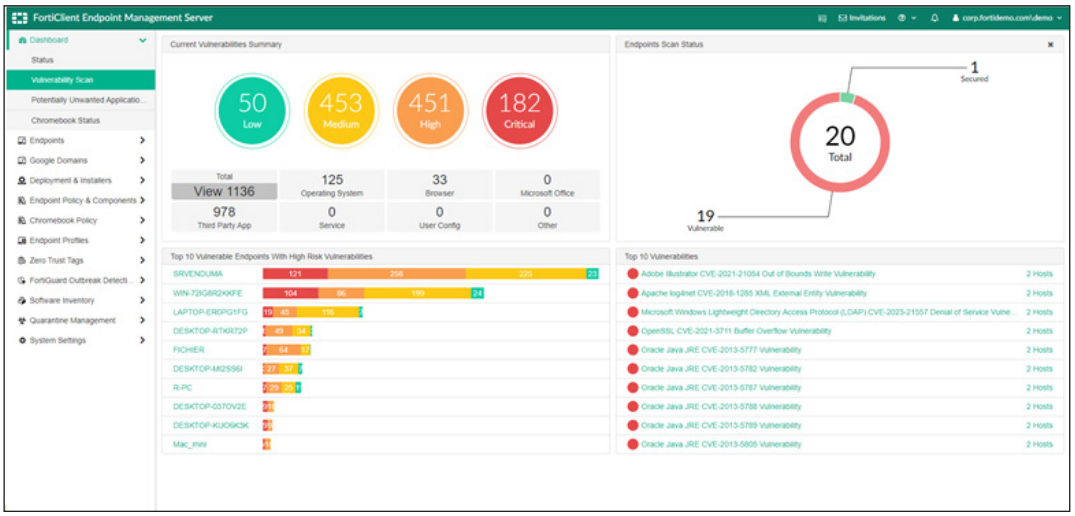
The unified agent provides Zero Trust Network Access based on the near real-time security posture of the endpoint. It leverages the endpoint posture and endpoint behavior to detect threats. The agent offers proactive attack surface reduction and behavior-based threat identification, effectively detecting and stopping advanced threats, including fileless malware. This approach ensures continuous protection, even for compromised and offline devices, while minimizing dwell time and maintaining robust security across all endpoints. The solution prevents data exfiltration, command and control (C2) communications, file tampering, and ransomware encryption. Seamlessly integrated with the Fortinet Security Fabric, it offers comprehensive visibility and compliance across all endpoints. Centralized management simplifies administration, enabling rapid vulnerability mitigation and robust defense for both remote and on-premises environments.

Available in

Hosted

Central Management Tools
Endpoint Management System (EMS)

- Simple and user-friendly UI
- ZTNA orchestration
- Real-time dashboard
- Software inventory management
- Active Directory (AD) and Azure AD integration
- Central quarantine management
- Automatic group assignment
- Dynamic access control
- Automatic email alerts
- Supports custom groups
- Remote actions
- Cloud-based management
- Zero trust tagging rules
- Security policy provisioning



Vulnerability Dashboard

Benefits

Security Fabric

Security Fabric Integration

The unified agent integrates seamlessly with Fortinet's Security Fabric, enhancing visibility and control across all endpoints while ensuring consistent enforcement of security policies. It includes Fabric agent capabilities that provide near real time endpoint visibility to FortiOS. The XDR capabilities can also automate a coordinated threat response across both the Security Fabric and third-party tools like firewalls, NAC, SIEM, NDR, and more in order to streamline operations and strengthening the organization's overall security posture. The XDR functionality taps into existing data lakes such as your SIEM or FortiAnalyzer without requiring replication which lowers the total cost of ownership of the solution.

Zero Trust Access

Universal ZTNA

Fortinet's Universal ZTNA works with FortiOS to enable secure granular access to applications no matter if the user is local or remote. Each session is initiated with an automatic, encrypted tunnel from the agent to the FortiOS ZTNA Application Gateway for user and device identity verification. In addition, it performs continuous near real-time endpoint posture checks that enables ZTNA application gateway to provide adaptive real-time access control based on dynamic endpoint posture validation. You can also use multi-factor authentication to provide an additional layer of security. With Universal ZTNA, organizations benefit from not only more secure and better remote access but in addition can offer consistent security and user experience for secure access to applications for on-premises and remote users regardless of endpoint location.

VPN

VPN

This agent provides flexible options for VPN connectivity. The split tunneling feature enables remote users on VPNs to access the Internet without their traffic having to pass through the corporate VPN headend, as in a typical VPN tunnel. This feature reduces latency, which improves user experience. At the same time, the agent includes protections to ensure that Internet-based transactions cannot backflow into the VPN connection and jeopardize the corporate network.

In addition to simple remote connectivity, it simplifies the remote user experience with features such as autoconnect and always-on VPN, as well as dynamic VPN gate selection. You can also use multifactor authentication to provide an additional layer of security.

Web Filtering

Web Filtering and SaaS Control

The agent provides on-client web and video filtering. This function provides phishing and botnet protection as well as granular application traffic control including web-based applications, YouTube, and software as a service (SaaS).

Benefits continued

Vulnerability Management

Vulnerability Detection and Patching

Since the unified agent scans endpoints for all applications, their versions, and vulnerabilities (CVEs), it shares that information for appropriate action. It proactively mitigates risks by allowing one to create granular virtual patching policies based on user/device groups, addressing vulnerabilities before they can be exploited. These vulnerabilities can also be managed by firewall and ZTNA policies, or by quarantining compromised endpoints to prevent further spread. This approach ensures that endpoints remain secure even if traditional patching is delayed, providing continuous protection across the ecosystem.

It further automates this process by identifying vulnerabilities and automatically applying patches across all managed devices. By continuously assessing and patching risks without user intervention, it minimizes the window of exposure and ensures timely protection even for remote endpoints, reducing the need for manual patch management.

Virtual Patching

Patch Policy Enforcement

Keeping endpoints up to date with the latest firmware can be difficult. The agent simplifies this task by managing endpoint patching, even when the endpoints are not on the network.

Malware

Malware and Exploit Prevention

The agent integrates Fortinet Cloud Sandboxing and FortiGuard global threat intelligence to enhance the onboard AI's real-time threat detection and decision-making. By consulting these included microservices, it refines alert classifications as more context becomes available. This dynamic approach allows for more accurate threat assessment, providing analysts with deeper insights or enabling automated responses through playbooks, ensuring continuous protection against evolving threats.

Ransomware

Ransomware Protection and Rollback

The unified agent provides patented technology that tracks real-time system changes in a non-production environment, allowing it to inspect for malicious activity before any changes are allowed to occur in the production environment. This proactive approach ensures that any suspicious modifications are identified and neutralized before they can affect critical systems. In the event of an infection, the agent can roll back ransomware encryption across Windows, macOS, and Linux systems, restoring the endpoint to its preinfected state and maintaining business continuity.

FortiGuard Security Services
www.fortiguard.com

FortiCare Worldwide 24/7 Support
support.fortinet.com

Services

FortiEndpoint Managed Services include: threat detection, hunting, remediation, and reporting

Managed Services

The managed service provides 24/7 threat monitoring, detection, and response by a globally located, 100% internal team of security experts. This service continuously monitors alerts, proactively hunts for threats, and takes action to protect your organization. The team leverages deep expertise in malware analysis, threat hunting, and incident handling, ensuring that all alerts are promptly addressed. In addition, the managed service offers incident response services as an add-on, providing expert support during critical security events. This comprehensive service reduces the burden on your security team, enhances threat detection capabilities, and ensures continuous protection against evolving threats. Please see the table at the end for management option tiers.

Access global knowledge of Fortinet customer best practices

Best Practice Service (BPS)

Best Practices Service is an account-based annual subscription available for all new customers. This service delivers guidance remotely via a specialized team that will assist with your deployment, upgrades, and ongoing operations. Customers share details about their deployment, user requirements, and resources, and the Best Practices team offers tailored recommendations, best practices, sample configurations, and links to useful tools.

Provide visibility, compliance, data security and threat protection

Fortinet CASB Service

To safely embrace the cloud, a Cloud Access Security Broker (CASB) can act as a gatekeeper by providing visibility, control, and protection to allow organizations to extend their security policies beyond their own infrastructure. CASB sits between cloud service users and secures SaaS cloud applications, monitors all activity, and enforces security policies. Fortinet's dual mode solution provides security, scalability, and performance using both inline and API-based CASB protections to address all cloud security needs. A unified agent license enables inline CASB services on a FortiGate and provides a license for FortiCASB, Fortinet's API-based CASB service.

Central management tools provide the ability to centrally manage Windows, macOS, and Linux endpoints

Feature Highlights

Central Management

The management of the solution give IT and Security Operations teams the following features.

Real-time Endpoint Status: Continuously monitors endpoint activity, including security events, compliance status, and potential vulnerabilities.

Vulnerability Dashboard: Identifies and prioritizes vulnerabilities, enabling IT teams to quickly address security risks.

Software Inventory Management: Keeps track of installed software and ensures endpoints are compliant and up to date.

Dynamic Access Control: Automates access control based on real-time endpoint security posture, integrating with firewall policies for dynamic enforcement.

Central Quarantine Management: Allows for the isolation of compromised endpoints to prevent the spread of threats within the network.

Device Discovery: Continuously scans the network to identify and monitor rogue or unmanaged devices, including IoT devices, ensuring that all assets are accounted for and secured.

Virtual Patching: Applies risk-based proactive policies to mitigate vulnerabilities through virtual patching, protecting critical systems even before traditional patches are deployed.

Forensics: Captures detailed endpoint activity and maintaining memory snapshots, allowing for full attack chain visibility through patented code tracing, and enabling security teams to accurately reconstruct and analyze security incidents.

Threat Hunting: Delivers advanced threat hunting capabilities with comprehensive attack-chain visibility, supported by MITRE ATT&CK framework tagging.

Integrated Response Playbooks and Automated Remediation: Combines customizable incident response playbooks with automated remediation to swiftly neutralize threats, reducing the need for manual intervention while maintaining system uptime.

By leveraging role-base access control (RBAC), organizations can ensure comprehensive and coordinated security management across all endpoints. IT teams can focus on compliance and policy enforcement, while SecOps teams manage advanced threat detection and response. This integrated approach streamlines security operations, reduces manual workloads, and significantly enhances the organization's overall security posture.

For a list of supported operating systems, please refer to:

https://docs.fortinet.com/document/fortiendpoint/latest/administration-guide/393635/product-integration-and-support

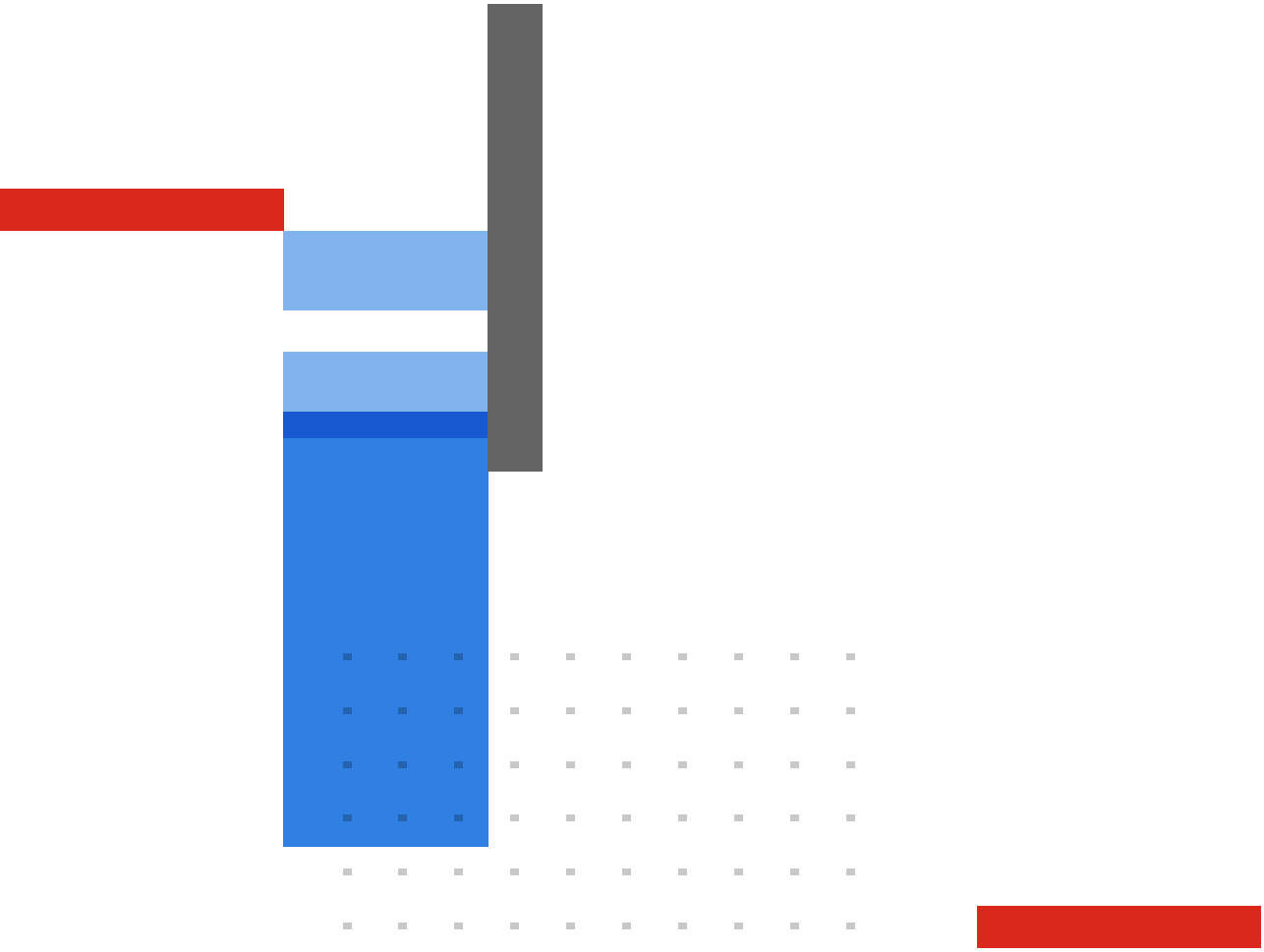
Order Information

MANAGED OPTIONS			
	PREVENT	EDR ESSENTIALS	XDR
24/7 Monitoring	✓	✓	✓
Vulnerability Monitoring	✓	✓	✓
Security Fabric Setup	✓	✓	✓
Group and Security Policy Provisioning	✓	✓	✓
Exception Building		✓	✓
Threat Hunting		✓	✓
Incident Handling		✓	✓
Reporting		✓	✓
Threat Detection			✓
Extended Detection and Response			✓

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

June 2, 2025

FEP-DAT-R03-20250602