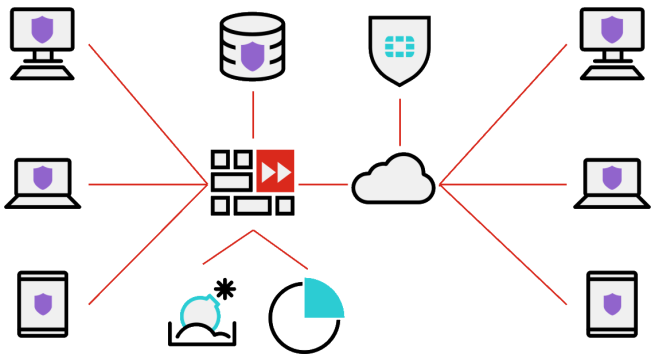
# Lumen® SASE Solutions with Fortinet FortiClient 7.0

Endpoint agent for visibility and control, endpoint protection, and secure remote access using VPN and Zero Trust technologies



FortiClient's Fortinet Security Fabric integration provides endpoint visibility through telemetry and ensures that all Security Fabric components – FortiGate, FortiAnalyzer, EMS, managed APs, managed Switches, and FortiSandbox –have a unified view of endpoints in order to provide tracking and awareness, compliance enforcement, and reporting. Traditional virtual private network (VPN) tunnels or new, automatic ZTNA tunnels provide secure remote connectivity. Provide security and protection for endpoints when local or remote.

### Central Management Tools

- Simple and user-friendly UI
- Remote FortiClient deployment
- Real-time dashboard
- Software inventory management
- Active Directory (AD) integration
- Central quarantine management
- Automatic group assignment
- Dynamic access control
- Automatic email alerts
- Supports custom groups
- Remote triggers
- On-premise and cloud-based options

Unified Endpoint features including compliance, protection, and secure access into a single modular lightweight client.

Zero Trust Applied, with automatic, encrypted tunnels for controlled validated per-session access to applications.

Advanced Threat Protection against exploits and advanced malware, powered by FortiGuard along with FortiSandbox integration.

Simplified Management and Policy Enforcement with FortiClient EMS, FortiClient Cloud, and FortiGate.

# Benefits

FortiClient integrates the endpoints into Fortinet's Security Fabric for early detection and prevention of advanced threats. This integration delivers native endpoint visibility, compliance control, vulnerability management, and automation. FortiOS and FortiAnalyzer leverage FortiClient endpoint telemetry intelligence to identify indicators of compromise. With the automation capability, administrators can investigate in real time and set policies to automate responses, including quarantining suspicious or compromised endpoints to contain incidents and stem outbreaks. Fortinet's endpoint compliance and vulnerability management features simplify the enforcement of enterprise security policies preventing endpoints from becoming easy attack targets.

### Web Filtering and SAAS Control

FortiClient provides remote web filtering, delivering web security and content filtering. The web application firewall provides botnet protection and granular application traffic control including web-based applications and software as a service (SaaS).

### ZTNA

FortiClient 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 FortiClient to the FortiOS proxy point for user and device verification. If verified, access is granted for that session.

### Endpoint Hygiene

FortiClient helps organizations reduce their attack surface with vulnerability scanning and optional autopatching. Combined with zero trust access principles, this approach can enhance an organization's hygiene and security posture.

### Malware and Exploit Prevention

By integrating with FortiClient Cloud Sandbox and leveraging FortiGuard global threat intelligence, FortiClient prevents advanced malware and vulnerabilities from being exploited.

FortiClient integrates with FortiClient Cloud Sandbox to analyze all files downloaded to FortiClient endpoints in real time. Millions of FortiClient and FortiSandbox users worldwide share information about known and unknown malware with the cloud-based FortiGuard threat intelligence platform. FortiGuard automatically shares the intelligence with FortiClient endpoints to protect against emerging threats.

### VPN

FortiClient provides flexible options for VPN connectivity. It supports both secure sockets layer (SSL) and Internet Protocol security (IPsec) VPN. The split tunneling feature enables remote users on SSL VPNs to access the Internet without their traffic having to pass through the corporate VPN headend, as in a typical SSL VPN tunnel. This feature reduces latency, which improves user experience. At the same time, FortiClient 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, FortiClient 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.

### Ransomware Protection

Ransomware attacks have increased recently. In response, FortiClient has introduced new ransomware protection, with the ability to roll back changes made by malicious programs, putting the endpoint back to a preinfection state.

### Flexible Licensing

The benefits of FortiClient are available through either the traditional device-based licensing or the new user-based FortiTrust licensing. Both options offer the same functionality and allow customers to decide how they want to subscribe to benefits of FortiClient.

## Services

### FortiClient Managed Services

To assist and offload busy IT teams, Fortinet is offering FortiClient Managed services to streamline the configuration, deployment, and monitoring of FortiClient agents. Services included with this offering include the following:

- **Initial FortiClient Cloud provisioning:** The managed services team works with customers to set up and configure their FortiClient Cloud environment for the following capabilities.
    - Endpoint groups setup
    - ZTNA
    - VPN
    - Endpoint security
    - Vulnerability management
    - Security profiles and policies configuration
    - Endpoint posture check rules
    - Custom FortiClient installer creation and ongoing installer updates
- **Endpoint onboarding:** The managed services team creates customer FortiClient installers for customer-specific use cases, sends invitation emails to users, and onboards them for FortiClient Cloud management and provisioning.
- **Security Fabric setup and integration:** The managed services team integrates FortiClient Cloud with the Fortinet Security Fabric to support uses cases such as ZTNA, incidence response, and automation.
- **Endpoint vulnerability monitoring:** The managed services team monitors customer endpoints to identify high risk endpoints and alert them of endpoints with critical and high vulnerabilities that would be easy targets for cyber attacks. The managed services team detects, reports, and guides customers to remediate those vulnerable endpoints.

### Best Practice Service (BPS)

FortiClient Best Practices Service is an account-based annual subscription providing access to a specialized team that delivers remote guidance on deployment, upgrades, and operations. The service allows customers to share information about their deployment, user requirements, resources, and other related items. Based on the information provided,

the BPS experts can provide recommended best practices, sample code, links to tools, and other materials or assistance to speed adoption and guide the customer towards best practice deployments. The team does not log into customer devices to make changes for them. This is a consulting and guidance service which may include sample configurations or playbooks. This is not an on-site professional services offer.

### FortiClient Forensics Analysis Service

FortiClientForensic Service provides analysis to help endpoint customers respond to and recover from cyber incidents.

For each engagement, forensic analysts from Fortinet's FortiGuard Labs will assist in the collection, examination, and presentation of digital evidence, including a final, detailed report. FortiClient subscriptions that include Forensic Services entitle the customer to call on these endpoint forensic experts whenever an event happens, offloading internal teams and accelerating investigations by analysts deeply familiar with the tools of endpoint security.

## Feature highlights

Central management tools provide the ability to centrally manage Windows, macOS, Linux, Chrome, iOS, and Android endpoints. FortiClient EMS provides on-premise management and FortiClient Cloud provides cloud-based management.

FortiGate provides awareness and control over all your endpoints.

**Software Inventory Management** provides visibility into installed software applications and license management to improve security hygiene. You can use inventory information to detect and remove unnecessary or outdated applications that might have vulnerabilities to reduce your attack surface.

**Windows AD Integration** helps sync organizations' AD structure into the central management tools so that you use the same organizational units from your AD server for simplified endpoint management.

**Real-time Endpoint Status** always provides current information on endpoint activity and security events.

**Vulnerability Dashboard** helps manage organizations attack surface. All vulnerable endpoints are easily identified for administrative action.

**Centralized FortiClient Deployment and Provisioning** that allows administrators to remotely deploy endpoint software and perform controlled upgrades. Makes deploying FortiClient configuration to thousands of clients an effortless task with a click of a button.

**FortiSandbox integrations** assist with configuration and suspicious file analysis. Sandbox settings are synchronized across managed endpoints, simplifying setup. A detailed analysis of FortiClient submitted files is available in the central management tools. Administrators can see all the behavior activity of a file, including graphic visualization of the full process tree.

**Telemetry** provides real-time endpoint visibility (including user avatar) on FortiGate console so administrators can get a comprehensive view of the whole network. Telemetry also ensures that all fabric components have a unified view of the endpoints.

**Dynamic Access Control for Compliance Enforcement** requires EMS to create virtual groups based on endpoint security posture. These virtual groups are then retrieved by FortiGate and used in firewall policy for dynamic access control. Dynamic groups help automate and simplify compliance to security policies.

**Endpoint Quarantine** helps to quickly disconnect a compromised endpoint from the network and stop it from infecting other assets.

**Automated Response** helps detect and isolate suspicious or compromised endpoints without manual intervention.

**Application-based Split Tunnel** supports source application- based split tunnel, where you can specify application traffic to exclude from the VPN tunnel, such as high bandwidth apps.

**Web Filtering with Keyword Search / YouTube Filters** blocks web pages containing words or patterns that you specify as well as limit users' access by blocking or only allowing specified YouTube channels.

LUMEN®

FORTINET®

# Bundles

| FORTICLIENT EDITION | VPN / ZTNA | EPP / APT | MANAGED SERVICES | CHROMEBOOK |
|---|---|---|---|---|
| **Zero Trust Security** | Windows, macOS, Linux | Windows, macOS, Linux | Windows, macOS, Linux | Chromebook |
| **Zero Trust Agent with MFA** | ✔ | ✔ | ✔ | |
| **Central Management via EMS or FortiClient Cloud** | ✔ | ✔ | ✔ | ✔ |
| **Central Logging and Reporting** | ✔ | ✔ | ✔ | ✔ |
| **Dynamic Security Fabric Connector** | ✔ | ✔ | ✔ | |
| **Vulnerability Agent and Remediation** | ✔ | ✔ | ✔ | |
| **SSL VPN with MFA** | ✔ | ✔ | ✔ | |
| **IPSEC VPN with MFA** | ✔ | ✔ | ✔ | |
| **FortiGuard Web Filtering** | ✔ | ✔ | ✔ | ✔ |
| **Integration with FortiSandbox (on-Premise or PaaS)** | ✔ | ✔ | ✔ | ✔ |
| **Next Generation Endpoint Security** | | | | |
| **AI powered NGAV** | | ✔ | ✔ | |
| **FortiClient Cloud Sandbox1** | | ✔ | ✔ | |
| **Removable Media Control** | | ✔ | ✔ | |
| **Automated Endpoint Quarantine** | | ✔ | ✔ | |
| **Application Firewall[1]** | | ✔ | ✔ | |
| **Software Inventory** | | ✔ | ✔ | |
| **Ransomware Protection[2]** | | ✔ | ✔ | |
| **Additional Services** | | | | |
| **Best Practice Service (BPS) Consultation** | Account add-on | Account add-on | N/A | Account add-on |
| **24x7 Support** | ✔ | ✔ | ✔ | ✔ |
| **On-Premise/Air Gap Option** | ✔ | ✔ | | ✔ |
| **FortiGuard Forensics Analysis Service Option** | Account add-on | Account add-on | Account add-on | Account add-on |

1. FortiClient (Linux) does not support this feature.
2. Only FortiClient (Windows) supports this feature.

CERTIFIED

NSS LABS RECOMMENDED

AV comparatives

vb 100 VIRUS virusbtn.com

# Features per platform and requirements

| Zero Trust Security | WINDOWS | MACOS | ANDROID | IOS | CHROMEBOOK | LINUX |
|---|---|---|---|---|---|---|
| Endpoint Telemetry[1] | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Compliance Enforcement Using Dynamic Access Control[1] | ✔ | ✔ | ✔ | ✔ | | ✔ |
| Endpoint Audit and Remediation with Vulnerability Scanning | ✔ | ✔ | | | | ✔ |
| Remote Logging and Reporting[2] | ✔ | ✔ | | ✔ | ✔ | ✔ |
| IPSec VPN | ✔ | ✔ | ✔ | | | |
| SSL VPN3 | ✔ | ✔ | ✔ | ✔ | | ✔ |
| ZTNA Remote Access | ✔ | ✔ | | | | ✔ |
| Windows AD SSO Agent | ✔ | ✔ | | | | |
| Removable Media Control | ✔ | ✔ | | | | ✔ |
| **Endpoint Security** | | | | | | |
| Antivirus | ✔ | ✔ | ✔ | | | ✔ |
| Cloud-based Threat Detection | ✔ | ✔ | ✔ | | | |
| Sandbox integration (on-premise) | ✔ | ✔ | ✔ | | | ✔[4] |
| Sandbox integration (cloud-based) | ✔ | ✔ | ✔ | | | |
| Automated Endpoint Quarantine | ✔ | ✔ | ✔ | | | |
| Web Filter[5] | ✔ | ✔ | ✔ | ✔ | ✔ | |
| AntiExploit | ✔ | | | | | |
| Application Firewall | ✔ | ✔ | | | | |
| FortiClient Forensic Analysis | ✔ | ✔ | | | | ✔ |

**PLUS - Add Sandbox Cloud subcription for Proactive Advanced Threat Detection.** [1]

Requires EMS or FortiClient Cloud to centrally manage FortiClient.

[2] Requires FortiAnalyzer.

[3] Also compatible with Windows mobile.

[4] No file submission.

[5] Also compatible with Chrome OS.

The above list is based on the latest OS for each platform.

| FORTICLIENT |
|---|
| **Supported Operating Systems*** |
| Microsoft Windows 7 (32-bit and 64-bit) Microsoft |
| Windows 8, 8.1 (32-bit and 64-bit) Microsoft |
| Windows 10 (32-bit and 64-bit) |
| Microsoft Windows 11 (64-bit) |
| Microsoft Windows Server 2012 or later |
| macOS 11+, 10.15, 10.14 |
| iOS 9.0 or later |
| Android 5.0 or later |
| Linux Ubuntu 16.04 and later, Red Hat 7.4 and later, CentOS 7.4 and later with KDE or GNOME |
| **Authentication Options** |
| RADIUS, LDAP, local database, xAuth, TACACS+, digital certificate (X509 format), FortiToken |
| **Connection Options** |
| Autoconnect VPN before Windows logon |
| IKE mode configuration for FortiClient IPsec VPN tunnel |

| FORTICLIENT EMS |
|---|
| **Supported Operating Systems** |
| Microsoft Windows Server 2012 or later |
| **Endpoint Requirement** |
| FortiClient 6.4 or later, FortiClient for Windows and macOS X, 6.4 for iOS and Android |
| **System Requirements** |
| 2.0 GHz 64-bit processor, six virtual CPUs, 8 GB RAM, 40 GB free hard disk, Gigabit (10/100/1000BaseT) |
| Ethernet adapter, Internet access |