TWO DECADES OF SECURITY-DRIVEN NETWORKING
Overview
Fortinet’s mission is to deliver the most innovative, highest-performing network security fabric to secure and simplify your IT infrastructure. We are a leading global provider of network security and SD-WAN, switching and wireless access, network access control, authentication, public and private cloud security, endpoint security, and AI-driven advanced threat protection solutions for carriers, data centers, enterprises, and distributed offices.

Share Price Performance

<table>
<thead>
<tr>
<th>FTNT Rank</th>
<th>1-year</th>
<th>3-year</th>
<th>5-year</th>
<th>Since IPO*</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTNT</td>
<td>53%</td>
<td>229%</td>
<td>177%</td>
<td>1785%</td>
</tr>
<tr>
<td>CHKP</td>
<td>10%</td>
<td>6%</td>
<td>52%</td>
<td>263%</td>
</tr>
<tr>
<td>PANW</td>
<td>20%</td>
<td>70%</td>
<td>42%</td>
<td>483%</td>
</tr>
</tbody>
</table>


* FTNT IPO on 11/18/2009 at $6.25 (split adjusted); PANW IPO on 7/20/2012 at $42. CHKP performance from FTNT IPO date.

Steadily Improved Operating Margins
Non-GAAP Operating Margin - Trailing Four Quarter Average

Q3 2020 Financial Spotlight:
Secure SD-WAN billings more than doubled year-over-year in the quarter and represented over 10% of total billings
#1 CYBERSECURITY COMPANY IN THE WORLD

**#1 Most Deployed Network Security**
- ~30% of all FW/UTM appliance shipments
  
  Source: IDC Worldwide Security Appliance Tracker, April 2020 (based on annual unit shipments of Firewall, UTM and VPN appliances)

**#1 Network Security Innovator**
- 3X more patents than comparable Network Security companies
  
  Source: US Patent Office, As of October 9, 2020

**#1 Broadiest Security Protection**
- From IoT to the Cloud
  
  Source: Fortinet estimates based on recent analyst research, 2024 opportunity shown.

**#1 Most 3rd Party Validations**
- NSS Labs, ICSA, VB and more
  
  Source: NSS Labs most recent test results, as of July 2020. See pages 10 and 11 for more details.

**The Only Company to Excel at All Key Stages of Network Security**
Today’s perimeter is no longer easily defined. The data center was once your network’s primary point of entry and exit, but now an explosion of new connected devices, 5G, and hyperscale cloud deployments have expanded the perimeter across the entire infrastructure.

First-generation network security (stateful firewalls) focused on securing the connection, and, led by Fortinet, a second generation of network security (next-generation firewalls and UTMs) expanded inspection to the application and content. However, in order to secure today’s digital innovations and the rapidly expanding and evolving perimeter, a third generation of network security is required: a broad, integrated, and automated security platform that provides end-to-end segmentation and protection for your data, users, and infrastructure everywhere.
The Fortinet Security Fabric

Third-Generation Network Security
Fortinet is once again leading the way with its Security Fabric, the first open architectural approach to security that dynamically adapts to and secures the evolving IT infrastructure.

Broad
visibility of the entire digital attack surface to better manage risk

Integrated
solution that reduces the complexity of supporting multiple point products

Automated
workflows to increase speed of operations and response

Complete protection across the digital attack surface

FortiGate
FortiSASE
FortiNAC
FortiAP
FortiSwitch
FortiExtender
FortiManager
FortiClient
FortiAnalyzer
FortiCASB
FortiSIEM
FortiSASE
FortiCWP
FortiMail
FortiEDR
FortiSandbox
FortiGate Cloud
FortiADC
FortiCloud
Our latest high-performance NGFW that enables fast exchange of AI-driven business insights, large securely connected remote workforces, segmentation, full visibility of encrypted traffic, and threat protection.

### Chassis-based  5000 & 7000 Series

<table>
<thead>
<tr>
<th>Feature / Performance</th>
<th>FortiGate 2600F</th>
<th>FortiGate 5144C</th>
<th>FortiGate 7060E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>Expandable, modular chassis</td>
<td>2RU – 5RU appliance</td>
<td>2RU – 5RU appliance</td>
</tr>
<tr>
<td>Interfaces</td>
<td>10, 40, and 100 GE</td>
<td>10, 25, 40, and 100 GE</td>
<td>10, 25, 40, and 100 GE</td>
</tr>
<tr>
<td>FW(TP) Throughput</td>
<td>More than 1 Tbps (Up to 189 Gbps)</td>
<td>52 Gbps – 1.2 Tbps (4 Gbps – 100 Gbps)</td>
<td>7 Gbps – 36 Gbps (1 Gbps – 7 Gbps)</td>
</tr>
<tr>
<td>Special Features</td>
<td>Carrier class, NEBS, fully redundant</td>
<td>Ultra-low latency, ultra high-speed SSL inspection</td>
<td>High-speed SSL inspection</td>
</tr>
</tbody>
</table>

### High-end Appliance  1000 – 4000 & 6000 Series

<table>
<thead>
<tr>
<th>Feature / Performance</th>
<th>FortiGate 6500F</th>
<th>FortiGate 2200E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>2RU – 5RU appliance</td>
<td>2RU – 5RU appliance</td>
</tr>
<tr>
<td>Interfaces</td>
<td>10, 25, 40, and 100 GE</td>
<td>10, 25, 40, and 100 GE</td>
</tr>
<tr>
<td>FW(TP) Throughput</td>
<td>52 Gbps – 1.2 Tbps (4 Gbps – 100 Gbps)</td>
<td>7 Gbps – 36 Gbps (1 Gbps – 7 Gbps)</td>
</tr>
<tr>
<td>Special Features</td>
<td>Ultra-low latency, ultra high-speed SSL inspection</td>
<td>High-speed SSL inspection</td>
</tr>
</tbody>
</table>

### Mid-range Appliance  100 – 900 Series

<table>
<thead>
<tr>
<th>Feature / Performance</th>
<th>FortiGate 600E</th>
<th>FortiGate 400E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>1RU – 2RU appliance</td>
<td>1RU – 2RU appliance</td>
</tr>
<tr>
<td>Interfaces</td>
<td>1 and 10 GE</td>
<td>1 and 10 GE</td>
</tr>
<tr>
<td>FW(TP) Throughput</td>
<td>7 Gbps – 36 Gbps (1 Gbps – 7 Gbps)</td>
<td>1 – 4 Gbps (150 Mbps – 700 Mbps)</td>
</tr>
<tr>
<td>Special Features</td>
<td>High-speed SSL inspection</td>
<td>Wi-Fi, PoE, ruggedized</td>
</tr>
</tbody>
</table>

### Entry-level Appliance  30–90 Series

<table>
<thead>
<tr>
<th>Feature / Performance</th>
<th>FortiGate 40F</th>
<th>FortiGate 50F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>Desktop</td>
<td>1RU – 2RU appliance</td>
</tr>
<tr>
<td>Interfaces</td>
<td>High-density 1 GE</td>
<td>10, 25, 40, and 100 GE</td>
</tr>
<tr>
<td>FW(TP) Throughput</td>
<td>1 – 4 Gbps (150 Mbps – 700 Mbps)</td>
<td>7 Gbps – 36 Gbps (1 Gbps – 7 Gbps)</td>
</tr>
<tr>
<td>Special Features</td>
<td>Wi-Fi, PoE, ruggedized</td>
<td>High-speed SSL inspection</td>
</tr>
</tbody>
</table>

### Virtual/Cloud Firewall

<table>
<thead>
<tr>
<th>Feature / Performance</th>
<th>Private Cloud</th>
<th>Public Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Cases &amp; Integrations</td>
<td>All major hypervisors</td>
<td>AWS, Azure, Google, Oracle, IBM, Alibaba</td>
</tr>
<tr>
<td>Throughput</td>
<td>Hardware dependent</td>
<td>Cloud dependent</td>
</tr>
<tr>
<td>Licensing</td>
<td>Perpetual, subscription, metered</td>
<td>BYOL or on-demand</td>
</tr>
</tbody>
</table>

---

**New Product Spotlight—FortiGate 2600F**

Our latest high-performance NGFW that enables fast exchange of AI-driven business insights, large securely connected remote workforces, segmentation, full visibility of encrypted traffic, and threat protection.

<table>
<thead>
<tr>
<th>Feature / Performance</th>
<th>FortiGate 2600F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>198 Gbps</td>
</tr>
<tr>
<td>Concurrent Sessions</td>
<td>24 Million</td>
</tr>
<tr>
<td>Connections Per Second</td>
<td>900,000</td>
</tr>
<tr>
<td>IPsec VPN</td>
<td>55 Gbps</td>
</tr>
<tr>
<td>SSL Inspection</td>
<td>20 Gbps</td>
</tr>
<tr>
<td>Interfaces</td>
<td>1G, 10G, 25G, 40G, 100G</td>
</tr>
</tbody>
</table>

---

1. Target performance metrics. Final performance metrics are subject to change.
2. An Elephant flow is a single session that consumes a large amount of bandwidth.

- High performance and secure 100 Gbps elephant flows
- Hardware assisted resiliency with DDoS prevention
- Hardware accelerated VXLAN segmentation & protection
- Industry’s best price/performance for Threat Protection, SSL Inspection, and Crypto VPN
FortiOS is the foundation of the Fortinet Security Fabric, consolidating many technologies and use cases into a simplified, single policy and management framework. FortiOS provides customers with superior protection, deeper visibility and control, reduced complexity, and greater operational efficiency across their entire attack surface.

The Security Processor Advantage

Fortinet Security Processors engineered for radically increasing the speed, scale, performance, efficiency and value of Fortinet solutions while greatly improving user experience, reducing footprint, and lowering power requirements. The Security Compute Rating is a benchmark that compares the performance of Fortinet’s purpose-built ASIC-based next-generation firewall (NGFW) appliance to other NGFW and SD-WAN vendors - in the same price range - that utilize generic processors for networking and security. The FortiGate 2600F series, powered by Fortinet’s NP7 security processor, enables superior Security Compute Ratings as noted in the chart below.

<table>
<thead>
<tr>
<th>Specification</th>
<th>FortiGate 2600F</th>
<th>Industry Average</th>
<th>Security Compute Rating</th>
<th>Palo Alto Networks PA-5220</th>
<th>Check Point CP28000</th>
<th>Cisco FPR-4145</th>
<th>Juniper SRX540</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>198 Gbps</td>
<td>29 Gbps</td>
<td>7x</td>
<td>N/A</td>
<td>26 Gbps</td>
<td>20 Gbps</td>
<td>40 Gbps</td>
</tr>
<tr>
<td>IPsec VPN</td>
<td>56 Gbps</td>
<td>5.9 Gbps</td>
<td>9x</td>
<td>11 Gbps</td>
<td>4.61 Gbps</td>
<td>3.2 Gbps</td>
<td>5 Gbps</td>
</tr>
<tr>
<td>Threat Protection</td>
<td>20 Gbps</td>
<td>7.9 Gbps</td>
<td>2.5x</td>
<td>10 Gbps</td>
<td>5.8 Gbps</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>SSL Inspection</td>
<td>20 Gbps</td>
<td>1.7 Gbps</td>
<td>10x</td>
<td>1.9 Gbps</td>
<td>N/A</td>
<td>1.4 Gbps</td>
<td>N/A</td>
</tr>
<tr>
<td>Concurrent Sessions</td>
<td>24 M</td>
<td>3.5 M</td>
<td>7x</td>
<td>4 M</td>
<td>2 M</td>
<td>3 M</td>
<td>5 M</td>
</tr>
<tr>
<td>Connections Per Second</td>
<td>900 K</td>
<td>167 K</td>
<td>5x</td>
<td>180 K</td>
<td>164 K</td>
<td>75 K</td>
<td>250 K</td>
</tr>
</tbody>
</table>

Sources: Fortinet data from internal tests. Competitor data from public datasheets. PA-5220 SSL Inspection from NSS Labs 2019 NGFW Performance Comparative Report

The FortiGuard Threat Intelligence Advantage

Our FortiGuard Labs threat research team develops the threat intelligence that informs all of our solutions. FortiGuard Labs leverages leading-edge machine learning and AI technologies to provide consistently top-rated protection and actionable threat intelligence that protect and inform our customers worldwide. FortiGuard Labs partners with law enforcement agencies, government organizations, and security vendor alliances, taking a leadership role to ensure the industry is effectively responding to emerging security risks worldwide.

Bundled and A La Carte Offerings

<table>
<thead>
<tr>
<th>Bundled and A La Carte Offerings</th>
<th>Application Control</th>
<th>IPS</th>
<th>Advanced Malware Protection</th>
<th>Antivirus</th>
<th>Web Filtering</th>
<th>Industrial</th>
<th>AI Security</th>
<th>Security Rating Service</th>
<th>FortiConverter Service</th>
<th>Advanced Support Engagement</th>
<th>FortiManager Cloud</th>
<th>FortiAnalyzer Cloud</th>
<th>SD-WAN Orchestrator</th>
<th>SD-WAN Chassis-As-A-Service</th>
<th>Patrick Management</th>
<th>FortiGuard Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>360 Protection Bundle</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Enterprise Protection bundle</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Unified Threat Protection bundle</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Adv. Threat Protection bundle</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>A la carte services</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

FortiGuard subscription services | Operational & SD-WAN services

*Per many independent third-party tests. See pages 10-11 for more. ** Includes AV, Antivirus, Mobile Security, Cloud Sandbox, Content Disarm and Reconstruction, and Virus Outbreak Protection. The 360 Protection Bundle also includes upgraded Advanced Support Engagement (ASE) 24x7 support. Other bundles include standard 24x7 support.
Extensive Industry Cybersecurity Ecosystem

420+ Open Fabric Ecosystem Integrations

**Fabric Connectors (13)**
Fortinet-developed deep integrations that automate security operations and policies

![Fabric Connectors](logo.png)

**Fabric APIs (198)**
Partner-developed integrations using Fabric APIs that provide broad visibility with end-to-end solutions

![Fabric APIs](logo.png)

**Fabric DevOps (10)**
Community-driven DevOps scripts that automate network and security provisioning, configuration, and orchestration

![Fabric DevOps](logo.png)

**Extended Security Fabric Ecosystem (200+)**
Collaboration with threat sharing organizations and integrations with other vendor products

![Extended Security Fabric Ecosystem](logo.png)

Fortinet Corporate Social Responsibility

**Environment**
Environmental sustainability is a top Fortinet priority, including energy-efficient products and green workplace initiatives. We and our supply chain partners also meet the most stringent requirements around environmentally-friendly products, packaging, and recycling.

**Business & Innovation**
Fortinet’s mission is to innovate and develop the best technology to protect individuals and organizations, help ensure digital privacy, and protect customers from security breaches. As a leader in broadly-available cybersecurity training, we also help educate individuals to improve their career opportunities as well as help protect our customers, while doing our part to close the cybersecurity skills gap.

**Governance & Ethics**
Fortinet is committed to doing business ethically and in compliance with all laws. Our corporate governance practices provide review, oversight, and guidance to leadership, with a goal of ensuring accountability to meet our responsibilities to drive long-term value for our stockholders and meet our responsibilities to all of our other stakeholders.

**People and Communities**
Fortinet is building a diverse, inclusive, fair and safe workplace, a true meritocracy, to empower individuals to reach their full potential. We also support global communities through our philanthropic foundation, contribution matching, employee service days, and outreach services.

Our Response to COVID-19
Fortinet is committed to protecting the health and well-being of our employees, supporting communities, and working with our customers and partners to help maintain operations during this challenging time. Some of our actions include:

**Employees:** remote telework policies, proper social distancing measures, preventative sanitation measures, and more

**Cybersecurity Training:** free online security training for our partners, customers and communities to help protect our end users, empower our ecosystem with security skills, and narrow the security skills gap

**Customers and partners:** innovative, scalable built-in remote worker capabilities to ensure rapid protection for business continuity and secure remote working

**Charitable Commitment:** increased Fortinet’s employee charitable contribution matching program to $2M for non-profit organizations fighting COVID-19

To learn more, visit our [website](https://www.fortinet.com).
Extensive Industry Cybersecurity Ecosystem

SECURITY ASSOCIATE
Develop a foundational understanding of the ever-changing threat landscape and general network security concepts.

SECURITY ASSOCIATE
Sales training for Fortinet employees and channel partners only.

Discover the types of security products that have been developed to address the threat landscape that was explored in NSE 1.

PROFESSIONAL
Develop the knowledge required to manage the day-to-day configuration, monitoring, and operation of FortiGate devices to support corporate network security policies.

ANALYST
Develop a detailed understanding of how to implement network security management and analytics.

SPECIALIST
Develop an understanding of the Security Fabric products that augment FortiGate, providing deeper and more comprehensive network security.

ARCHITECT
Develop the knowledge required to integrate Fortinet products into network security solution deployment and administration.

EXPERT
Demonstrate the ability to design, configure, install, and troubleshoot a comprehensive network security solution in a live environment.

Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East, and Asia, FortiCare offers services to meet the needs of enterprises of all sizes.

SECURITIES & SUPPORT SPOTLIGHT

360 Protection is a new support and service package that delivers advanced support, real-time network management, and a full suite of security and operational services.

FortiCare
- 24x7 FortiCare - Advanced Support engagement level

FortiGuard
- Enterprise Bundle level

Operational
- Cloud analytics/management
- SD-WAN related services
- FortiConverter

Fortinet NSE Certification Program
The Fortinet Network Security Expert (NSE) Program is an 8-level training and assessment program designed for customers, partners, and employees, with over 500,000 security certifications to date. Fortinet Authorized Training Centers (ATCs) deliver expert-level training in local languages in over 100 countries worldwide.

Fortinet Network Security Academy Program
The Fortinet Network Security Academy program provides industry-recognized Fortinet training and certification opportunities to students around the world. Launched in 2016, this innovative, rapidly growing program has already been adopted by 352 academies in 85 countries.

Expanded Free Cybersecurity Training
Fortinet has opened up our entire self-paced catalogue of advanced Network Security Expert training courses. The courses will be free for the remainder of 2020* to help address the rapidly evolving needs of organizations securing highly distributed and remote workforces.

* Self-paced courses in NSE 4-7 only, through 12/31/2020. Instructor-led courses, hands-on labs, and certifications are not included. Learn more about both programs at www.fortinet.com/support-and-training.html
Independently Tested and Validated Protection

Recommended IN 9 out of 9 NSS LABS Tests

Next-Generation Firewall Test (2019) FortiGate 500E

- “Recommended” 6th year in a row
- 99% Exploit Block Rate
- 100% Live Exploit Block Rate
- Best SSL Performance with least degradation
- Very low Total Cost of Ownership ($2 per Protected Mbps)

SD-WAN Test (2019) FortiGate 61E

- Second consecutive SD-WAN “Recommended” rating
- Lowest Total Cost of Ownership, 8X better than competitive offerings
- Deployment in under 6 minutes with Zero-Touch Provisioning
- Reliable Quality of Experience for Video and VOIP
- Best user experience in HA deployments
- In-built NGFW security
Unparalleled Third-Party Certification

Customer Recognition

Gartner Peer Insights Customers’ Choice distinctions are based on the ratings of vendors by verified end-user professionals across a variety of industries and from locations around the world. These distinctions take into account both the number of end-user reviews a vendor receives, along with the overall ratings score a vendor receives from those end users.

Fortinet is proud to be named a Gartner Peer Insights Customers’ Choice in several critical areas:

<table>
<thead>
<tr>
<th>CERTIFICATION</th>
<th>FORTINET</th>
<th>Check Point</th>
<th>Cisco</th>
<th>Palo Alto</th>
<th>Juniper SRX</th>
<th>FireEye</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. NSS Next-Gen Firewall</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. NSS DC Security Gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. NSS Next-Gen IPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. NSS DC IPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. NSS Breach Detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. NSS Breach Prevention</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. NSS WAF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. NSS Advanced Endpoint*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. NSS SD-WAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ICSAS ATD—Sandbox                                    |          |             |       |           |             |         |
ICSAS ATD—Email                                     |          |             |       |           |             |         |
ICSAS Network Firewall                               |          |             |       |           |             |         |
ICSAS Network IPS                                    |          |             |       |           |             |         |
ICSAS Anti-malware Network                           |          |             |       |           |             |         |
ICSAS WAF                                           |          |             |       |           |             |         |
Virus Bulletin 100                                   |          |             |       |           |             |         |
Virus Bulletin Spam                                  |          |             |       |           |             |         |
Virus Bulletin Web                                   |          |             |       |           |             |         |
Common Criteria                                      |          |             |       |           |             |         |
FIPS                                                |          |             |       |           |             |         |
UNH USGv6/IPv6                                      |          |             |       |           |             |         |

* Vendor products now receive a letter rating. Green here denotes a favorable “A” rating or better. As of July 2020

The Only NSS Labs Recommended Edge to Endpoint ATP Solution

Fortinet has participated in the following real-world group tests, open to the industry, and conducted by NSS Labs. In doing so, Fortinet stands out as the only vendor to provide an ATP solution that is NSS Labs Recommended from the data center to the edge to the endpoint in the latest group tests.

- NGFW & NGIPS
- DC Security Gateway & DCIPS
- Web Application Firewall
- Endpoint Protection
- Breach Detection and Prevention

See our Gartner Peer Insights reviews and distinctions at www.gartner.com/reviews
Rollins
Leading consumer and commercial services company providing essential pest control and protection to millions of customers in North America.
Scope: Improve security posture and enforce uniform security policies across entire network infrastructure consisting of over 700 locations, 2 data centers and multiple private cloud data centers.
Key Requirements: Migrate from aging MPLS to SD-WAN for business flexibility, cost reduction, improved network performance, and enhanced user experience.
Solution: Fortinet Secure SD-WAN solution, FortiExtender
Customer Benefits Realized
- Improved user experience and increased network speeds by 7-10x
- Reduced costs and outages
- Cut network setup time by 50 percent through a single console

"Fortinet Secure SD-WAN addressed our connectivity, security and management challenges with a comprehensive solution supporting advanced routing, SD-WAN, and security in a single appliance. With integrated SD-WAN functionality and security, we are able to simultaneously improve application performance and our overall security posture. The current state of the world has really re-emphasized the positive impact of Fortinet Secure SD-WAN for us."
— Kevin Morrison, VP ITC Operations

HR Path
Global Leader in Human Resource Technology
Scope: Increase bandwidth and support cloud-based services securely for 1250 customers in 18 countries
Key Requirements: GDPR compliance, replace MPLS with secure SD-WAN, multi-cloud protection, simplified network management
Solution: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiSwitch, FortiGuard Services
Customer Benefits Realized
- €12,000 (US$13,000) per site annual infrastructure cost savings by replacing MPLS infrastructure with SD-WAN solution
- Projected 100% ROI in five years
- Enhanced security through improved visibility and control of all global ISPs
- Reduced risk of intrusion through identity and access management and integrated IPS
- Increased potential customer retention by meeting or exceeding their security standards

“We wanted to develop a process through which security would be an integral part of every IT project — rather than an add-on or afterthought.”
— Sébastien Griet, Infrastructure Director

Alaska Airlines
5th Largest Airline in United States
Scope: Secure connectivity and data protection (including PCI data) for over 44 million passengers, 23,000 employees and 1200 flights daily
Key Requirements: Protect the e-commerce edge, data center and network, provide secure SD-WAN capabilities
Solution: FortiGate, FortiAnalyzer, FortiAuthenticator, FortiClient, FortiExtender, FortiManager, FortiSwitch, FortiWifi, FortiGuard Services
Customer Benefits Realized
- Ability to secure from the e-commerce edge to the data center
- Simplified configuration, management, authentication and reporting
- Ease of deployment and rollout to distributed locations

“We were already pleased with the performance of Fortinet’s Next-Generation Firewalls in our data center and the protection they provide for employee access and authentication. We recently chose to leverage Fortinet’s Secure SD-WAN capability because it provides superior security features in one simple offering. Fortinet helps us reduce complexity and gives us the single-pane-of-glass visibility across all our locations.”
— Brian Talbert, Director, Network and Connectivity Solutions

GTT
A leading, global cloud networking provider to large, global enterprises
Scope: Deliver additional value to customers though global access, security and cloud acceleration services.
Key Requirements: Combine global Tier 1 IP network with industry leading SD-WAN and security capabilities.
Solution: Fortinet Secure SD-WAN, FortiGuard Services
Partner Benefits Realized:
- Ability to securely connect customers’ locations to every application in the cloud.
- Smart, cost-effective connectivity platform with Fortinet Secure SD-WAN.
- Powerful combination of global last mile access with advanced security and application performance.

“Clients rely on GTT to securely connect their locations across the world and to every application in the cloud. Our broad portfolio of SD-WAN service options, that now includes Fortinet, ensures that clients can run their applications with superior security, performance and reliability to support their business goals.”
— Ernie Ortega, Interim CEO & Chief Revenue Officer

For more customer stories, go to www.fortinet.com/customers.html