Cisco Firepower Next-Generation Firewall

Prevent breaches, get deep visibility to detect and stop threats fast, and automate your network and security operations to save time and work smarter.

Expect more from your firewall

Organizations everywhere are worried about the next big cybersecurity breach. A breach can compromise sensitive data, erode confidence in an organization's brand, knock the network out of commission, and result in lost productivity and millions of dollars in revenue.

Meanwhile, malware is more sophisticated than ever, and cybercriminals are unrelenting in their attacks. The IT team deploys a firewall in hopes of preventing these attacks, but it lacks the deep visibility into their systems needed to detect stealthy threats and stop them before damage can be done.

In the face of these challenges, the IT team has limited resources, staff, and time. They're overwhelmed by too many alerts from their firewall and other security tools. and feel like they're just playing whack-a-mole with threats.

What if your firewall could prevent breaches and stop the stealthiest attacks, all while maintaining optimal network performance and uptime?

The Cisco Firepower Next Generation Firewall (NGFW) prevents breaches, and can quickly detect and mitigate stealthy attacks using deep visibility and the most advanced security capabilities of any firewall available today – all while maintaining optimal network performance and uptime.

“Our Cisco firewalls have prevented multiple breaches, blocked users from downloading malicious files, blocked outbound connections caused by malware, and prevented external threats through integration with intelligence and IPS rules.”

Network Administrator
Financial Services Company

Breach Prevention

In the face of constant attacks and successful breaches, organizations today are worried about the next big breach. That’s why Cisco Firepower Next-Generation Firewall (NGFW) employs a diverse set of capabilities to automatically prevent breaches, safeguard the organization, and keep the network, ergo the business, humming.

It all begins with the best threat intelligence captured by Talos, our team of 350+ threat researchers and analysts. They analyze millions of malware samples and terabytes of data per day, create security protections (Snort rules and threat indicators), and automatically share that information with Cisco NGFW. When the firewall inspects traffic, it utilizes that threat intelligence to protect your organization 24/7 against known, unknown, and emerging threats.

WannaCry? NotPetya? VPNFilter? Talos caught all of these (and others), and Cisco NGFW customers were automatically protected.

Breach Prevention Capabilities

- Cisco Talos is our world-class threat research team of 350+ researchers and analysts
- Talos creates automated security intelligence feeds used in Cisco NGFW to stop known, unknown, emerging attacks
- Thanks to Talos threat intelligence, Cisco NGFW customers were automatically protected against attacks like WannaCry, NotPetya and VPNFilter

Breach Prevention Resources

- Demo video
- Customer story

Deep Visibility

Malware is more sophisticated than ever, and cybercriminals are unrelenting in their attacks. IT teams today have deployed firewalls that don't provide the network and security visibility they need to see and stop stealthy threats.

Cisco NGFW goes beyond just prevention and access control to give you deep visibility into telemetry and potentially malicious file activity across users, hosts, networks, and infrastructure. This enables you to detect malicious activity fast and eliminate it before damage can be done. Our advanced security capabilities help you see more so you can stop more.

Visibility Resources

- Demo video
- Customer story

Visibility Capabilities

- Cisco NGFW offers visibility into threat activity across users, hosts, networks, and infrastructure
- Network file trajectory maps how hosts transfer files, including malware, across your network to scope an attack, set outbreak controls, and identify the source of the threat
- Centralized management provides contextual threat analysis and reporting, with consolidated visibility into security and network operations
- Next-Generation Intrusion Prevention System (NGIPS): The top-rated intrusion prevention system in the market helps you see more and block advanced threats automatically.

"We discovered that Cisco Firepower NGFW delivered considerably more volume, variety, and granularity of information than the other next-gen firewalls we evaluated. Firepower's at-a-glance dashboards made it quick and easy to see what's happening and prioritize our response."

Chris Langford, Director of Network, Infrastructure, and Cyber Security, Lewisville Independent School District

“The seamless integration and interoperability of the Cisco NGFW with the rest of the Cisco portfolio made our choice a fairly easy one. The visibility that the Cisco security portfolio provides has been invaluable to our organization.”

Joshua Thums
Forest County Potawatomi

Automation & Integration

IT teams today have limited resources, staff, and time. Let Cisco NGFW do more of the work for you.

Automated policy application and enforcement frees up time so you can focus on high priority items. In Firepower Management Center, threat alerts are prioritized so you can focus on what matters most.

Cisco NGFW also works together seamlessly with the rest of our integrated security portfolio. Different tools share threat information, policy information, and event data.

For instance, Cisco NGFW shares policy information with ISE so that it can automatically enforce policy on devices. Cisco AMP for Endpoints will notify the Cisco NGFW if it has quarantined a file on a specific device. With integrations like these, you can get visibility across multiple attack vectors, from edge to endpoint, so that when you see a threat in one place, you can stop it everywhere.

Instead of having to learn and pivot between a multitude of disparate security tools, Cisco’s security tools work together to make your life easier.

Automation Capabilities

- Automated policy application and enforcement frees up time so you can focus on high priority items
- Automatic IPS tuning blocks more threats and reduces the volume of alerts
- Prioritized threat alerts show you where to focus on what matters most
- Cisco’s integrated security tools share and correlate data automatically to see and stop threats

Automation Resources

- Demo video
- Customer story

Why Cisco?

Cisco Firepower NGFW is the foundation of the integrated Cisco security architecture. It prevents breaches, and can quickly detect and mitigate stealthy attacks using deep visibility and the most advanced security capabilities of any firewall available today – all while maintaining optimal network performance and uptime.

No matter the size of your organization, we have a next-generation firewall to meet your requirements. Cisco offers a range of options to address the needs of small and medium-sized businesses, enterprises, government organizations and service providers.

Customers agree on reasons for choosing Cisco NGFW. They praise the ease of implementation, integration of multi-layered security features into a single platform, flexible management options, innovative security automation, great performance, and low operational costs among others. For these reasons and more, Cisco was named a leader in Gartner's 2018 Magic Quadrant for Enterprise Network Firewalls.

Models & Options

Cisco Firepower 2100 Series Appliances

The 2100 series firewall addresses use cases from the Internet edge to the small-scale data centers. Features sustained performance when advanced threat functions are enabled.

- Four 1RU models: FPR2110, FPR2120, FPR2130, FPR2140
- Firewall throughput from 2.0 to 8.5 Gbps
- Threat inspection from 2.0 to 8.5 Gbps
- Firepower Device Manager is included for local management of single firewall deployments

Cisco Firepower 4100 Series Appliances

Suitable for internet edge, large-scale data center and high-performance environments. Cisco Firepower 4100 Series deliver superior threat defense, at faster speeds, with a smaller 1RU footprint. This series supports flow-offloading, programmatic orchestration and the management of security services with RESTful APIs.

- Four 1RU models: FPR2110, FPR2120, FPR2130, FPR2140
- Firewall throughput from 12 to 30 Gbps
- Threat inspection from 10 to 24 Gbps
- 1/10/40 GE
- Available behavioral DDoS mitigation

Cisco Firepower 9300 Security Appliances

Carrier-grade, modular platform designed for service providers, high-performance computing centers, large data centers, campuses, high-frequency trading environments, and other environments that require less than 5-microsecond offload latency and exceptional throughput. Cisco Firepower 9300 supports flow-offloading, programmatic orchestration, and the management of security services with RESTful APIs.

- 10/40/100 GB network interfaces
- Firewall throughput from 30Gbps and up to 1.2 Tbps clustered throughput
- Available behavioral DDoS mitigation

Cisco ASA 5500-FTD-X Series Appliances

Cost-effective option offering throughput to address use cases for small to medium business, branch office. They deliver Firepower Threat Defense in a lower-cost appliance.

- Three desktop and 8 1RU models: ASA 5506-FTD-X, ASA 5506H-FTD-X, ASA 5506W-FTD-X, ASA 5508-FTD-X, ASA 5516-FTD-X, ASA 5525-FTD-X, ASA 5545-FTD-X, ASA 5555-FTD-X
- Firewall throughput from 250 to 1750 Mbps
- Threat inspection from 125 to 1250 Mbps

Cisco Firepower NGFW Virtual (NGFWv) Appliances

NGFWv is available on VMware, KVM, and the Amazon Web Services (AWS) and Microsoft Azure environments for virtual, public, private, and hybrid cloud environments. Organizations employing SDN can rapidly provision and orchestrate flexible network protection with Firepower NGFWv. Organizations using NFV can further lower costs utilizing Firepower NGFWv.

Get Started

Get started with Cisco NGFW today.
Visit cisco.com/go/ngfw.