

Cisco Firepower and Splunk: Turn Your Access Control Perimeter into a Threat Control Perimeter

Turn your access-control perimeter into a threat-control perimeter

Perimeter security has evolved. Rather than rely solely on traditional access control firewalls, you can strengthen your defenses against advanced threats with next-generation firewall solutions. The Cisco Firepower® NGFW can put up a “threat-control perimeter” around your organization using:

- Next-Generation IPS (NGIPS)
- Advanced malware protection
- Application visibility and control
- Vulnerability awareness
- Asset-value context
- Cisco and partner threat intelligence
- Web reputation and URL filtering

Benefits

- **Migrate from traditional firewall access control** and make the perimeter a wall of threat defense
- **Manage firewall events with confidence** viewing Cisco ASA and Cisco Firepower events in Splunk
- **Proactively identify and analyze security threats** quickly across multivendor security environments
- **Customize reports and historical trends** to flexibly address compliance and other requirements
- **Gain an enterprise-class integrated solution** with support and migration services

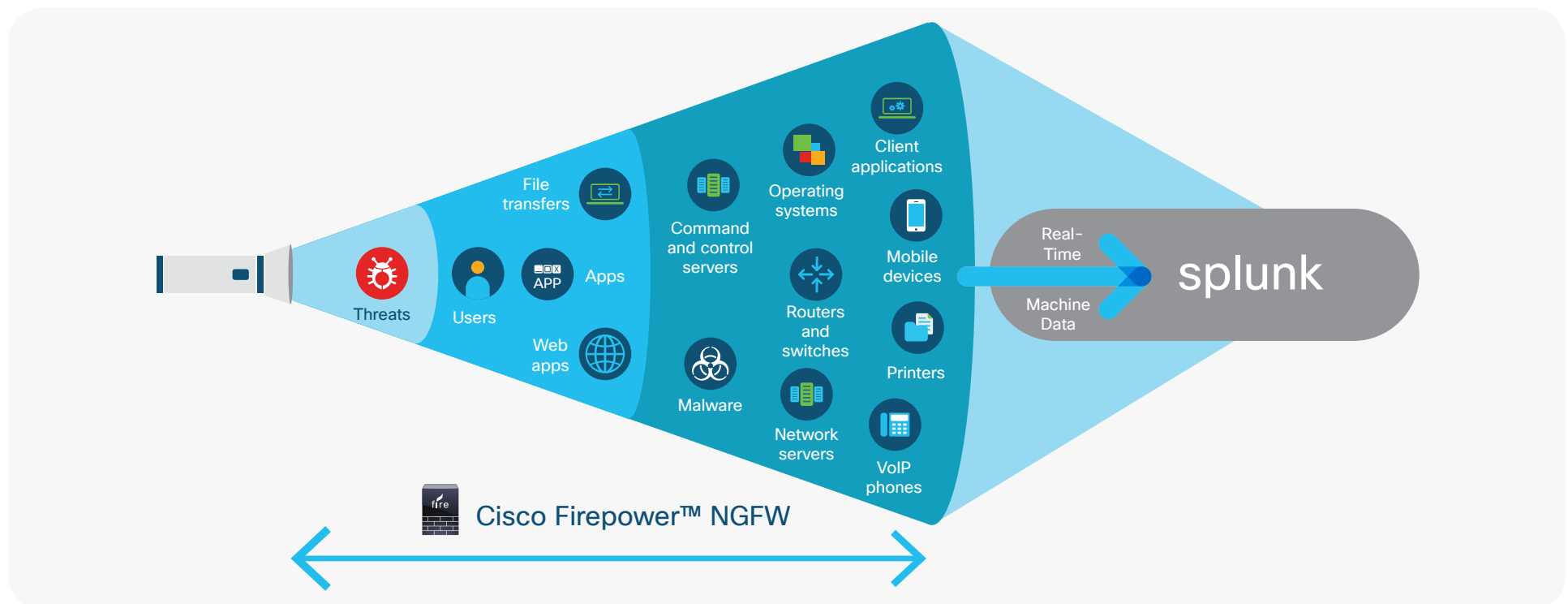
You gain insights into client-side apps and operating systems, mobile device types and browsers, virtual machine communications, and network devices while detecting the most advanced malware.

And, to fully harness the visibility that Cisco Firepower delivers, Splunk offers a powerful event-analytics platform. Splunk enables a proactive stance to investigation and response – from monitoring and triage, verifying and escalating, to responding to a breach or infection. With it, you can investigate and respond to threats in the cloud, on premises, and in hybrid environments.

Together, Cisco and Splunk streamline firewall event management and threat response through:

- Comprehensive support for Cisco Firepower events in a Splunk environment
- Customizable monitoring dashboards to address compliance, departmental, and other needs
- The ability to expand investigations across multiple Cisco products as well as multivendor security deployments
- A single repository for both Cisco ASA and Cisco Firepower events
- Integrated threat response and mitigation through Cisco Rapid Threat Containment and Splunk Adaptive Response

Figure 1 Threat hunting with context-rich visibility



Next steps

Customers using Cisco ASA infrastructures may migrate to Cisco Firepower offerings by:

- Upgrading to Cisco FirePOWER Services on a compatible ASA appliance. See <https://www.cisco.com/c/en/us/products/security/asa-firepower-services/index.html> for additional details
- Migrating from ASA appliances to Firepower appliances. Cisco provides tools for migrating ASA configuration to Firepower. Furthermore, firewall platform management partners such as Tufin, FireMon, and AlgoSec offer a variety of migration features

Cisco Advanced Services offer comprehensive planning, design, and deployment for your migration of ASA to Cisco Firepower.

Learn more about the products outlined in this brief:

- [Cisco Firepower](#)
- [Splunk](#)
- [Cisco Firepower Integration with Splunk](#)
- [Cisco ISE](#)
- [Cisco Rapid Threat Containment](#)
- [Other Cisco and Splunk security integrations](#)

How the integration works

The base solution is composed of Cisco Firepower NGFW appliances or Cisco ASA with FirePOWER™ Services; the Cisco Firepower Management Center version 6.x; Splunk Enterprise or Splunk Cloud software; the Cisco Firepower eNcore App for Splunk; and the Cisco eStreamer Add-On for Splunk. These integrations are also compatible with the Splunk Enterprise Security next-generation Security Information and Event Management (SIEM) system.

In the integrated solution:

- Cisco Firepower Management Center exports Cisco Firepower security events through the eStreamer API
- The Cisco eStreamer Add-on for Splunk enables Splunk software to ingest the events from all 6.x versions of Firepower Management Center into Splunk software
- The Cisco app for Splunk provides charts, graphs, metrics, and a geolocation map for all the main eStreamer event types

Threat response actions, such as user and device network quarantine, are executed from the Splunk console. The Cisco Identity Service Engine (ISE), if present in the network environment, implements these threat actions through its Rapid Threat Containment capabilities.