



Drive Security Resilience

with Secure Firewall

Data and applications live everywhere, and most organizations are operating across multiple environments to achieve greater agility and flexibility.



82%

of global IT professionals have adopted hybrid clouds¹



47%

of organizations use between two and three public clouds¹

1. 2022 Cisco Global Hybrid Cloud Trends Report

But the unforeseen by-product of this evolution is **complexity** – spawning an expanding attack surface and new vulnerabilities.

Adding to this complexity...



...is **the potential for disruption** driven by new levels of global uncertainty.

To tackle these challenges, organizations are investing in resilience across all lines of business...

But these efforts are incomplete unless **security** and the **principles of Security Resilience** are incorporated across the organization.



What do we mean by Security Resilience?

Security Resilience means organizations have the ability to quickly adapt to change, remain operational in the face of disruption, and apply the learnings so they emerge stronger.

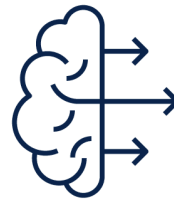
To achieve these outcomes, network security must promote four principles:



Flexibility



Visibility



**Actionable
intelligence**



**Unifying
controls**

To help overcome new threats and attack vectors, as well as new operational challenges.



Sustaining hybrid work

Requires seamless access from anywhere




Responding to massive global attacks

Requires visibility over encrypted traffic



Managing unpredictability

Requires insights and rapid delivery of innovation



Cisco Secure Firewall is your cornerstone for driving Security Resilience across your hybrid and multicloud environment.

The firewall is more than a box. It is the advanced capabilities and outcomes that can be applied anywhere, on-prem or in the cloud, protecting your data and applications wherever they live.

The **flexibility** of Secure Firewall makes it a fundamental building block for network security.

It can **easily be inserted into any environment** to protect your data in even the most complex and distributed hybrid environments.

And for critical cloud operations, Secure Firewall can be consumed as a service, enabling **rapid deployment and lower cost of ownership**.



On-premises



Public cloud



Hybrid

With Secure Firewall, you can **see more**
and **detect threats faster.**

Only Secure Firewall gives you the **visibility** to identify potentially malicious applications in encrypted traffic flows with an Encrypted Visibility Engine. It also receives hourly threat intelligence updates from **Cisco Talos®** – one of the largest commercial threat intelligence teams in the world.

Combined with URL filtering, malware defense, and Snort 3 IPS, Secure Firewall delivers **robust protection against even the most sophisticated threats.**

Actionable intelligence enables you to prioritize and share critical information so you can rapidly respond – the right way.

To accelerate detection, response, and recovery, Secure Firewall includes a license entitlement to **Cisco SecureX**, our cloud-native platform with XDR capabilities.

Together, Secure Firewall and SecureX can **cut investigation and response time up to 75%** by sharing global intelligence and local context.¹

75%



Response time

1. Forrester, Total Economic Impact of Secure Firewall

Unifying security controls reduces risk and streamlines operations.



Cloud-delivered Firewall Management Center (FMC), brings firewall management into one easily accessible application, allowing you to control your firewalls from anywhere in real time.

Updates are applied automatically, **reducing potential risks and simplifying operations**. A SaaS application, it contains the same functionality and look as its on-prem sibling, eliminating the need for new training.

And like the on-prem version, cloud-delivered FMC includes a ribbon to access Cisco SecureX, accelerating response and remediation from one place.



Promote stronger security and greater collaboration.

In keeping with the principle of **unifying security controls**, Secure Firewall dynamically shares policies driven by intelligence from Secure Workload, which protects your applications and data by segmenting workloads to prevent unauthorized lateral movement.

This enables your **NetOps team to run at DevOps speed**, closing gaps to increase security efficacy and driving collaboration across teams.

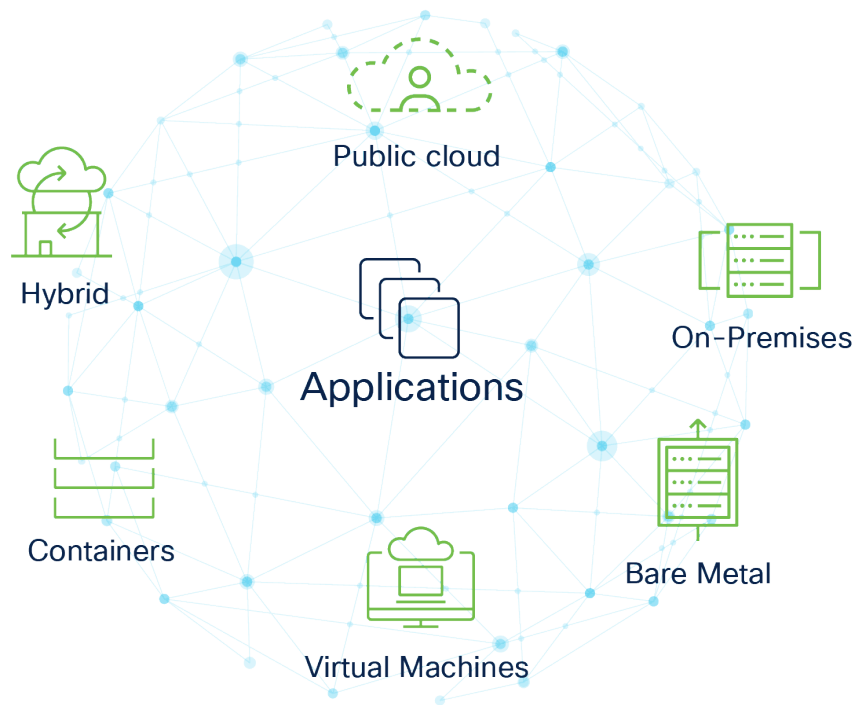


Secure Workload protects the applications that power your business.

The benefits of Secure Workload extend beyond sharing and synchronizing policies with Secure Firewall.



Secure Workload seamlessly enforces **zero trust microsegmentation** across your entire application landscape – regardless of environment, location, or form factor.



The magic of Secure Workload is its ability to see and understand every workload interaction. The result is **security tailored to your application's behavior**, backed by powerful automation to do the heavy lifting – consistently and accurately.

Today's business depends on the hybrid and multicloud environment.

With workers, data, and offices located all over, your firewall is more relevant than ever. Secure Firewall helps you plan, prioritize, close gaps, and recover from disaster – stronger.

Secure Firewall drives Security Resilience across your hybrid and multicloud environment so that you can rapidly respond to threats in the face of disruptions.



Thank you for reading

Drive Security Resilience with Secure Firewall

For more information and a demo, see the [Secure Firewall](#) and [Secure Workload](#) landing pages:

[Secure Firewall](#)
[Secure Workload](#)

