CATO NETWORKS

Switching Firewall Vendors?

Drop The Box

Introducing the Firewall Challenge

While traditional firewalls have long played a key role in securing enterprise networks, they often struggle to keep up with the demands of today's cloud-first, hybrid work environments. These hardware-based solutions can introduce significant costs, integration challenges, and ongoing maintenance requirements—all while lacking the flexibility, scalability, and visibility that modern enterprises require. As a result, organizations may face security gaps, operational inefficiencies, and increasing difficulty adapting to evolving cyber threats. A more agile, cloud-delivered security approach can help bridge these gaps and support the needs of the modern enterprise.

Introducing Firewall as a Service: The Modern Security Evolution

Firewall as a Service (FWaaS) is the modern alternative. Delivered through a cloud-native architecture, FWaaS integrates seamlessly into today's dynamic enterprise environments, providing centralized management, advanced threat prevention, and unparalleled scalability. By eliminating hardware constraints, FWaaS enables organizations to extend uniform security policies across all users, devices, and locations while simplifying IT operations.

Discover how FWaaS, as a core component of Cato's Secure Access Service Edge (SASE) platform, future-proofs your network and security infrastructure for whatever's next.

Why Legacy Hardware Firewalls Fall Short

As enterprises embrace cloud applications, hybrid work, and geographically dispersed operations, traditional hardware-based NGFWs are increasingly misaligned with modern business needs. These appliances, designed for static, perimeter-based networks, struggle to provide the flexibility and scalability required to secure today's dynamic environments.

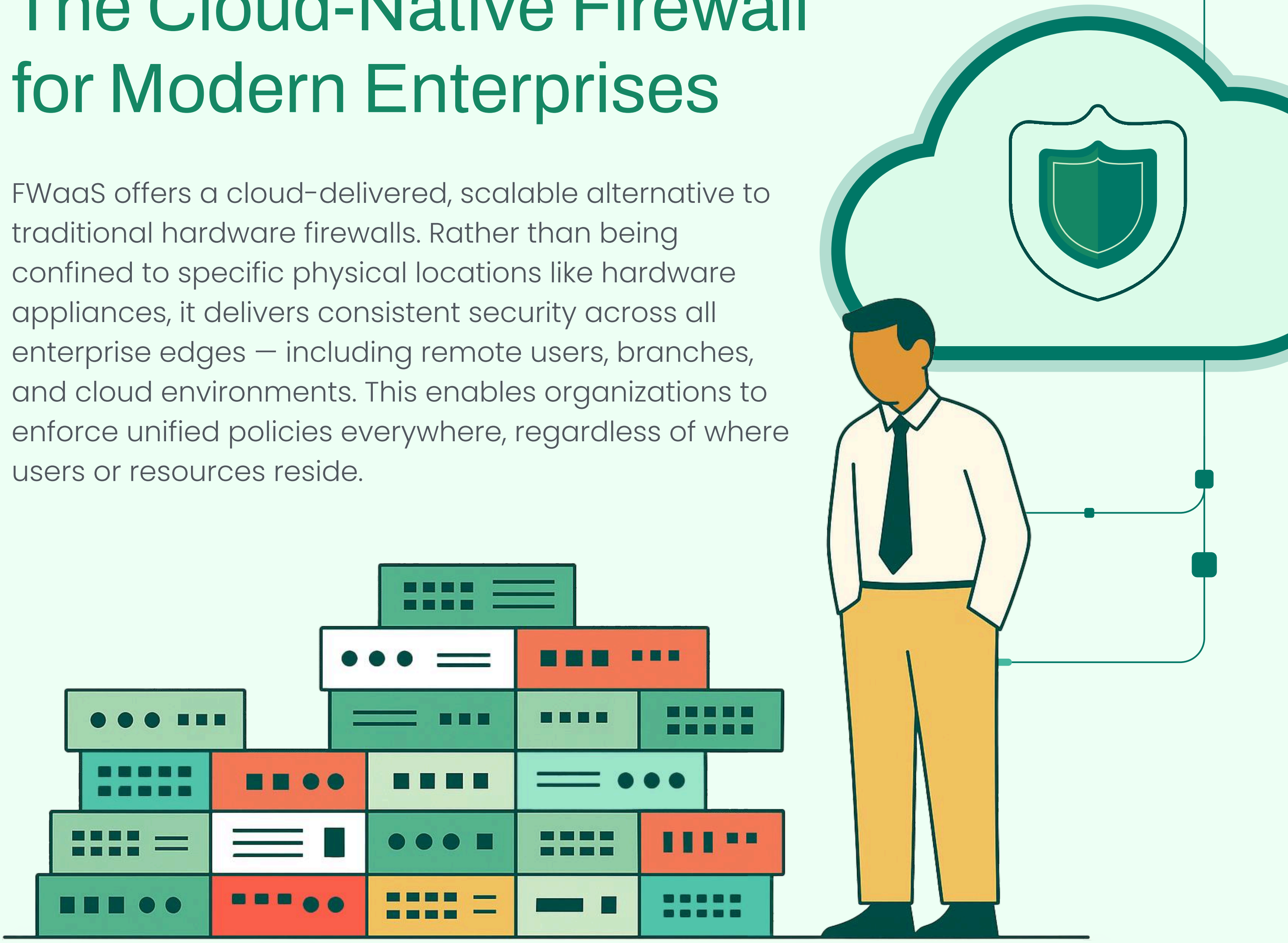
Hardware firewalls operate within a fixed infrastructure, which limits their ability to adapt to shifts in traffic patterns or rapid scaling demands. Deploying or upgrading these devices across multiple sites can be time-intensive and resource-heavy, adding complexity to IT operations. Moreover, hardware refresh cycles result in ongoing capital expenditures, while maintenance, updates, and patch management strain IT teams, consuming time that could be better spent on strategic initiatives.

Visibility is another challenge. NGFWs are often deployed at specific locations, such as data centers or branch offices, which creates fragmented security coverage. This lack of centralized oversight makes enforcing consistent policies across cloud environments, mobile users, and remote locations difficult, leaving gaps that sophisticated threats can exploit.

FWaaS addresses these shortcomings by shifting security to the cloud. By consolidating policy management, threat detection, and enforcement into a unified platform, FWaaS provides the agility, scalability, and efficiency enterprises need to secure their networks in today's cloud-first world.

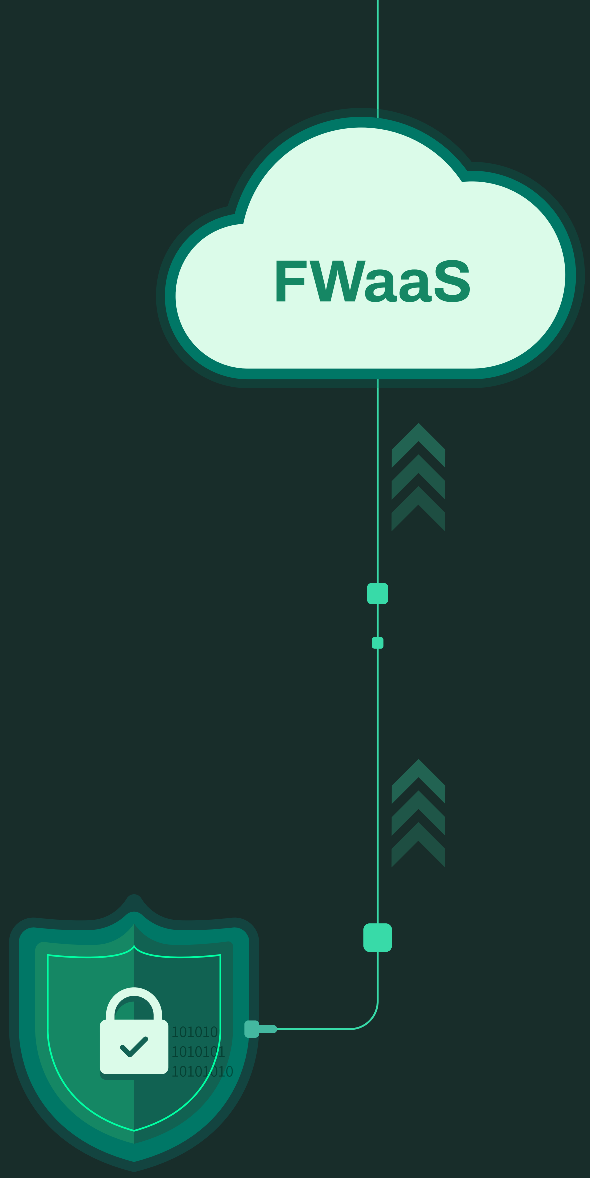
Meet FWaaS:
The Cloud-Native Firewall for Modern Enterprises

FWaaS offers a cloud-delivered, scalable alternative to traditional hardware firewalls. Rather than being confined to specific physical locations like hardware appliances, it delivers consistent security across all enterprise edges — including remote users, branches, and cloud environments. This enables organizations to enforce unified policies everywhere, regardless of where users or resources reside.



With deep packet inspection, intrusion prevention, and application-aware controls built in, FWaaS delivers advanced capabilities through a cloud-native service model. Software upgrades and security patches are handled for you, removing a major burden from IT teams. As part of the service, platforms are maintained and updated automatically. A single console can manage policies and activities centrally, ensuring better visibility and operational efficiency.

Scalability is a core advantage of FWaaS, enabling seamless adaptation to evolving business needs. Whether expanding into new regions, migrating to the cloud, or supporting a distributed workforce, organizations can scale security instantly — without the delays or costs of deploying hardware. This allows for a more agile and unified security posture that aligns with today's dynamic IT environments.

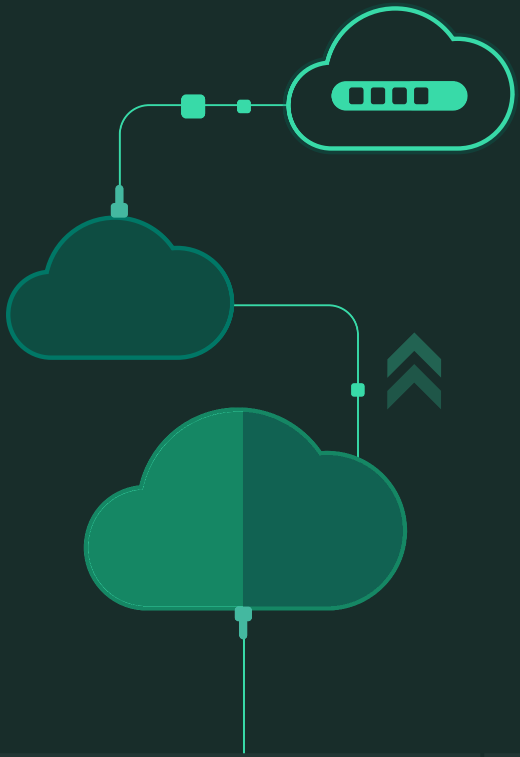


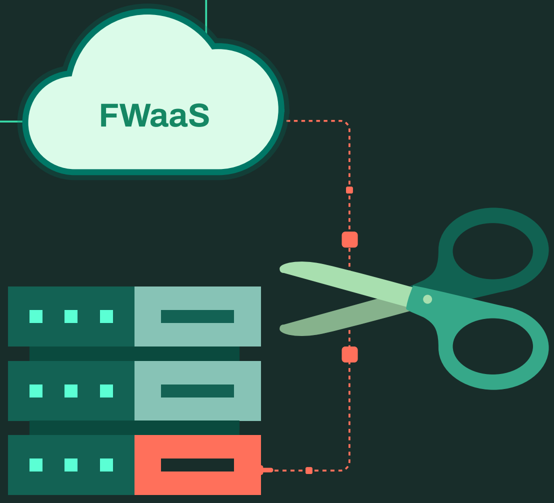
Why FWaaS?
The Advantages of a Cloud-Native Firewall

Transitioning from hardware-based firewalls to FWaaS offers several tangible benefits for enterprises seeking to modernize their security infrastructure, including:

Scalability

FWaaS eliminates the limitations of physical appliances, allowing enterprises to scale security seamlessly as their network grows. New sites, users, and cloud environments can be secured instantly without deploying additional hardware. This flexibility ensures consistent policy enforcement across global locations while adapting to evolving business needs without infrastructure constraints.





Removing Hardware Dependency

By shifting firewall functionality to the cloud, FWaaS removes the need for on-premises appliances, reducing capital expenditures and maintenance overhead. Organizations avoid hardware refresh cycles, complex installations, and capacity planning, ensuring continuous protection without physical limitations. This also enhances resilience, as security enforcement is no longer tied to specific locations.

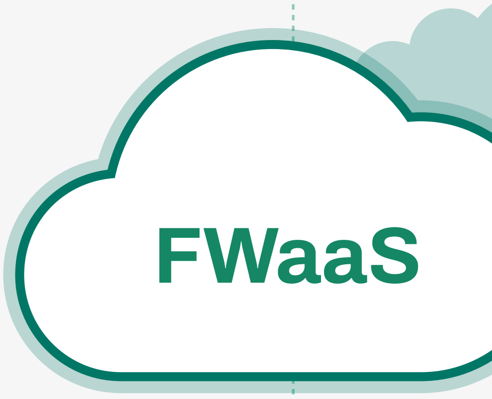
Centralized Management

FWaaS provides a unified platform to configure and enforce security policies across all sites, users, and cloud environments. IT teams gain full visibility into network traffic, threat activity, and policy effectiveness from a single interface. This simplifies administration, reduces misconfigurations, and enables faster response to security incidents, improving overall operational efficiency.

Seamless Updates and Upgrades

Traditional firewalls require manual patching and upgrades, leading to potential security gaps and operational disruptions. FWaaS, delivered as a cloud-native service, ensures automatic updates for threat intelligence, security policies, and software enhancements. This guarantees enterprises stay protected against emerging threats without downtime or the need for constant IT intervention.

Making the Switch: A Practical Roadmap to FWaaS Adoption



Switching from traditional hardware firewalls to FWaaS is a strategic move that requires careful planning to minimize disruption and ensure success. Below is a recommended roadmap to guide enterprises through the transition.

01 Assess Your Current Network Architecture

Start by auditing your current firewall infrastructure, including hardware appliances, network topology, and security policies. Identify dependencies, such as applications tied to specific firewall rules, and document network flows to understand how traffic is routed and secured.

02 Define Security and Operational Goals

Establish clear objectives for the transition. These may include reducing hardware management, ensuring consistent security across cloud and on-premises environments, and enabling faster response to security threats. Align these goals with your broader IT and business strategies.

03 Plan for Gradual Deployment

Gradually replace hardware firewalls with FWaaS to minimize disruption. Begin with simpler use cases, such as internet-bound traffic from branch offices, before moving to more complex scenarios, like securing data centers or east-west traffic. This approach reduces risks and provides time for adjustment.

04 Integrate FWaaS into Existing Systems

Integrate FWaaS with your identity and access management (IAM) systems, SD-WAN infrastructure, and security information and event management (SIEM) tools. This ensures seamless operations and centralized policy management across your network.

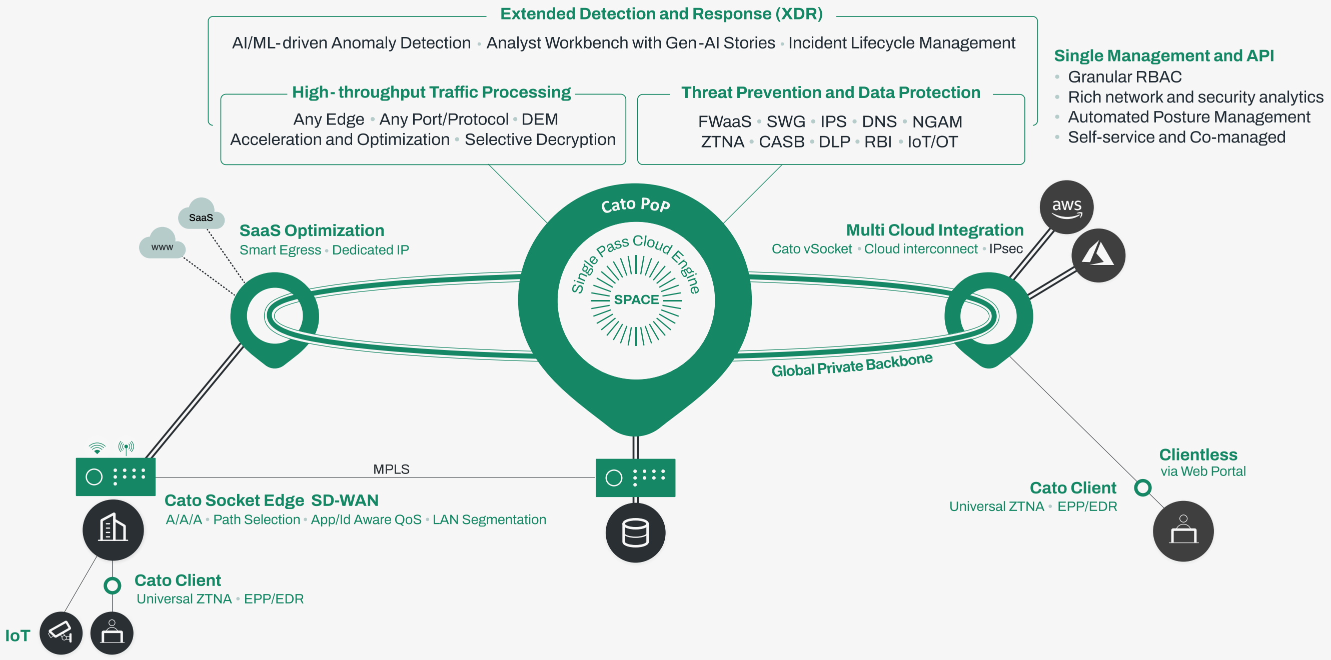
05 Test and Optimize

Conduct thorough testing to validate security policies, network performance, and scalability. Involve IT teams in testing to ensure familiarity with the new system and address any gaps in visibility or functionality.

Winning with FWaaS: **Proven Strategies for Optimal Security**

- Leverage an FWaaS solution as part of a broader Secure Access Service Edge (SASE) platform for unified network and security management.
- Maintain redundancy by running FWaaS alongside hardware firewalls during the transition.
- Train your IT teams on the FWaaS management interface to maximize its capabilities and efficiency.

Cato Networks FWaaS: Cloud-Native Security without Limits



Extended Detection and Response (XDR)
AI/ML-driven Anomaly Detection • Analyst Workbench with Gen-AI Stories • Incident Lifecycle Management
High-throughput Traffic Processing
Any Edge • Any Port/Protocol • DEM
Acceleration and Optimization • Selective Decryption
Threat Prevention and Data Protection
FWaaS • SWG • IPS • DNS • NGAM
ZTNA • CASB • DLP • RBI • IoT/OT
Single Management and API
Granular RBAC
Rich network and security analytics
Automated Posture Management
Self-service and Co-managed
SaaS
www
SaaS Optimization
Smart Egress • Dedicated IP
Cato PoP
Single Pass Cloud Engine
SPACE
Multi Cloud Integration
Cato vSocket • Cloud interconnect • IPsec
aws
Global Private Backbone
MPLS
Cato Socket Edge SD-WAN
A/A/A • Path Selection • App/Id Aware QoS • LAN Segmentation
Cato Client
Universal ZTNA • EPP/EDR
IoT
Clientless
via Web Portal
Cato Client
Universal ZTNA • EPP/EDR

Cato Networks' FWaaS offers a cloud-delivered alternative to traditional next-generation firewalls (NGFWs), integrating network security directly into a globally distributed platform. Unlike appliance-based firewalls that require on-site hardware and complex maintenance, Cato's FWaaS enforces security policies across all edges—data centers, branches, remote users, and cloud environments. It provides layer 7 application control, WAN security, and segmentation without relying on physical firewall appliances.

With FWaaS, organizations can eliminate hardware refresh cycles, simplify policy management through a centralized interface, and enhance security posture by leveraging Cato's real-time threat prevention capabilities. This approach ensures scalability, consistent enforcement, and improved agility for enterprises transitioning from legacy firewall architectures.

Closing the Loop:
Your Next Steps toward FWaaS Adoption

The limitations of hardware-based firewalls make them increasingly unsuited to today's dynamic, cloud-driven enterprise environments. FWaaS offers a flexible, scalable, and centrally managed solution that addresses these challenges, enabling organizations to simplify their security operations, reduce costs, and ensure consistent protection across all locations and users.

Transitioning to FWaaS gives enterprises the agility to stay ahead of evolving business demands and cyber threats. With its cloud-native architecture, FWaaS supports seamless scalability, centralized policy enforcement, and advanced security capabilities—all while simplifying operations and eliminating hardware complexities.

Cato Networks delivers a fully integrated FWaaS as part of its Secure Access Service Edge (SASE) platform, offering a unified approach to securing your network. Take the next step in modernizing your security infrastructure with Cato Networks. Visit our website to learn how our FWaaS can help you future-proof your network and ensure secure, efficient operations.

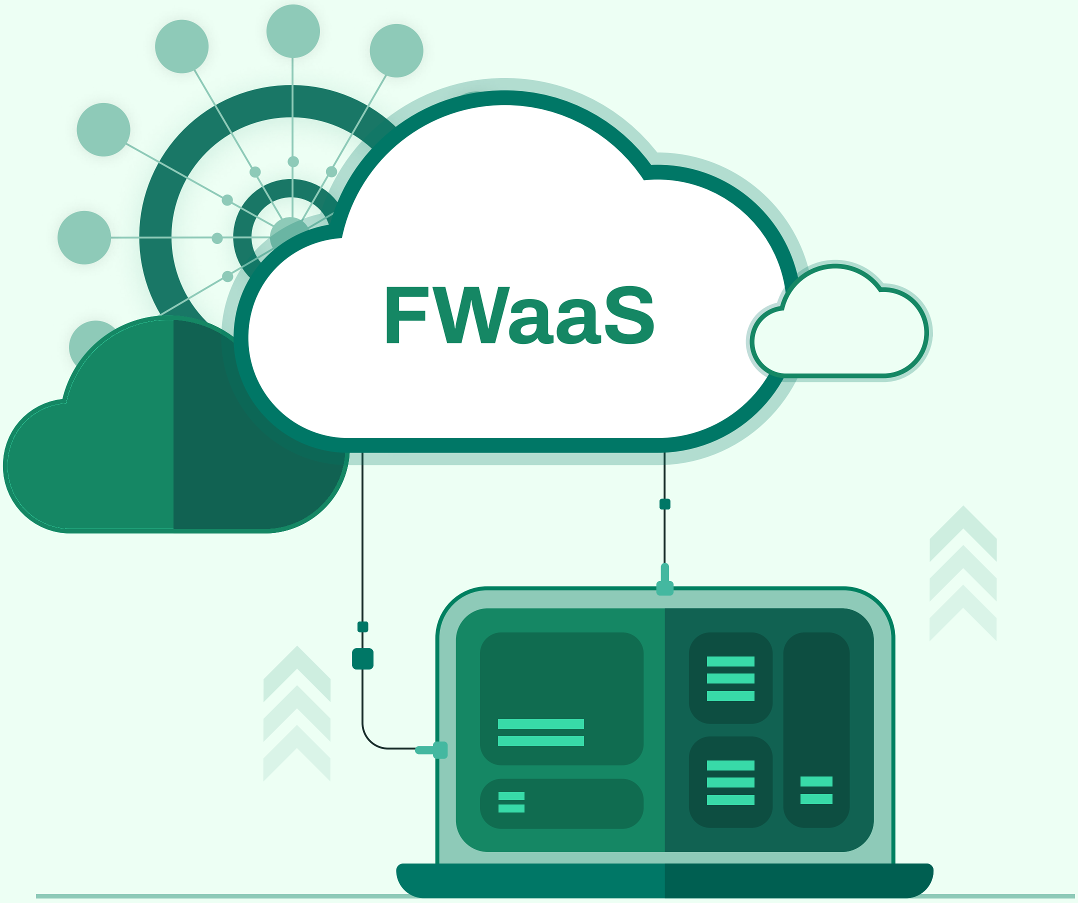
- Hardware-based firewalls are increasingly ineffective for today's dynamic, cloud-driven enterprise environments.

- FWaaS provides a **flexible, scalable, and centrally managed** solution that:
  - Simplifies security operations
  - Reduces costs
  - Ensures consistent protection across all users and locations

- Transitioning to FWaaS enables enterprises to:
  - Stay ahead of evolving business demands and cyber threats
  - Benefit from **seamless scalability, centralized policy enforcement, and advanced security capabilities**
  - Eliminate hardware complexities and streamline operations

- **Cato Networks** offers a fully integrated FWaaS within its **SASE platform,** providing a unified approach to network security.

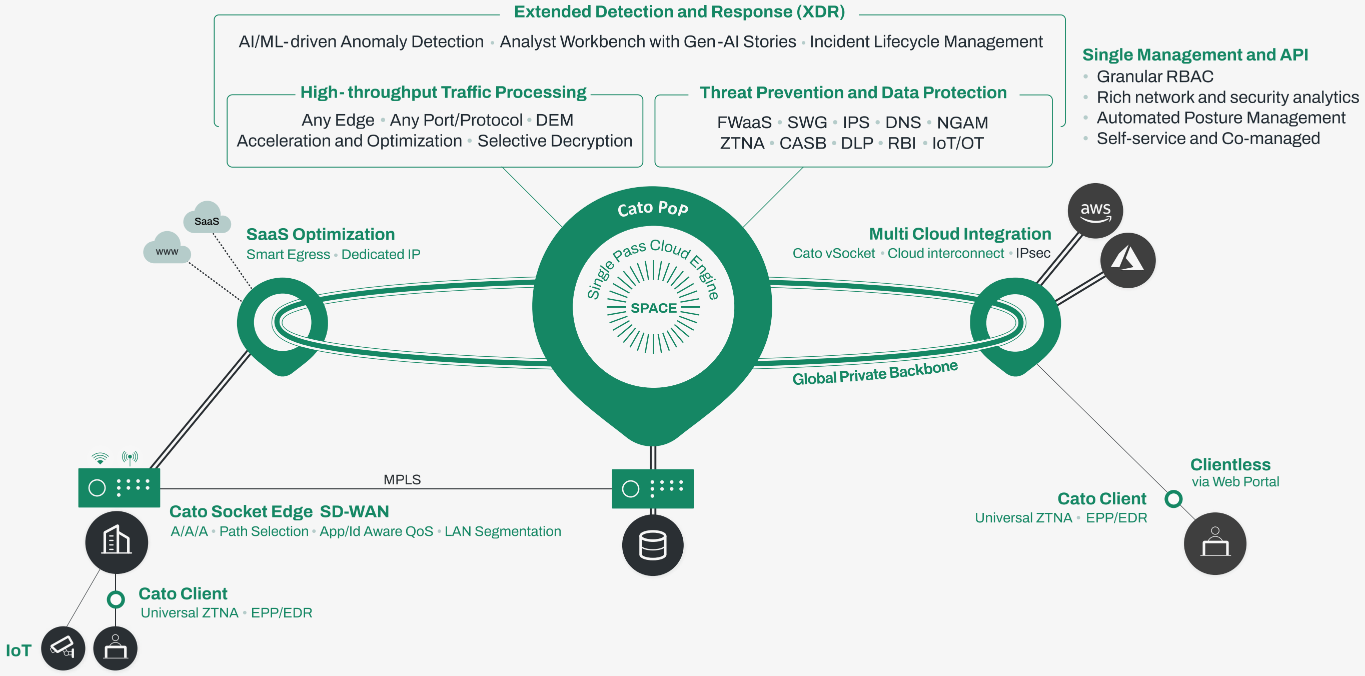
- **Take the next step** in modernizing your security infrastructure—visit our website to learn how Cato's FWaaS can future-proof your network.



About Cato Networks

Cato provides the world's leading single-vendor SASE platform. Cato creates a seamless and elegant customer experience that effortlessly enables threat prevention, data protection, and timely incident detection and response. Using Cato, businesses easily replace costly and rigid legacy infrastructure with an open and modular SASE architecture based on SD-WAN, a purpose-built global cloud network, and an embedded cloud-native security stack.

Cato SASE Cloud Platform



Extended Detection and Response (XDR)

AI/ML-driven Anomaly Detection • Analyst Workbench with Gen-AI Stories • Incident Lifecycle Management

High-throughput Traffic Processing

Any Edge • Any Port/Protocol • DEM
Acceleration and Optimization • Selective Decryption

Threat Prevention and Data Protection

FWaaS • SWG • IPS • DNS • NGAM
ZTNA • CASB • DLP • RBI • IoT/OT

Single Management and API

- Granular RBAC
- Rich network and security analytics
- Automated Posture Management
- Self-service and Co-managed

SaaS Optimization

Smart Egress • Dedicated IP

Multi Cloud Integration

Cato vSocket • Cloud interconnect • IPsec

Cato Socket Edge SD-WAN

A/A/A • Path Selection • App/Id Aware QoS • LAN Segmentation

Cato Client

Universal ZTNA • EPP/EDR

Cato Client

Universal ZTNA • EPP/EDR

Clientless

via Web Portal

Cato. WE ARE SASE.

Cato SASE Cloud Platform

Connect

Cloud Network

Cloud On-Ramps

Protect

Network Security

Endpoint Security

Detect

Incident Life Cycle Management

Run

Unified Management and API

Use Cases

Network Transformation

MPLS to SD-WAN Migration

Global Access Optimization

Hybrid Cloud and Multi-Cloud Integration

Business Transformation

Vendor Consolidation

Spend Optimization

M&A and Geo Expansion

Security Transformation

Secure Hybrid Work

Secure Direct Internet Access

Secure Application and Data Access

Incident Detection and Response

Contact Us