CLOUD4C
A CtrlS Company

Cloud4C Next-Generation Firewall

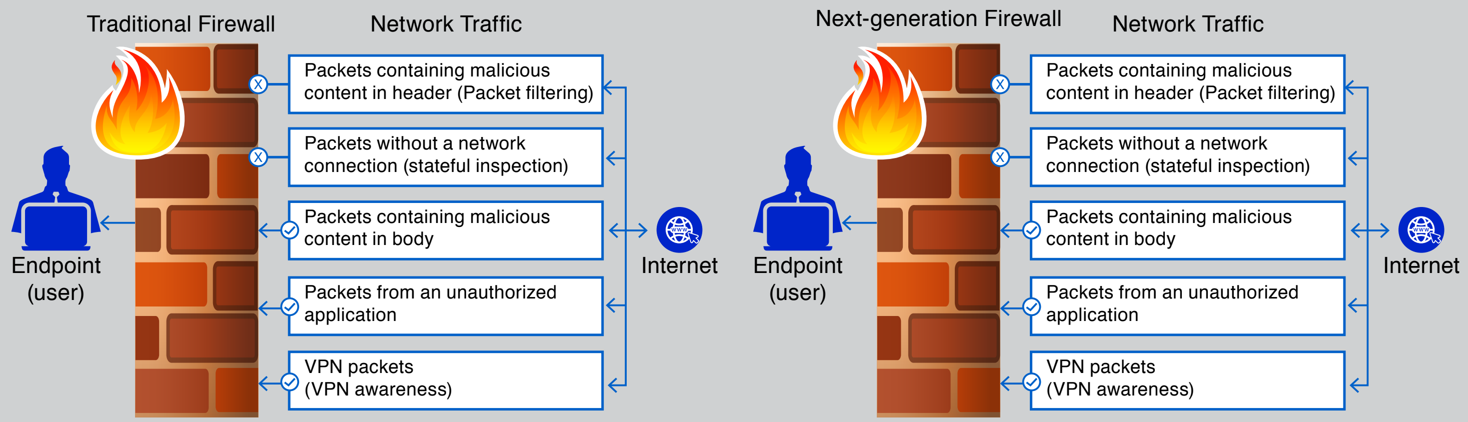
Dynamic Protection for All Your
End-points and Applications

Overview

Today's increasingly complex cyber threat landscape calls for more robust threat awareness and evolved firewalls, equipped to thwart sophisticated vulnerabilities like APTs (advanced persistent threats).

Cloud4C's AI-powered, scalable Next-Generation Firewall is the ideal solution for enterprise network security to stay resilient in today's risk landscape. Cloud4C NGFW combines visibility, simplicity, control and protection into one single package. The NGFW is designed to protect, converge and scale security to help enterprises meet escalating business needs.

Combined with the power of AI and automation, the NGFW is built to deliver the most effective network protection in the industry, closely safeguarding devices, users and applications on-premises or in the cloud.


Traditional Firewall
Network Traffic
Packets containing malicious content in header (Packet filtering)
Packets without a network connection (stateful inspection)
Packets containing malicious content in body
Packets from an unauthorized application
VPN packets (VPN awareness)
Endpoint (user)
Internet
Next-generation Firewall
Network Traffic
Packets containing malicious content in header (Packet filtering)
Packets without a network connection (stateful inspection)
Packets containing malicious content in body
Packets from an unauthorized application
VPN packets (VPN awareness)
Endpoint (user)
Internet

Features & Highlights

Comprehensive visibility and vulnerability prevention with IPS

- Industry's highest IPS performance
- Industry's highest zero day—1000+

Capabilities

- Central on-hold monitoring & release (FOS 7.2)
- RBAC preview, install, etc. (FOS 7.2)
- NOC-SOC share same security platform
- AI/ML powered security services

Benefits

- Protect business applications irrespective of their locations

Secure segmentation to prevent lateral threats

- Extremely low latency
- Ultra-scalable hardware acceleration
- Highly Flexible—Micro, macro, network-based

Capabilities

- End-to-end network segmentation
- AI/ML powered and industry leading security services
- Segment & connect physical and virtual networks with VXLAN and L4 Firewall

Benefits

- Prevent lateral movement
- Compliance separation and controls

Content security

- Advanced malware protection
- Anti-virus, Sandbox detection, botnet + C2 as well as protection from mobile malware

Capabilities

- Inline blocking of previously unknown threats with Sandbox SaaS service
- Advanced AI/ML
- Queueing optimization
- Hardware acceleration

Benefits

- Protection from ransomware, insider threat
- Real-time detection and prevention of known and unknown virus and malware

Web security

- New SaaS Security (Inline CASB) service focused on securing business SaaS data, combined with SASE
- Inline traffic inspection with ZTNA posture check

Capabilities

- URL filtering
- DNS filtering
- Video filtering
- Botnet + C2

Benefits

- Protection from phishing attempts, web-based threats
- Compliance ready and offers security policy enforcement points

Zero trust network access

- Integrated ZTNA enforcement
- Simplified licensing
- Universal ZTNA – on-net, off-net

Capabilities

- Enforcement close to the user and applications
- Constant authentication and security posture check to build consistent security
- Granular application-level segmentation

Benefits

- Deliver strong user-to-application controls, compliance and consistent convergence

Enable HTTP/3 & accelerate digital innovation

- Industry's highest SSL performance
- Video filtering

Capabilities

- HTTP/3 over QUICK (FOS 7.2)
- AI/ML powered web, video and DNS security
- Deep visibility into top applications, threats, destinations
- Integrated services DB – Dynamic & Scalable

Benefits

- Manages external threats with full visibility to detect hidden malware and avoid ransomware

Solution highlights

AI-powered Protection

Protect any user, app, edge with Cloud4C's industry-leading Integrated IPS deployed within world's leading financial institutions.

Hyperscale

Meet escalating business needs with industry's first purpose-built hardware to accelerate any security function.

Integrated ZTNA

Enterprise-level protection from a vendor qualified for "Gartner Universal ZTNA" with integrated Proxy.

Segmentation

Manage risks and enable trusted access with the only firewall vendor powered by integrated ZTNA proxy to provide explicit application access.

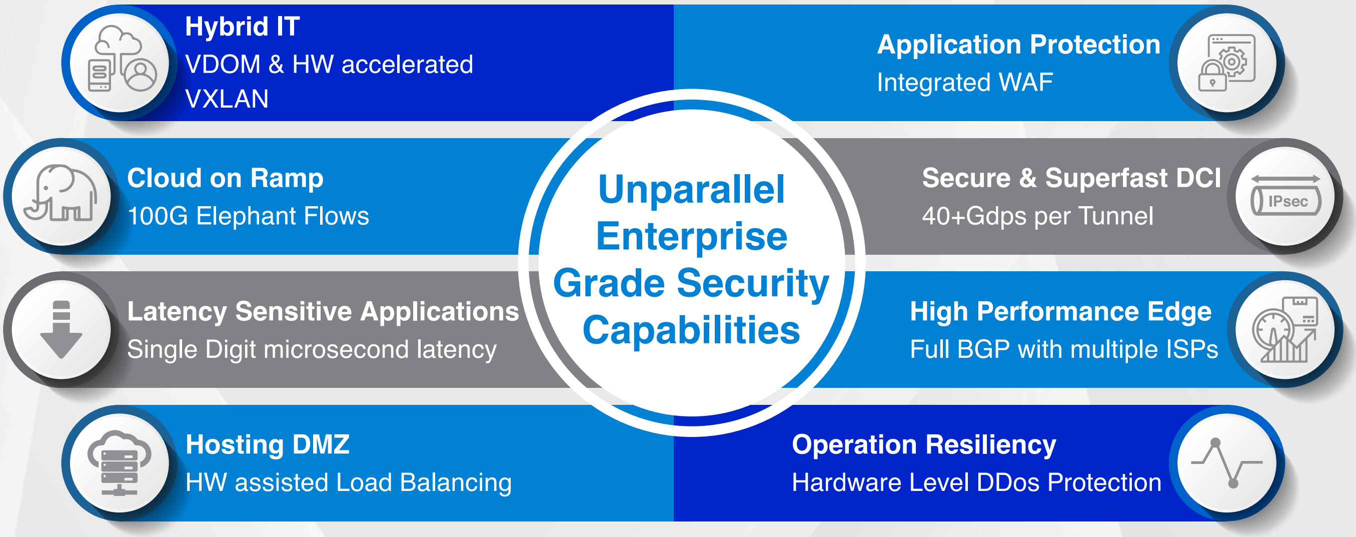
Deep Visibility

Manage external risks with TLS1.3. We also offer the industry's highest SSL performance measured IPS remediation.

Simplified Operations

Efficient and centralized operations achieved through a unified, single pane that automates operations across large (100k+) networks to achieve better economics.

Why Cloud4C NGFW?



Unparallel Enterprise Grade Security Capabilities

Hybrid IT
VDOM & HW accelerated VXLAN

Application Protection
Integrated WAF

Cloud on Ramp
100G Elephant Flows

Secure & Superfast DCI
40+Gdps per Tunnel

Latency Sensitive Applications
Single Digit microsecond latency

High Performance Edge
Full BGP with multiple ISPs

Hosting DMZ
HW assisted Load Balancing

Operation Resiliency
Hardware Level DDos Protection

Managed Support for Cloud4C NGFW

In addition to having the industry's best next-generation firewall, an enterprise must also have the required skill and knowledge to manage and monitor the tools to ensure maximum network security. Here's what makes Cloud4C not only your trusted NGFW advisor but a holistic partner that offers the right support:

Automation-enabled support

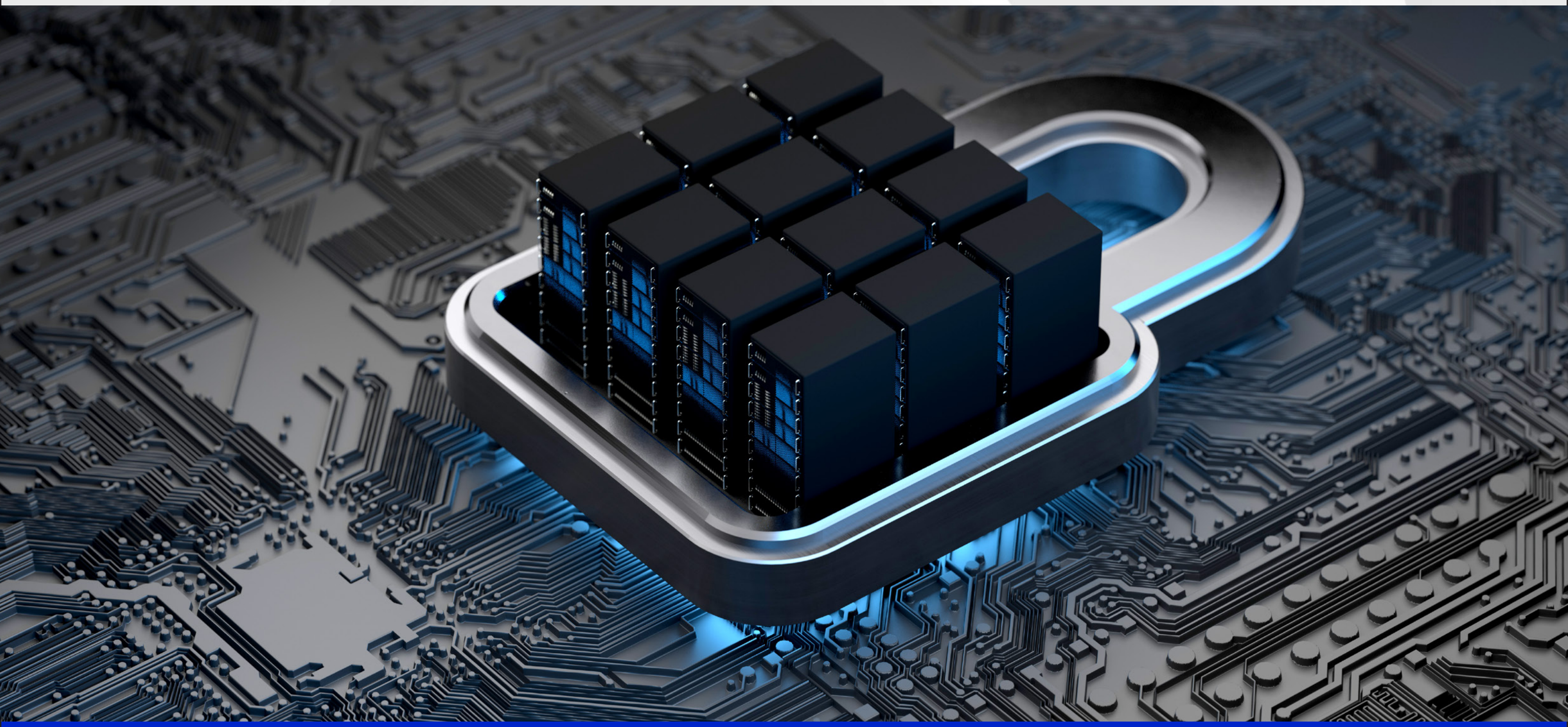
To increase operational efficiency and effectiveness while reducing truck-roll costs, accelerate speed of operations as well as eliminate costly human errors.

Hyperscale security for data center protection

Industry's highest security compute rating and most energy efficient data center protection.

External services connected with ease

We help you bring external services onto the cyber security platform while also syncing security beyond the security solutions to reduce overall enterprise risk.



Assessment Workshop

Before you switch to Cloud4C Next-generation Firewall, here’s a comprehensive assessment workshop to help you gain insights to your present enterprise security landscape.

CAF Security Assessment Workshop Scope & Deliverables

Scope	• CAF workshop focused in Security and Compliances • Discuss industry specific compliances required for the organization • Understand the current compliance control mapping • Assessment of tools configuration mapped against complaince control mapped • Identity Gaps in current compliance control and prepare check list • High-level assessment of cloud governance • CAF based security recommendation covering-Revised Tools mapping (Cloud Native), recommended security tools configuration & Governance policy
Deliverables	• Security Assessment Report ▶ Recommendation on security control mapping (remapping) against tools ▶ Recommendation on governing Industry specific compliance controls & maintenance of controls green state ▶ Remediation plan • Landing Zone (MVP) • Remediation SOW
Dependencies	• Stakeholders and required access to information and tools
Delivery Structure	• 3 to 6 hour interactive workshop and Cloud native Tool assessment (CAF and War) • CIS 20 Benchmarking Assessment • 1-2 days internal processing to create the Report • 2 hours report walk through and agree next steps

Connect With Us Now

info@cloud4c.com | www.cloud4c.com