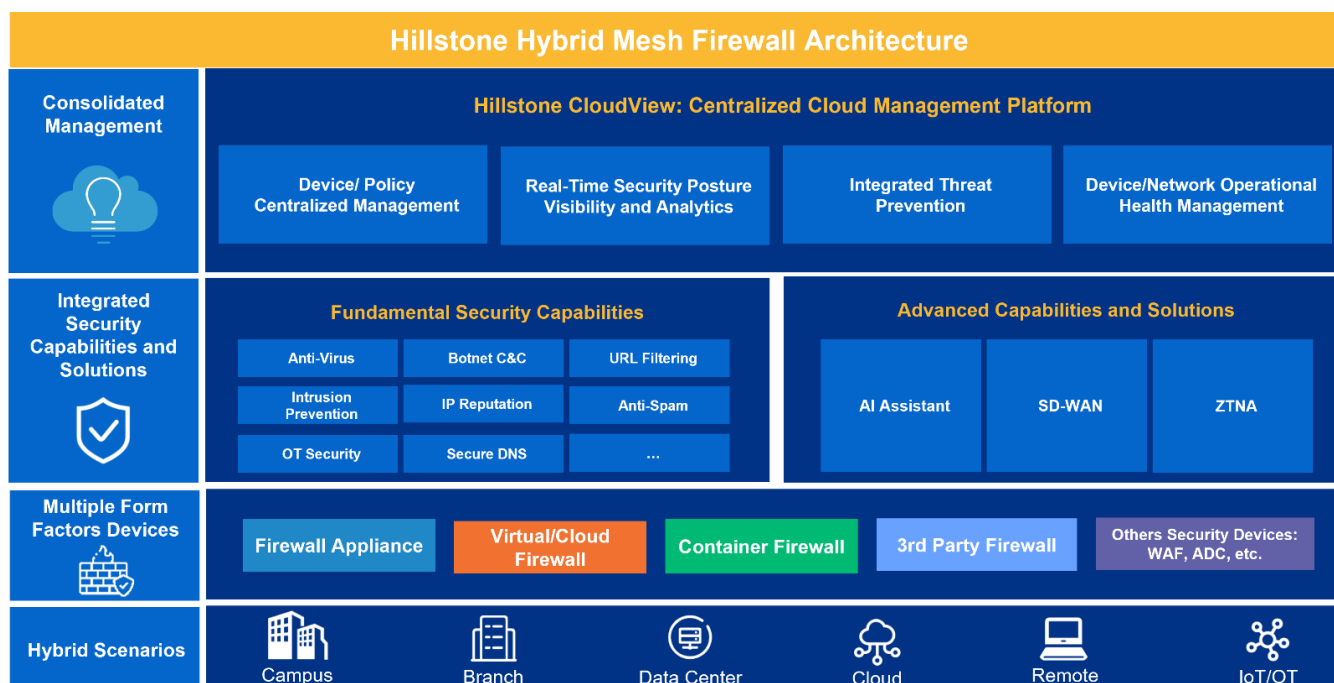# Hillstone Hybrid Mesh Firewall (HMF) Solution

Secure Hybrid Enterprises

Today's enterprises face unprecedented cybersecurity challenges amid shifts to hybrid cloud and edge computing, where sophisticated threats exploit fragmented visibility across borderless boundaries. Disjointed point products often create operational friction and dangerous "security gaps". Hillstone's Hybrid Mesh Firewall (HMF) solution addresses these risks by unifying Hillstone's hardware, virtual/cloud, and container firewalls into a single, cohesive security fabric. Centrally orchestrated via Hillstone CloudView—HMF cloud manager, it enables centralized management for device and policy, real-time multi-dimensional visibility and analytics, as well as integrated threat prevention to ensure a robust, identical security posture across the entire digital estate and distributed network environment. By consolidating diverse security resources, Hillstone HMF eliminates management complexity while providing a scalable, adaptive foundation that transforms modern security into a streamlined, high-performance driver for continuous business growth across all dynamic deployment modes in the hybrid environment.
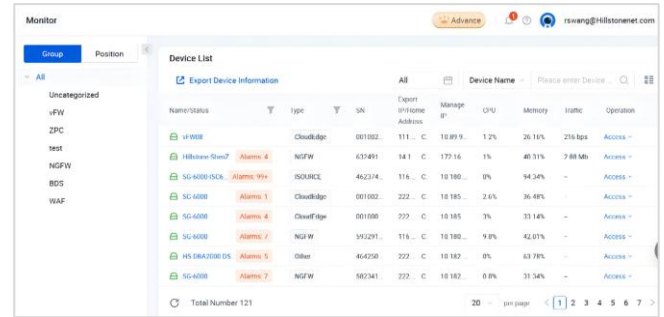
Hillstone Hybrid Mesh Firewall Architecture

Consolidated Management

Hillstone CloudView: Centralized Cloud Management Platform

Device/ Policy Centralized Management	Real-Time Security Posture Visibility and Analytics	Integrated Threat Prevention	Device/Network Operational Health Management

Integrated Security Capabilities and Solutions

Fundamental Security Capabilities

Anti-Virus	Botnet C&C	URL Filtering
Intrusion Prevention	IP Reputation	Anti-Spam
OT Security	Secure DNS	...

Advanced Capabilities and Solutions

AI Assistant	SD-WAN	ZTNA

Multiple Form Factors Devices

Firewall Appliance	Virtual/Cloud Firewall	Container Firewall	3rd Party Firewall	Others Security Devices: WAF, ADC, etc.

Hybrid Scenarios

Campus	Branch	Data Center	Cloud	Remote	IoT/OT

Solution Highlights

## Centralized Cloud-based Management

Hillstone CloudView serves as the centralized orchestration hub for the HMF architecture, delivering a one-stop SecOps experience through a simplified "register-and-use" model. It provides centralized management and consolidated control across all firewall form factors and other security products such as WAF, ADC, etc. CloudView enables unified policy management through a single pane of glass to synchronize consistent security across hybrid environment. Additionally, its native CI/CD integration automates security provisioning, embedding protection directly into DevOps pipelines. By integrating real-time security posture monitoring, risk asset management, threat prevention and proactive health analytics, it transforms fragmented environments into a cohesive, automated security fabric, ensuring streamlined operations and unprecedented visibility across the entire hybrid environment and digital assets.

- SaaS-native Simplicity: As a SaaS service hosted on a public cloud infrastructure, Hillstone CloudView enables customers to access the service from the web from anywhere at any time from any devices. This empowers the customer to monitor network without any physical limitation, delivering optimal experience along with optimized security management and operational efficiency in distributed environments.

- Centralized Device Management: Hillstone CloudView delivers consolidated control over all firewall form factors—hardware, virtual, cloud, and containerized deployments. By providing a "single pane of glass," CloudView empowers organizations to manage diverse security assets as a cohesive fabric, significantly reducing operational complexity and ensuring total visibility across the entire digital estate.
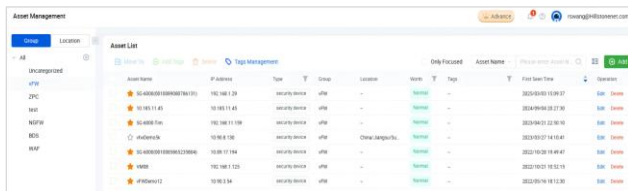

- Unified Policy Management and Orchestration: Hillstone CloudView orchestrates a unified security posture by extending granular and unified policy control across Hillstone's native firewalls, and policy configuration for third-party cloud firewall such as AWS. This normalizes security rules across multi-vendor environments, ensuring consistent enforcement and closing visibility gaps throughout the hybrid mesh fabric.

- Security Posture Monitoring: Hillstone CloudView delivers a holistic view of the HMF security posture, visualizing real-time metrics on top threats and incidents vectors, compromised assets, network and device status, resource utilization, etc. With the granular data, CloudView can proactively identify risks and anomalies in the hybrid environment, ensuring a resilient, consistent security posture for HMF architecture.
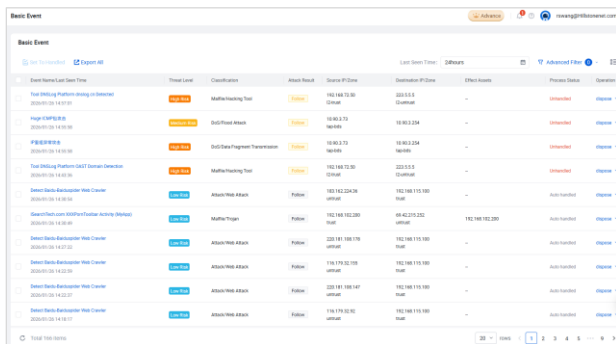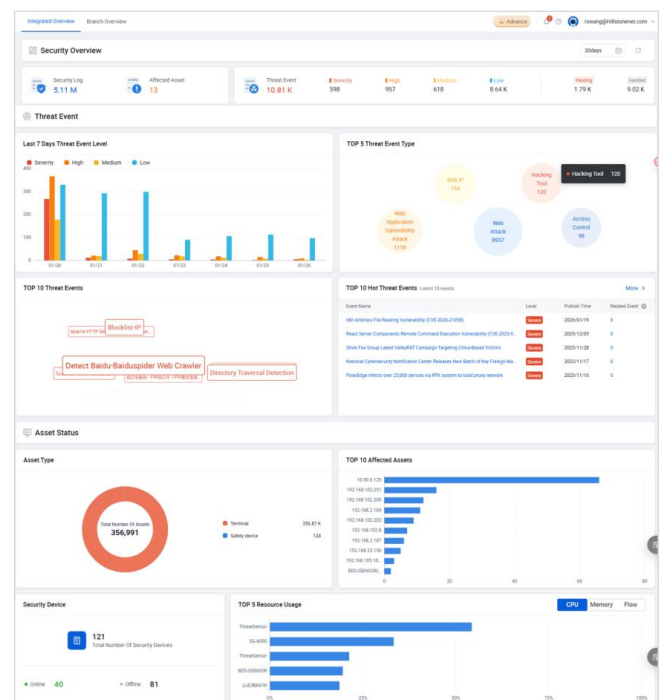
Solution Highlights (continued)

- Risk Asset Management: Hillstone CloudView empowers proactive defense through dynamic risk assessment, continuously evaluating asset status to instantly identify compromised endpoints. By transforming threat data into actionable mitigation strategies, it allows the HMF architecture to surgically isolate risks.

- Threat Monitoring, Analysis and Prevention: CloudView delivers comprehensive threat visibility by correlating global intelligence with granular event analysis to detect anomalies in real-time. It triggers a coordinated response across the security products in entire HMF ecosystem to automate mitigation. This synchronization transforms isolated defenses into a unified, proactive shield against sophisticated, multi-vector attacks.


- CI/CD Integration: Built for modern agility, CloudView seamlessly integrates into CI/CD pipelines to automate security provisioning. It allows enterprises to embed threat prevention and compliance checks directly into the application lifecycle, transforming security from an operational bottleneck into an automated, scalable enabler for business growth.

Industry-leading Hardware Security Foundation

Hillstone delivers a comprehensive, industry-leading portfolio of hardware firewalls engineered for diverse environments. From corporate edges (NGFW and SD-WAN) to high-traffic data centers (Data Center Firewall for Tbps-level east-west traffic) and harsh industrial sites, our appliances provide the high-throughput, massive concurrent connections and low-latency foundation required for modern organizations.

- Advanced Hardware Architecture: Hillstone firewall appliance features compact form factor and a powerful computing foundation that ensures high performance with uncompromising security.

- Comprehensive Security Capabilities: Hillstone firewall appliances consolidate security into a cohesive fabric by integrating rich security functions including IPS, AV, URL filtering, botnet C&C, DDoS, etc. This eliminates security gaps, providing advanced threat prevention and consistent protection across all physical deployments.

- Hillstone Proprietary ASIC: Powered by self-developed ASIC, Hillstone firewall hardware delivers high-density interfaces, high-performance, ultra-low-latency, and energy efficiency while ensuring maximum stability. This hardware-accelerated approach drives innovation, meeting the rigorous scalability and elastic protection demands of modern enterprise hybrid infrastructures.
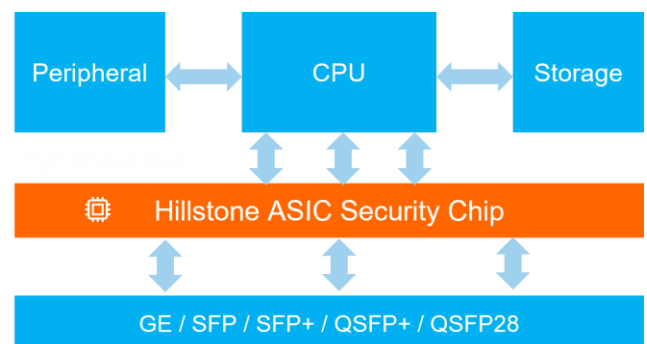

Comprehensive Cloud Infrastructure Protection for Virtualized Workloads

Hillstone CloudEdge provides the elastic cloud security foundation for the HMF solution, delivering robust, high-performance protection across private, public, and hybrid cloud environments. Supporting major hypervisors like VMware and KVM, alongside public clouds such as AWS and Azure, it enables rapid, scalable deployment to meet dynamic enterprise business needs in virtualized environments. CloudEdge

Solution Highlights (continued)

effectively eliminates security blind spots by inspecting North-South and East-West traffic, delivering consistent inspection via core StoneOS technology shared with hardware firewalls. By supporting automated instantiation and API-driven orchestration, CloudEdge delivers elastic, granular security that moves with workloads to ensure zero-gap protection throughout the hybrid mesh fabric. This synergy streamlines operations and reduces complexity, transforming multi-cloud environments into a secure foundation for continuous business growth.
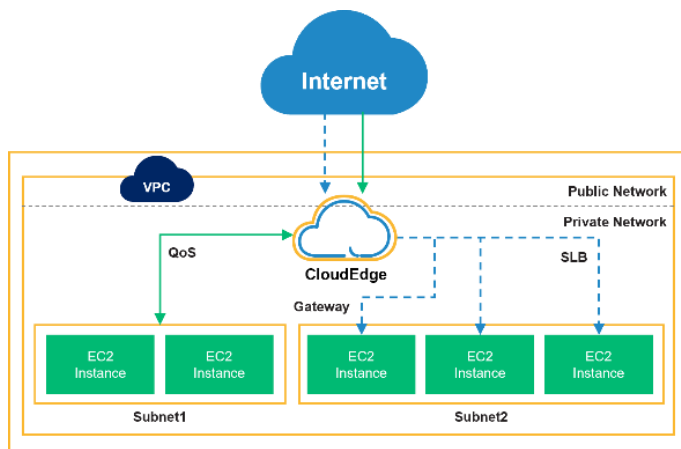
### Purpose-built Container Security Foundation

Hillstone CloudArmour delivers purpose-built container security, serving as the essential container firewall within the HMF architecture. It extends advanced, zero-trust protection to cloud-native workloads across Kubernetes and multi-cloud environments. By integrating real-time asset management and continuous image scanning, it ensures only verified artifacts enter production. With the capabilities of granular micro-segmentation for Kubernetes and real-time runtime protection, it effectively secures lateral east-west traffic, eliminating the visibility blind spots inherent in modern application delivery. In addition, CloudArmour leverages attack surface management and policy simulation with traffic modeling to enable

automated, data-driven policy generation. The synergy allows HMF to maintain a consistent, high-performance security posture from physical edges to microservices, empowering enterprises to accelerate digital transformation with streamlined compliance and scalable defense.
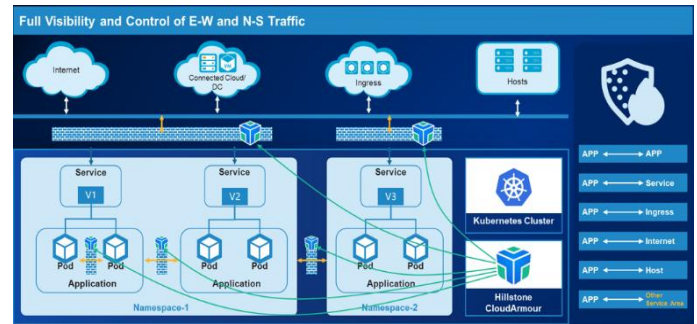
AI-Driven Intelligent Operations and Analytics

Hillstone AI platform seamlessly integrates AI computing resources, foundation models, and security agents to deliver full-stack intelligence across SecOps, operation and maintenance (O&M), data governance, etc. Hillstone AI assistant on firewall acts as an intelligent co-pilot, transforming complex O&M into a streamlined, conversational experience. It provides real-time threat event analysis, automated policy optimization, and guided configuration and troubleshooting, alongside proactive device health monitoring and contextual knowledge retrieval. These capabilities drastically enhance O&M efficiency and accuracy, enabling administrators to resolve complex issues with precision. By embedding this intelligent layer into the hybrid mesh fabric, Hillstone simplifies the orchestration of diverse environments, transforming security from a source of operational friction into a streamlined, adaptive foundation for business growth.
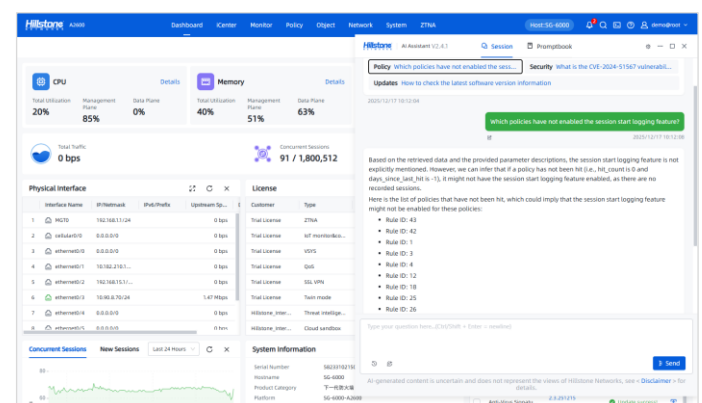
Solution Highlights (continued)

Advanced Security Capabilities and Converged Solutions

The Hillstone HMF architecture supports multiple critical enterprise solutions and security capabilities including SD-WAN and Zero Trust Access control (ZTNA), and secure DNS. These integrated solutions and capabilities ensure a consistent security posture across every corner of the modern hybrid network.

• Secure DNS: Hillstone Secure DNS provides a proactive defense layer within the HMF architecture, neutralizing advanced threats at the query stage. Utilizing ML-based analytics, it identifies sophisticated DGA and DNS tunneling attempts, while rich threat intelligence enables real-time blocking of phishing and malware. With integrated DNS sinkholing, it rapidly isolates infected devices and automates incident response, ensuring a resilient and unified security posture throughout the entire hybrid mesh fabric.
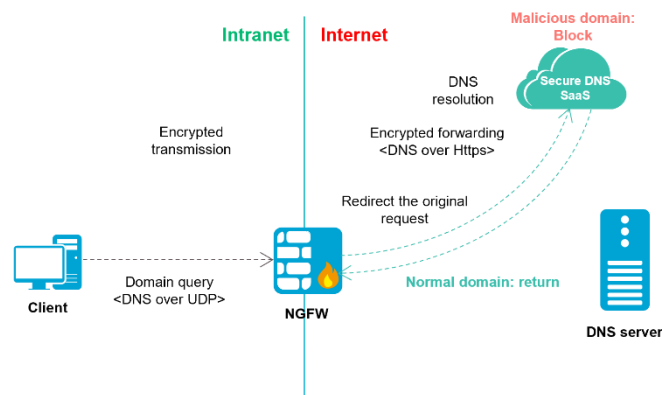
• Secure SD-WAN: Hillstone's SD-WAN solution provides robust, comprehensive enterprise security to mitigate SD-WAN risks. The solution offers not only the visibility to see into network traffic, but also the ability to understand traffic context, and the capability to take action, protecting traffic at the edge. In addition, in provides centralized management, zero-touch provisioning, and superior QoS with active link monitoring for fast, simplified deployment, operation and protection for SD-WAN networking with enterprise-grade security foundation.
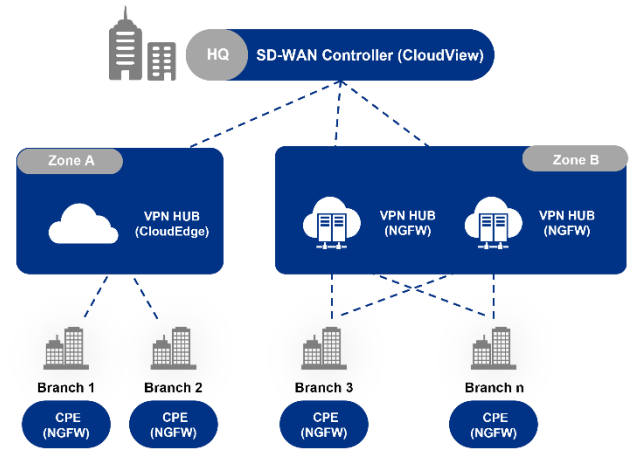
• Universal ZTNA: Built on Hillstone award-winning enterprise-grade firewall foundation, Hillstone ZTNA delivers comprehensive endpoint visibility, and identity-aware, least-privileged, context-aware adaptive access control across the distributed environments. Featuring centralized management and high-availability distributed gateways with up to 24 backups, it ensures a consistent security posture and seamless experience. Hillstone ZTNA effectively secures remote access while significantly reducing operational complexity for diverse, hybrid environment.