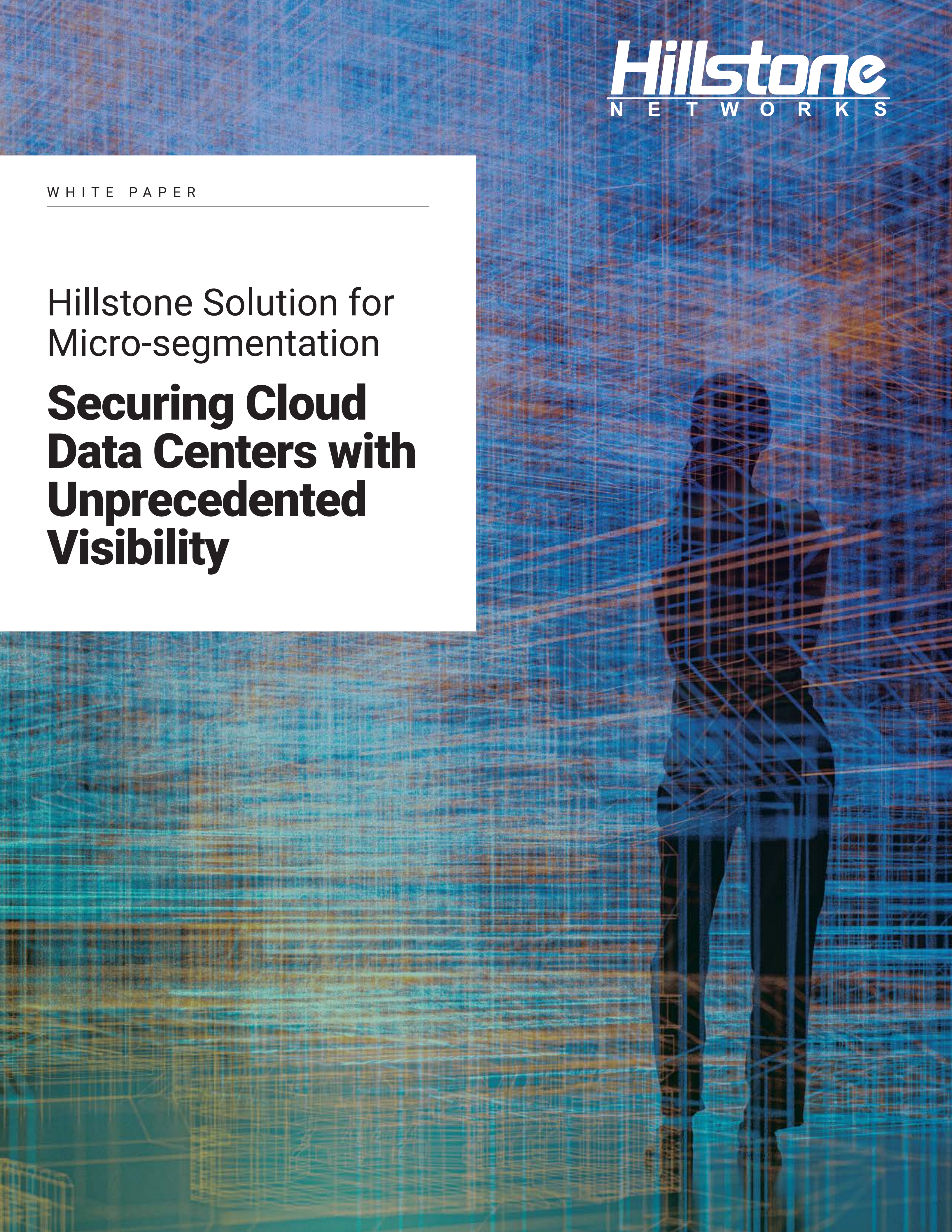

WHITE PAPER

Hillstone Solution for Micro-segmentation

Securing Cloud Data Centers with Unprecedented Visibility

Introduction

There are some clear trends that have greatly altered the data center cybersecurity landscape as datacenters have evolved from physical to virtual, enterprise to cloud, including:

Multitenancy The days of a data center serving a single organization are fading fast. Today's virtual and cloud enabled data centers—whether private, public, community or hybrid—are more likely to serve several organizations, subsidiaries or departments. Examples include government agencies, healthcare organizations or other entities sharing a single community cloud or hundreds of unrelated organizations taking advantage of public cloud infrastructures and applications.

With multitenancy, an organization may be served by scores of virtual machines and applications that share not only the same datacenter but the same physical servers with other clients (tenants). To prevent data breaches and the spread of malware from tenant to tenant, each organization's virtual infrastructure must be isolated and protected from that of the other organizations sharing the same cloud, network or server.

Multicloud The concept of the datacenter as a physical place has faded as organizations have extended infrastructure and applications across public, private, and multiple clouds. Today, even a single business process or application may depend on infrastructure and components that span multiple cloud services and cloud deployment types.

North-South and East-West Traffic In the early physical days of the data center, security was mostly about monitoring and securing traffic entering and exiting a well-defined network perimeter. Today, east-west traffic among virtual machines, web services and applications sharing the same data center and physical servers is just as or even more common, not only among different tenants but also with respect to servers and components of a single web-based or other composite application and microservices. Without proper protection, threats to one component or web service can easily infect the others.

Contents

Security Requirements in the Era of the Cloud Data Center 3

Hillstone CloudHive 5

The Many Benefits of Hillstone CloudHive 6

Conclusion 8

Software-Defined Networks and Network Functions Virtualization For many years, virtualization was mostly about servers, applications and storage. Today, the network has caught up, with network hardware morphing into virtual and software-defined networks. Software-based networks have obvious advantages in standardization, agility and mobility. But on the flip side, today's SDN and NFV solutions are often still catching up with the robust security of legacy network hardware developed over decades; although that security that was often difficult to configure and maintain.

Mobility and Elasticity Virtualization has enabled the dynamic, endlessly elastic mobile data center, with virtual machines, storage and network resources deploying, expanding, contracting and migrating at will. Securing such a dynamic data center environment with fixed, appliance-based solutions is not a viable strategy. It's possible to detour all VM-to-VM and tenant-to-tenant traffic through a fixed security solution, but such a strategy is inefficient and difficult to manage. It also comes with a negative impact on latency and application performance, slowing down the pace of business.

The net challenges from these trends boils down to this: how do you insert security functions deep into a shared, virtualized, dynamic, elastic environment?

Security Requirements in the Era of the Cloud Data Center

It's evident that the cloud-enabled data center needs a new security strategy and solutions that address these challenges with minimal performance impact. Such a solution must offer the following capabilities:

A Cloud-Enabled Solution Any security solution that supports a cloud platform must be as virtual, flexible and elastic as the infrastructure it serves. It should be hypervisor-aware and able to insert itself deeply into the virtual environment, protecting communications among virtual resources as they deploy, grow, shrink and migrate across the data center. It should be tightly integrated with virtual and cloud management and orchestration platforms such as VMware vCenter, and with hypervisors such as ESXi, and offer cloud-friendly APIs such as a RESTful API so that it can secure infrastructure and applications across a multicloud environment. While management platforms such as vCenter allow IT teams to configure vLANs to segment different users and virtual machines, the configuration process is still manual and tedious. A virtual security solution must be able to isolate traffic quickly and easily in an automated fashion based on policy and an assumption of constant change.

Comprehensive North-South and East-West Visibility When security was primarily for north-south traffic, in-network physical firewalls were a viable solution. A virtual, cloud-based solution must have deep visibility and insight into all north-south as well as east-west traffic among virtual servers, including the virtual network, virtual machines and applications. And, it must have the tools to display all that information clearly and draw attention to abnormalities and potential security issues in a format that makes it easy for IT teams to consume—to detect and address. When network or service performance issues occur, the datacenter admin or tenants should be able to quickly locate the root cause and resolve it with the help of traffic visibility.

Scalability and Elasticity The mobile, highly elastic virtual data center needs a mobile, highly elastic as well as scalable security solution that binds policies to each and every VM, remaining with each VM as it is deployed, moved or migrated—without any impact on security or application performance. Because of the constraints of manual configuration and physical network deployment, legacy security solutions were not designed to keep up with the fast, dynamic pace andrequirements of the cloud data center, where workloads can be orchestrated, provisioned, scaled, migrated and automated at a pace never seen in traditional networks.

Multifunctional L2-L7 Security As malware and data breaches grow increasingly sophisticated, concealed and able to bypass traditional security solutions, the days of security addressed by a single application, tool or technology have long passed. For a cloud security solution to be successful, it must leverage multiple security strategies and capabilities, including access control, application identification and detection, as well as firewall, intrusion prevention and malware protection, among others. And again, the solutions must address all these capabilities with minimal performance impact.

Micro-segmentation technology has been the panacea for securing cloud data centers. With this technology, security admins can segment the data center into distinct areas and then define and deliver security policies for each of these areas, down to a VM or a workload. However, not all micro-segmentation solutions are the same.

CloudHive

Hillstone CloudHive is an advanced micro-segmentation solution designed from the ground up for the demands of cloud data centers. Using advanced micro-segmentation and a standard cloud orchestration API, CloudHive integrates its visibility and security capabilities deeply and seamlessly into the virtual environment. It monitors and addresses all north-south and east-west traffic to detect, isolate and eliminate malware, potential data breaches and other security issues before they can spread across VMs in virtualized networks.

CloudHive automatically scales its virtual security resources exactly where and when they are needed, binding and enveloping all VMs as they're deployed, moved or migrated across the virtual data center. All of the CloudHive components are VM- and software-based. To distribute and scale the security service in a flexible manner with minimal performance impact, the CloudHive architecture separates security functionality into four different planes, as illustrated.

CloudHive's asset discovery feature automatically creates a visual map of all data center and multicloud resources—including virtual networks, virtual machines (VMs), and all the connections between them. Its mapping capability presents IT teams with comprehensive views of all application traffic flow, traffic types and potential threats across VMs. Tight integration with existing cloud orchestration platforms such as VMware vCenter and OpenStack ensures rich, real-time contextual visibility across multiple clouds and allows security resources to grow or shrink alongside the virtual resources to be secured.

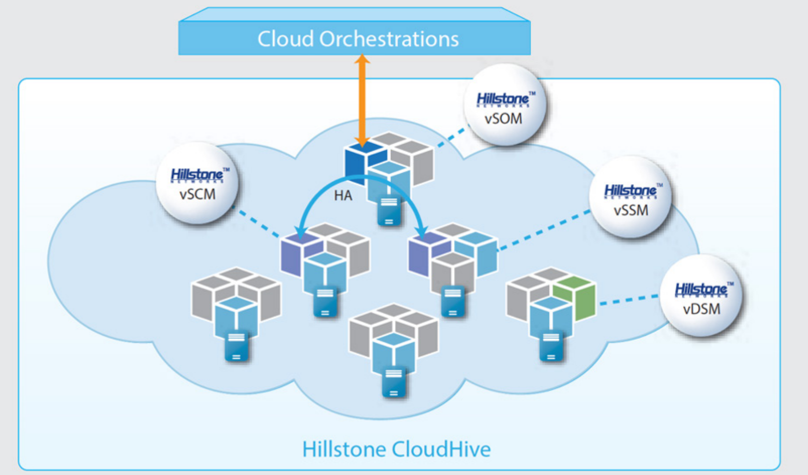

Figure 1. CloudHive Deployment Architecture

- **vSOM** (Virtual Security Orchestration Module) is responsible for managing the CloudHive security service life-cycle and dynamically sensing cloud platform transactions.
- **vSCM** (Virtual Security Control Module) is responsible for security configuration management and flexible scheduling of vSSM.
- **vSSM** (Virtual Security Service Module) is responsible for performing specific security functions such as access control and attack prevention.
- **vDSM** (Virtual Data Service Module) is responsible for efficiently forwarding the logs generated by vSSM to an external Syslog server.

Built on the Hillstone security foundation, Hillstone CloudHive provides not only comprehensive visibility, but also security to cloud data centers. This multi-layered security defense architecture can identify advanced threats and attacks in a timely manner.

Next Generation Firewall CloudHive leverages Hillstone's next generation firewall benefits, including Layer 7 VM and port-based access control across the entire cloud and virtual environment.

Intrusion Prevention Hillstone IPS features include protocol anomaly; rate based; custom attack signatures; and DOS attack detection and prevention. It filters threats based on severity, target, OS, application or protocol.

Anti-Virus CloudHive provides signature and flow-based antivirus capabilities, including compressed file scanning.

Sandbox CloudHive provides comprehensive file security analysis, effectively detecting and preventing the spread of malicious files.

URL filtering This feature delivers web page access control based on IP, VM, or service group attributes, with real-time update of URL signature database.

Attack Defense This includes port scans and anti DoS/DoS SYN Flood, DNS Query Flood, abnormal protocol and ARP attacks.

IT and security teams can take advantage of one of two CloudHive deployment modes for a seamless deployment experience:

TAP mode non-intrusively monitors traffic via mirroring without policy enforcement. It can serve as a viable first step in providing IT teams with deep visibility into network resources and traffic flow via asset discovery, VM traffic monitoring, and logging.

Transparent mode (or inline mode) is typically used as a subsequent step to inspect traffic and enforce security policies.

The Many Benefits of Hillstone CloudHive

The Hillstone CloudHive distributed security architecture has several benefits:

Scalability and Mobility Separating management, control and security deployment allows each function to scale independently of the others, applying the appropriate level of resources precisely where it is needed. Since all services are elastic and distributed throughout the virtual environment, they are always close to the virtual resources that they protect. This allows for policy enforcement without the traffic detours that typically add latency and impact performance. CloudHive applies security services on demand to any and all new workloads and VMs. The vSCM deployment unifies security policy configuration across the data center, and the policies will also automatically adapt to changes in the environment.

To prevent any service disruption or delay, the CloudHive control plane harnesses Hillstone's distributed architecture, vMotion awareness and a patented flow session distribution technology to maintain state as

VMs grow, shrink or move across multiple clouds.

Comprehensive Visibility CloudHive's asset discovery feature automatically delivers a comprehensive display of cloud networks, VMs and virtual network traffic, displaying all inbound and outbound traffic and highlighting communication paths, traffic types and trends on each path. CloudHive's Service Performance Monitoring (SPM) feature monitors key network and service performance metrics on selected network paths and services for both east-west and north-south traffic. It can flag negative performance trends and help admins take early action to avoid service disruptions. Or it can directly pinpoint the source of performance issues among multi-tier service architectures.

CloudHive offers real-time visibility and control of the VM topology, east-west and north-south traffic, applications and inter-VM attacks. CloudHive's visualization and report logs allow enterprises and Cloud Service Providers (CSPs) to meet any and all compliance, security audit, and policy reviews, as well as threat vulnerability analysis and remediation requirements.

Multifunction L2-7 Security CloudHive protects all VM-bound traffic and inter-VM traffic with L2-L7 security services, including firewall features such as policy control and session limits, Intrusion Prevention, URL Filtering, Anti-Virus and Attack Defense (AD), with fine-grained application control. Real-time mitigation capabilities block, impede or quarantine active attacks. The vSSM component secures all VM directed traffic—both north-south and east-west—enabling 100% traffic security coverage and a zero-attack surface.

Hillstone CloudHive's agility and comprehensive security capabilities uniquely differentiate it among other micro-segmentation solutions. Customers reap the benefits of complete Layer 7 protection without the need for any change in their existing cloud network configuration. CloudHive delivers protection without comprise for business continuity.

Low Total Cost of Ownership The CloudHive components install non-disruptively, allowing security services to be added or removed simply by adding and removing VMs from security services (vSSMs) distributed across the physical servers.

CloudHive's Layer 2 deployment does not impact existing network topology. Along with unique configuration optimization tools and features, it minimizes deployment and configuration overhead, without business impact or network interruption. In addition, the advantage of having a single appliance reduces operational errors and improves overall management efficiency. The total cost of ownership is also reduced as CloudHive security services do not require upgrades or an expansion of existing cloud platforms.

Conclusion

Today's cloud data centers provide a raft of security challenges that did not exist in legacy, physical data center environments. Hillstone CloudHive's distributed, virtual security solution provides unprecedented cloud asset and traffic visibility, reducing the data center threat surface to near-zero. It offers the deployment flexibility, elasticity, and orchestration integration that are mandated by cloud environments at a lower total cost of ownership.

Furthermore, CloudHive seamlessly integrates with major virtualization platforms including VMware and Openstack, and has achieved the VMware Ready Certificate with NSX integration.

By inserting and integrating components deeply and seamlessly into the virtual environment, Hillstone CloudHive delivers robust, dynamic, effective, scalable, efficient and non-intrusive security for today's cloud data center.

About Hillstone Networks

Hillstone Networks' Integrative Cyber Security approach delivers coverage, control, and consolidation to secure digital transformation for more than 26,000 enterprises worldwide. Hillstone Networks is a trusted leader in cyber security, protecting enterprise critical assets and infrastructure, from edge to cloud, regardless of where the workload resides. Recognized as a Visionary in Gartner's Magic Quadrant for Network firewalls, Hillstone Networks' entire suite of cyber security solutions is relied upon in many of the world's most challenging technology environments.

Hillstone NETWORKS

Visit **www.hillstonenet.com** to learn more

or contact Hillstone at **inquiry@hillstonenet.com**