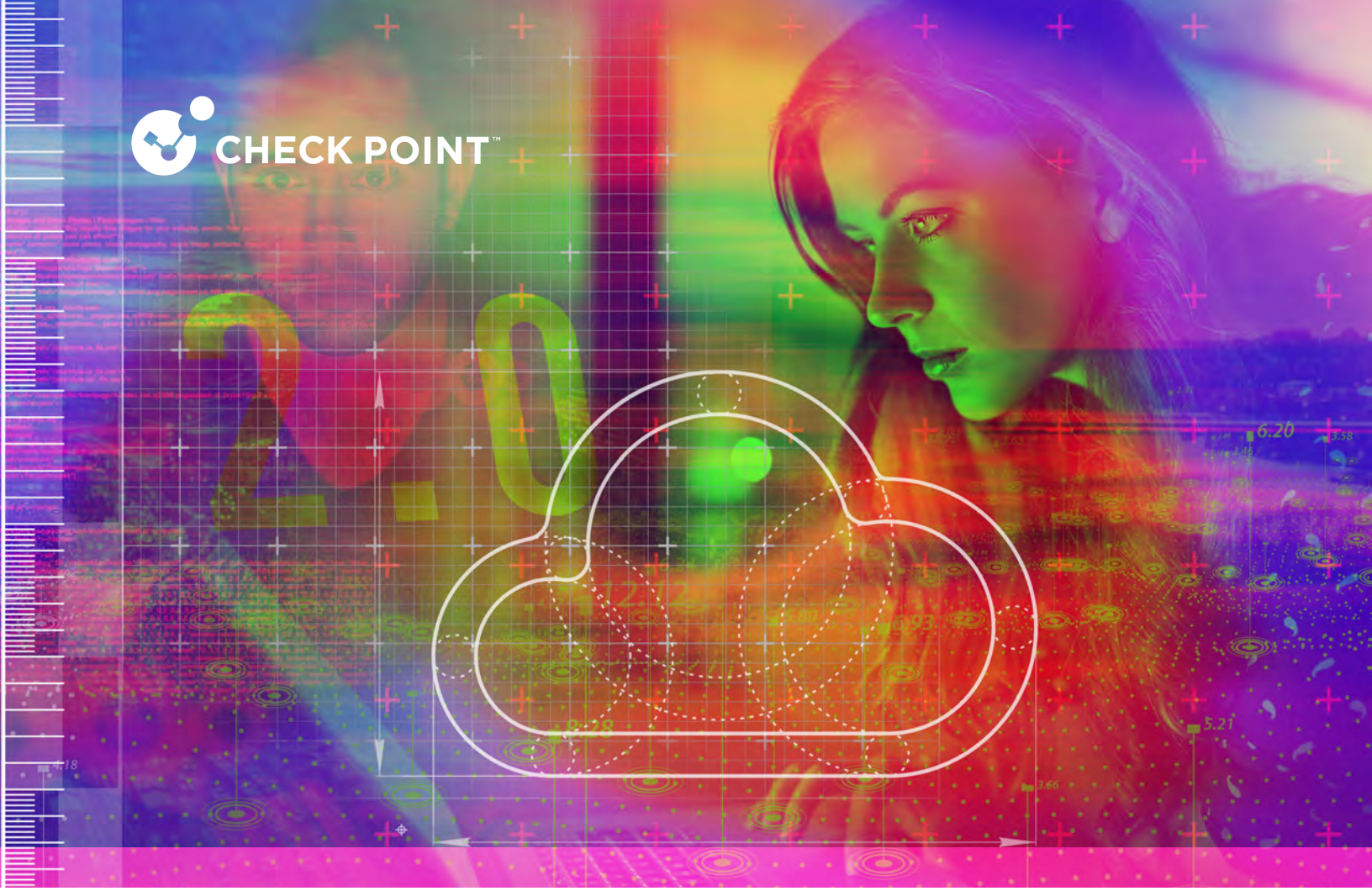

CLOUD SECURITY BLUEPRINT 2.0:
ARCHITECTURES AND SOLUTIONS

Contents

Introduction

In Introduction to Cloud Security Blueprint 2.0 we discussed the basic concepts (Shared Responsibility model, Zero Trust) as well as the advanced challenges that must be addressed by a modern cloud security architecture. Those challenges include increased attack surfaces, diminished visibility, dynamic and ephemeral workloads, automated DevOps processes, excessive privileges, and multiple cloud environments.

We then described cloud security architectural principles that are essential in order to meet those challenges effectively. These principles include:

- Advanced threat protection for network perimeter security
- Securing other attack vectors such as identity, control plane, and data
- Security by design: Designing the architecture in a way that preserves security as part of the environment itself, in addition to configuration-based controls
- Segmentation to minimize attack surfaces and reduce the blast radius
- Agility, automation, elasticity without compromising security
- Borderless, agnostic to cloud platform specifics

In this second white paper we discuss Cloud Security Blueprint 2.0 architectures and solutions.

We first introduce the Check Point cloud security solutions which can be used to design a secure cloud deployment. We then show how these solutions address the cloud security challenges and architectural principles covered in the introductory white paper.

Advanced Threat Prevention and Cloud Network Security

Check Point CloudGuard Network Security (CGNS) provides advanced threat prevention security for applications and data in private, public, and hybrid clouds. CGNS is essentially similar to Check Point's security gateways for physical appliances, but adapted and configured specifically for deployment on cloud platforms and software defined data centers. The key features and benefits of using CloudGuard Network Security are:

- **Enterprise-grade advanced, multi-layered threat prevention security for dynamic, elastic cloud infrastructures**: Protects cloud services and applications from unauthorized access and denial of service attacks, provides secure connectivity to cloud resources, implements two-factor authentication for mobile access, prevents data loss, and protects against malware and zero-day attacks.

- **Borderless:** Works with multiple public cloud service providers (AWS, Azure, GCP, etc.) and software defined data center solution providers (VMware NSX, Microsoft Hyper-V, Openstack, Cisco ACI, Nuage Networks, etc.).

- **Rapid deployment:** Available in all leading public cloud marketplaces and supporting both Pay as You Go and Bring Your Own License models, deployment and configuration of CloudGuard gateways takes minutes. Provider-specific IT-authorized workflows and templates can be leveraged to ensure alignment with the corporate security ecosystem.

- **Agility through dynamic, automated policies:** Integrated with all leading public cloud management solutions, CloudGuard Network Security ensures that all cloud-defined elements such as asset tags, objects, and security groups are updated in real-time. Security policies are then adjusted automatically to changes in the cloud environment. In this way DevOps and Line of Business teams can be given the freedom to provision and consume cloud resources without compromising the corporate security posture.

- **Centralized management across cloud and on-prem infrastructures:** Enforce a consistent corporate security policy from a single management console, view security events across complex environments, and correlate events to applications and policies.

- **Consolidated logs and reporting:** End-to-end visibility and enhanced forensic analysis through consolidated logs and reports for hybrid cloud environments.

Introducing the Hub-and-Spoke Model

When designing a secure cloud environment using CloudGuard Network Security, it is strongly recommended to use the hub-and-spoke model. In order to achieve the cloud security architectural principles already described, in this model the environment is set up as a system of connections arranged like a bicycle wheel, in which all spokes are connected to a central broker (hub) and all traffic to and from the spokes traverses through a broker (hub). The blueprint design can be single hub or multiple hubs, as shown in Figure 1.

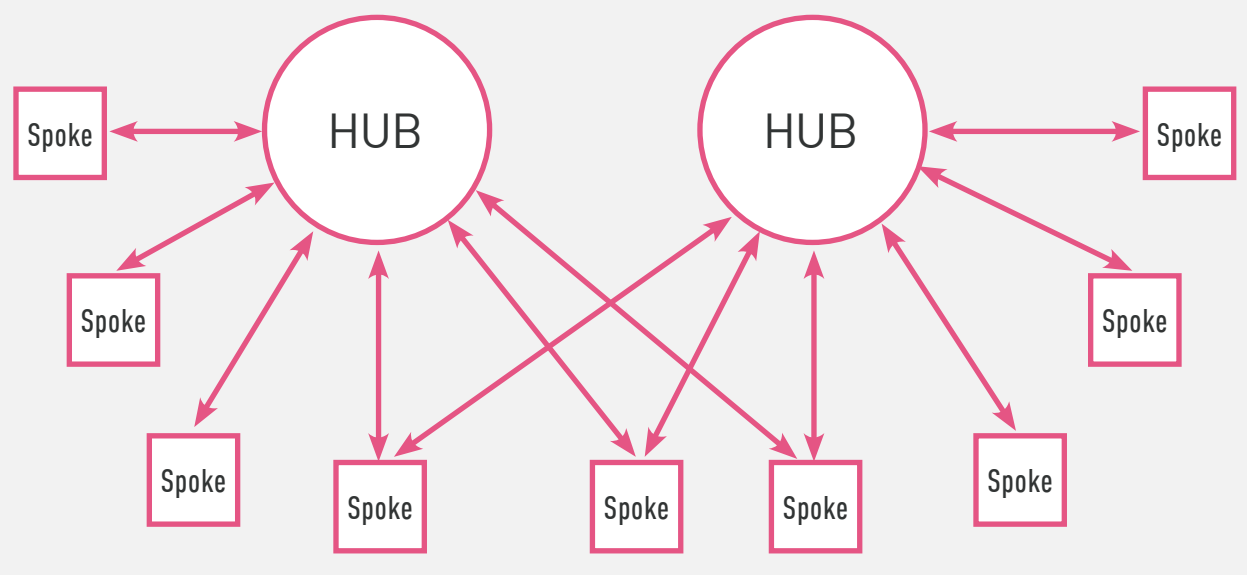

Figure 1: Hub-and-spoke model (multi-hub design)

The Spokes

A spoke is an isolated network environment that contains a collection of one or more network subnets from which workloads can be installed and run. A common spoke use case is several virtual servers that, together, comprise an application stack (i.e., web, application, and database). Another use case is a spoke that acts as an extension of an existing on-premises network, such as a set of QA servers for testing purposes or a set of data processing servers that utilize the cloud's on-demand provisioning to lower costs and improve agility.

Spokes are highly versatile and we have seen our customers leverage them in their environments for a wide range of use cases. The common denominator for these use cases, however, is that the spokes are the entities in which business activities are implemented in the cloud environment.

The Hubs

Figure 2 below illustrates a two-hub design that promotes flexibility and the systematic separation of communication types throughout the environment. One of the hubs is designated for incoming traffic from the Internet, while the other hub is designated for lateral traffic between spokes, traffic into and out of the corporate network, and outgoing traffic to the Internet or other cloud environments.

As with spokes, what we describe here are only the most common use cases. In reality, each customer implements its hubs according to its own unique needs and requirements. In the white papers in this series that describe how the model is deployed on specific cloud provider platforms, we provide the key alternatives and designs.

Traffic Flow Inside The Environment

In the two-hub design shown in Figure 2 below, the hubs are the only way in and out of the environment, as well as the only way to traverse inside and between spokes. The spokes are not connected to each other directly and are accessible only through one of the hubs.

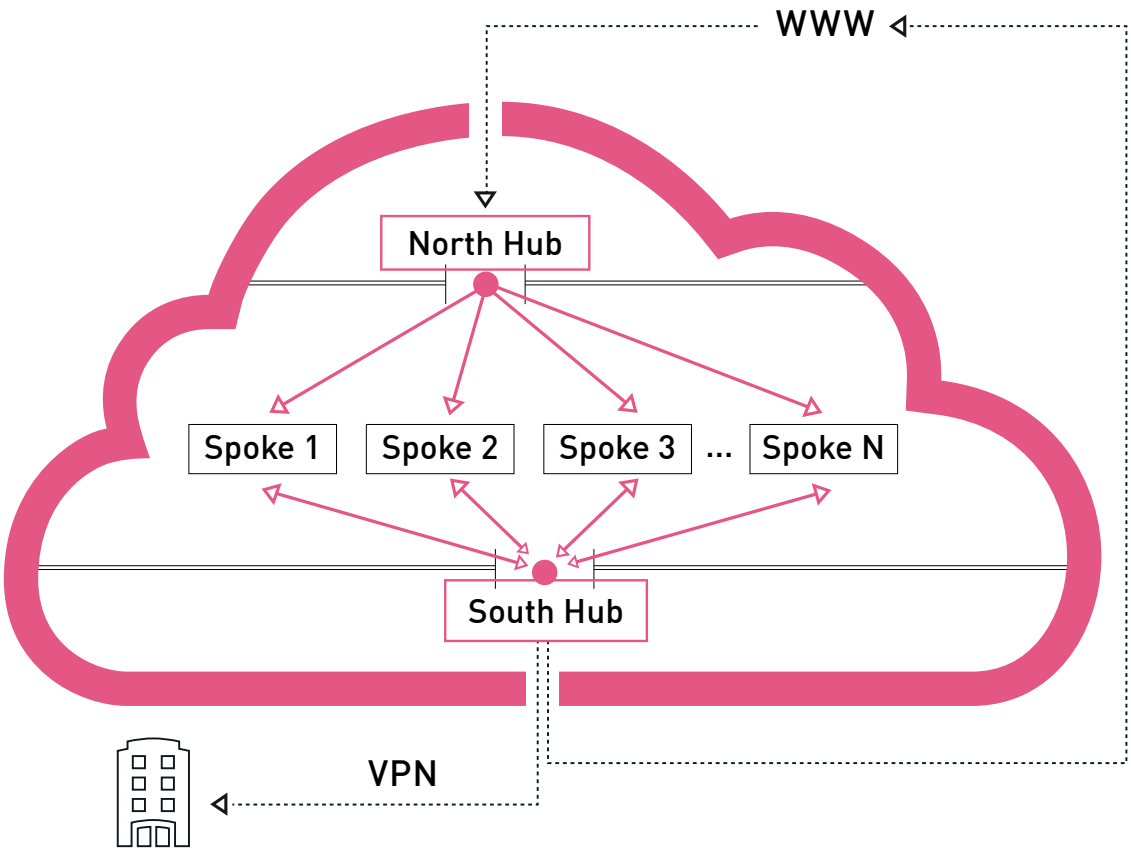

Figure 2: All traffic is routed through the hubs. The North Hub is for incoming traffic and the South Hub is for traffic to and from the corporate network, traffic to the Internet, and East-West access between spokes. Each spoke comprises cloud virtual machines with varying security and access levels.

Cloud Compliance and Orchestration

Now part of the CloudGuard family of products, CloudGuard Posture Management is an API-based SaaS platform that integrates natively with AWS, Microsoft Azure, GCP, and Kubernetes clusters deployed anywhere. CloudGuard Posture Management is a cloud security posture management (CSPM) solution for multi-cloud policy orchestration. CloudGuard Posture Management uses native cloud controls to implement compliance policies on each cloud. It lets an organization visualize and enforce its cloud security posture consistently across these public cloud services, ensuring compliance with cloud security best practices and regulations and helping to avoid configuration drift.

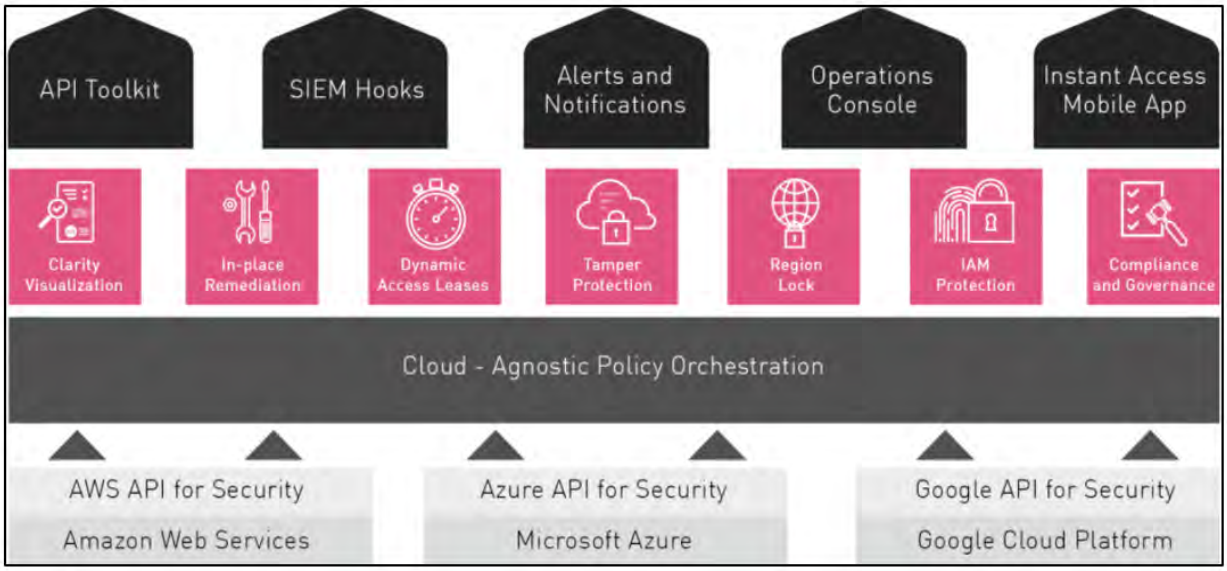

Figure 3: CloudGuard Posture Management Schematic

CloudGuard Posture Management capabilities and features play a particularly important role in upholding many of the key cloud security architectural requirements that underlie Blueprint 2.0, as described in the rest of this white paper.

Cloud Security Monitoring and Analytics

CloudGuard Intelligence is a cloud-native threat protection and security intelligence solution for the public cloud. It enriches cloud logs with context, transforms them into readable security logic, and enables security teams to take cloud security to the next level. Using CloudGuard Intelligence businesses can see every data flow and audit trail in today's elastic cloud environments and make sense of cloud data and activities to expedite investigation processes.

CloudGuard Intelligence delivers cloud intrusion detection, network traffic visualization and user activity analytics. Its object-mapping algorithms combine cloud inventory and configuration information with real-time monitoring data from a variety of sources including:

- VPC Flow Logs, CloudTrail, Amazon GuardDuty, AWS Inspector (for AWS customers)
- Azure vNET Flow Logs and blobs, Azure Monitor, Azure Advanced Threat Protection, Azure Security Center (for Azure customers)

as well as Check Point's ThreatCloud feeds, IP reputation and geo databases.

The outcome is rich contextualized information that is used for enhanced visualization, querying, intrusion alerts and notifications of policy violations. It can also be piped to third-party SIEM solutions, anywhere. With robust threat detection at core, CloudGuard Intelligence's CloudBots technology also extends remediation capabilities indefinitely – allowing you to create a custom response to any type of network alert or audit trail. CloudGuard Intelligence is the only platform that attributes network traffic to cloud-native ephemeral services such as:

- Amazon Lambda functions as well as other cloud-native platform components (RDS, Redshift, ELB, ALB, ECS) for AWS customers,
- Azure Automation functions as well as other cloud-native Microsoft Azure components (SQL Azure, Data Warehouse, Azure Virtual Machine, Azure Functions, and Azure Container Service) for Azure customers,

to provide a complete view and understanding of your cloud infrastructure across time.

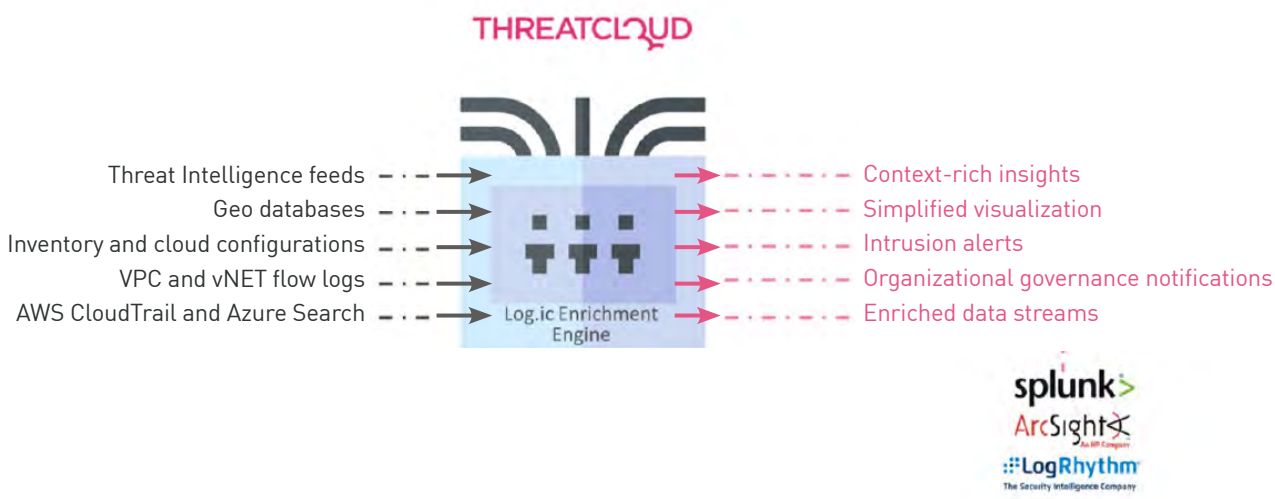

Figure 4: CloudGuard Intelligence schematic flow

CloudGuard Intelligence uses security best practices of signature detection, built-in rules, threat intelligence feeds and existing traffic flow to create a baseline of your network and user activity. It also uses AI and anomaly detection algorithms to spot potentially unauthorized or malicious activity within your cloud environments, including serverless applications. Log.ic can provide real-time policy violation and intrusion detection alerts based on user-defined criteria to the security admin team.

Feeding off of the world's largest IOC database: CloudGuard Intelligence leverages Check Point's ThreatCloud to enrich logs with intelligence from various feeds, including:

- 750M+ malicious hashes, sites and C&C addresses
- 11M behavioral signatures
- 2.5M daily detections
- Dozens of external feeds

Auto-remediation with CloudBots: CloudBots is a serverless framework that triggers a remediation function with a single click deployment, running entirely within your environment. Add CloudBots to create custom response to any type of network alert, audit trail, or other, and remediate threats at once with CloudGuard Intelligence.

CloudGuard Intelligence Explorer is a visual exploration tool that allows you to analyze the network activity and traffic traversing in and out of your cloud environment. You can choose from an extensive set of predefined queries or craft custom ones using CloudGuard Posture Management's expressive yet concise query language. The Explorer visualization feature lets you see every element and traffic in your AWS VPC or Azure vNET at a glance, and from there, zoom into the relevant entity or connection. Use CloudGuard Intelligence's rich contextualized visualization to fire: Deep investigation, Incident response, and Threat Hunting.

CloudGuard Intelligence's firehose connector feeds the enriched log traffic in a highly contextualized JSON format to various SIEM products for further investigation. Pipe into Splunk, ArcSight, LogRythm and more, to nurture with critical data on ephemeral assets and security posture awareness.

Blueprint 2.0: Architectural Principles and Solutions

The Cloud Security Blueprint 2.0 (as a high-level design) is applicable to all leading public cloud environments, including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure, Alibaba Cloud, IBM Cloud, and others.

In this section we explain in detail how the Blueprint 2.0 design can be implemented using Check Point products to uphold the cloud security architectural guidelines discussed in Introduction to Cloud Security Blueprint 2.0, such as protection across multiple perimeters (network, data, compute and identity), systematic separation of traffic flows inside the environment, segmentation and micro-segmentation, agility, automation, and unified management across multiple platforms.

Security by Design

Security by design is a multi-layer security approach that leverages characteristics inherent to the Internet as an additional means to block unwanted traffic patterns, in a way that cannot be overridden by security policy. Figure 5 shows schematically how the Blueprint 2.0 hub and spoke model, as implemented using CloudGuard Network Security, supports security by design.

Where possible, the North Hub uses a non-transitive peering connection with the spokes in order to control traffic flow by design. Non-transitive peering, by definition, systematically isolates cloud resources from the main incoming traffic path.

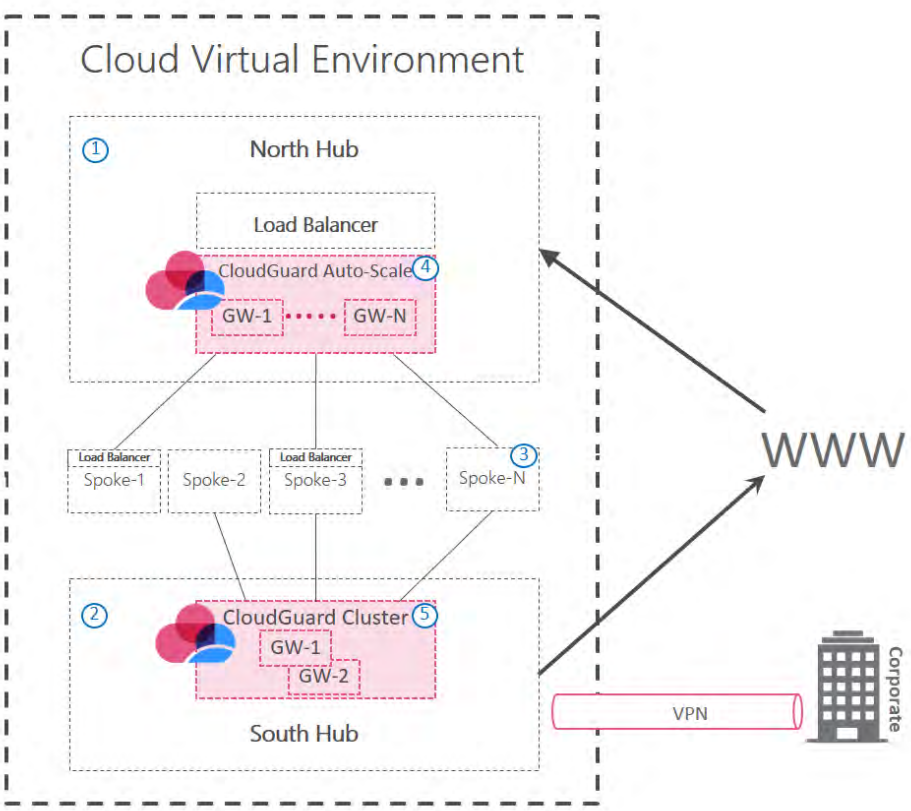

Figure 5: CloudGuard Network Security Hub and Spoke Model

where:

1 = North Hub for incoming traffic from the Internet

2 = South Hub for traffic to and from the corporate network, east-west access between spokes, and outgoing traffic to the Internet

3 = Spoke to segment cloud VMs with different security and access levels

4 = CloudGuard Auto Scaling: an elastic set of firewalls for Internet-based security enforcement

5 = CloudGuard Network Security high availability cluster.

For example, the cloud security architecture can utilize Amazon VPC peering, which is non-transitive (a documented limitation), to connect the incoming traffic path to isolated network environments. This ensures that lateral movement of traffic between the isolated segments is done exclusively through that Hub.

The above design example also allows a spoke to not be connected to the North Hub at all, preventing any possible exposure to the Internet.

Network Perimeter Security

Network perimeter enforcement is performed on the North and South Hubs, with various security protections enabled efficiently and on demand. Ingress or egress traffic from/to the internet is inspected by the CloudGuard Network Security Security Gateways deployed on the hubs, thereby enforcing the organization's security policy.

Note that it is possible (and recommended) that different policies and protection blades be applied to the North and South Hubs. For example, it is recommended that the South Hub be configured with anti-malware protection to prevent lateral threat movement. Traffic moving through the security hub is inspected by the gateways and matched against the security policy.

Segmentation

CloudGuard Network Security supports inter-VPC/vNET segmentation by placing cloud workloads in different spokes and enforcing security controls on traffic entering or exiting a spoke. The three main types of spokes in Blueprint 2.0 are:

- **Internet facing only** (e.g., SPOKE-1 in Figure 5): These spokes are connected to North Hubs only and are accessible only to incoming traffic from the Internet. These spokes typically host front-tier servers that have to be accessible from the Internet such as, for example, websites hosting public campaigns. In order to avoid undesired public exposure of private (corporate) resources, connectivity from these spokes to corporate resources or to other spokes in the environment is blocked systematically and cannot be enabled by a simple routing/policy configuration.
- **Private facing (corporate) only** (e.g., SPOKE-2 in Figure 5): These spokes are only connected to South Hubs and are thus systematically not accessible from the Internet. They are accessible through any combination of VPN, direct connectivity from the corporate network, or from other spokes in the environment (as per the security policy on South Hub firewalls). A typical use case for a private facing spoke is hosting database servers to which we want to have secure connectivity but do not want them to be directly accessible from the Internet.

- **Combined** (e.g., SPOKE-3 in Figure 5): These spokes are suitable for servers that have to be accessible from the Internet but also require backend access to other spokes or to the corporate network. An example would be a web server that is exposed to the Internet on one end and needs access to an application server or database server on the other.

CloudGuard Posture Management supports intra-VPC/vNET segmentation by using cloud-native security controls to block traffic between workloads within a subnet. CloudGuard Posture Management's single-pane management of cloud access lists and security groups is particularly helpful in multicloud environments. Using CloudGuard Posture Management, you can achieve higher granularity than the subnet level and theoretically (and also practically - should you choose to do so) create a VM/instance specific policy/isolation on layer 4.

In this specific use-case, CloudGuard Posture Management's functionality extends that of CloudGuard Network Security: While CloudGuard Network Security is mostly used for infrastructure level segmentation and guardrails, CloudGuard Posture Management supports the implementation of micro-segmentation performed using the cloud native controls.

CloudGuard CloudGuard Posture Management adds another layer of segmentation (between services and between users) with just-in-time privileged elevation on top of cloud native IAM services in order to protect sensitive administrative operations. IAM users who wish to access protected services can elevate themselves or can be elevated by the CloudGuard Posture Management Administrator. The authorization window is provided for a limited period. During this time, the IAM user can access the protected services. At the end of the window, access to the services will be blocked again.

This feature hardens the provider's account console and restricts users from making unauthorized or accidental changes to account settings without the knowledge and authorization of an administrator. It also significantly reduces the blast radius if a hacker seeks to take over an account identity with excessive privileges.

Agility and Automation

Today, IT seeks to operate efficiently and be a business enabler instead of a business roadblock. The Blueprint 2.0 hub-and-spoke model supports business agility since spokes can be created and entirely owned by the organization's different lines of business or, in fact, anyone within the organization. CloudGuard Posture Management can enforce the principle of no direct connectivity between spokes, forcing spoke traffic to go through the South Hub and its security controls. In this way spoke owners can be given the freedom to own and handle security inside their spokes, without compromising security.

CloudGuard Network Security ensures that this agility does not undermine the corporate security posture through automation at multiple layers. On the infrastructure level, the deployment of CGNS resources can be automated using implementation templates such as AWS CloudFormation or Azure Resource Manager Template. These pre-configured scripts simplify the implementation of CGNS gateways in different deployment configurations such as standalone, cluster, and auto-scaling. The required environment (subnets, Internet access, routing configuration, and so on) is created out of the box.

Another automation layer provided by CloudGuard Network Security involves using the CME (Cloud Management Extension) to automatically provision resources in dynamic public cloud configurations such as auto-scaling and load balancing. Any addition or deletion of security gateways within the environment invokes an automated process to commission or decommission the gateway from the policy/SmartConsole layer. For example, any time a new gateway is added into the environment, the CME-based automation process will automatically discover the new gateway, perform the initial "first-time wizard" setup on it, reboot the gateway, establish SIC (Secure Internal Communication) with the management server, and push security policy to the gateway.

Similarly, the CME can also automate the security configuration of load balancing settings since it detects the listener configuration on the load balancer and automatically creates the relevant rules on the security policy. This behavior brings significant benefits to day to day operations with security becoming part of the operation rather than a showstopper. Changes on the Load Balancer are automatically reflected in the firewall policy, without downtime.

Automatic behavior is also achieved on the security policy rules level, with the CloudGuard Controller allowing cloud native objects to be used in the security policy. The added cloud native objects are automatically and continuously tracked by the management server and any changes made on the cloud side (such as tagging an instance with a tag that is included in the security policy, changing an IP or the name of an instance, etc.) are automatically and instantly enforced to all gateways connected to the management server. In this way Line of Business managers can proceed at velocity while making sure that the company's security policies and standards are upheld.

CloudGuard Posture Management also actively protects workloads, PaaS and serverless functions running in the public cloud, surrounding them with guardrails that keep them secure without forfeiting agility. For example, it can scan the text in a serverless function for potential leakages (e.g., API keys); check the list of permissions and privileges in its code; and check the communication of serverless functions against lists of suspicious URLs. These, together with other CloudGuard Posture Management features, decrease attack surfaces and prevent many and various exploitation attempts in ways that are transparent to the spoke owners, who are free to pursue their business activities.

Cloud Compliance and Governance

Given the lack of visibility into cloud assets as well as the highly dynamic nature of the cloud environment, the cloud presents significant compliance and compliance auditing challenges. If you factor in the impact of complex hybrid and multicloud environments, upholding a cloud security posture that complies with corporate governance and regulatory requirements can sometimes feel like mission impossible.

While it is not primarily a solution for cloud compliance, CloudGuard Network Security contributes to cloud compliance through automated enforcement of security policy rules changes to all security gateways connected to the management server. In addition, CloudGuard Network Security leverages Check Point Security Compliance to monitor security gateways on a 24/7 basis and deliver:

- Instant alerts about policy changes that could undermine security, with recommendations for remediation
- Realtime assessments of compliance with regulations
- Audit reports that highlight poor configuration settings and security weaknesses

The CloudGuard Posture Management Compliance Engine tests cloud environments for compliance against industry standards and best practices or against the organization's own security policies. It can also test compliance using sets of rules (CloudGuard Posture Management rulesets) that are available out-of-the-box.

CloudGuard Posture Management's comprehensive cloud security rulesets cover many of the common standards such as PCI-DSS and HIPAA, ISO 27001, GDPR, NIST, CIS and more. They can be run immediately "as is" across all the organization's cloud accounts. In addition, new rules can be built and tested or existing rules modified using an intuitive graphical rule builder, tailoring policies to each organization's specific compliance needs and goals. In all these ways the powerful CloudGuard Posture Management Compliance Engine allows the organization to comply with both third-party regulations and specific corporate security policies, and respond quickly to misconfigurations and accidental changes.

The Compliance Engine works with all three major cloud providers (AWS, Azure, and GCP) to easily check compliance in multi-cloud environments. It can also run assessments in Kubernetes clusters checking against compliance standards such as CIS Benchmarks for Kubernetes and others.

The Compliance Engine tests cloud accounts continuously and sends notifications when issues are detected. It also has rich reporting capabilities, from detailed test results to summary reports of findings across various regions and VPC/vNET accounts. It is easy to drill down from high-level results to details. To gain insights faster, the reports can be organized and filtered according to severity levels, tested entities, and so on. Historical reports can be used to highlight trends for a wide range of parameters.

Visibility

Cloud customers often complain about the lack of visibility that makes it difficult to identify and quantify their cloud assets. These invisible and unmanaged assets create serious gaps in security enforcement. Cloud customers require cloud-oriented orchestration tools in order to effectively identify and monitor their cloud assets as well as visualize their cloud environments.

In the hub and spoke architecture all network traffic traverses through the hubs, making it possible to achieve visibility through the use of security logs.

CloudGuard Network Security uses SmartEvent event management to provide full threat visibility with a single view into security risks thus accelerating incident response. Users can take control and command the security event through real-time forensic and event investigation, compliance, and reporting. Additionally, they can use this functionality to respond to security incidents immediately and gain network true insights.

CloudGuard Posture Management allows organizations to visualize all assets that are running in the cloud, assess security posture (including security groups, instances, and more), fix misconfigurations to pre-empt threats, manage cloud-native security groups, and enforce security from a single source of network authority.

In addition, CloudGuard Intelligence is a cloud-native security intelligence technology that combines cloud inventory and configuration information with realtime and diverse monitoring data to deliver cloud intrusion detection, network traffic visualization and user activity analytics.

CloudGuard Intelligence analyzes the cloud providers' network traffic and event logs, making them human-readable and providing a context that is otherwise missing.

CloudGuard Intelligence lets the organization see all the assets that are active in any given account, which ones are connected and sending traffic to/from each other, and the statistics per each element. Log.ic also visualizes the network events in the cloud. Thus, for example, organizations can see which serverless function was invoked, through which gateway the traffic is flowing, which type of asset is communicating, and to which VPC/vNET it belongs.

CloudGuard Intelligence integrates with a leading threat intelligence feed, spotting inbound and outbound traffic from and to malicious hosts. CloudGuard Intelligence will alert to malicious activity or suspicious and unwanted events and alert the user to take actions accordingly. Out-of-the-box or custom queries can be used to search through logs for events of interest—and all of this takes place in real time.

Borderless

There is a well-documented trend of enterprises implementing complex multi-cloud and hybrid environments. The Cloud Security Blueprint design inherently supports scaling outside of the limits of a single cloud platform. It also manages the connectivity between cloud platforms while maintaining the same architectural principles and security posture across all the environments.

In order to minimize the risks associated with monitoring and securing these complex environments, CloudGuard Network Security implements a VPN Mesh (see Figure 6) that secures connectivity among the multiple sites.

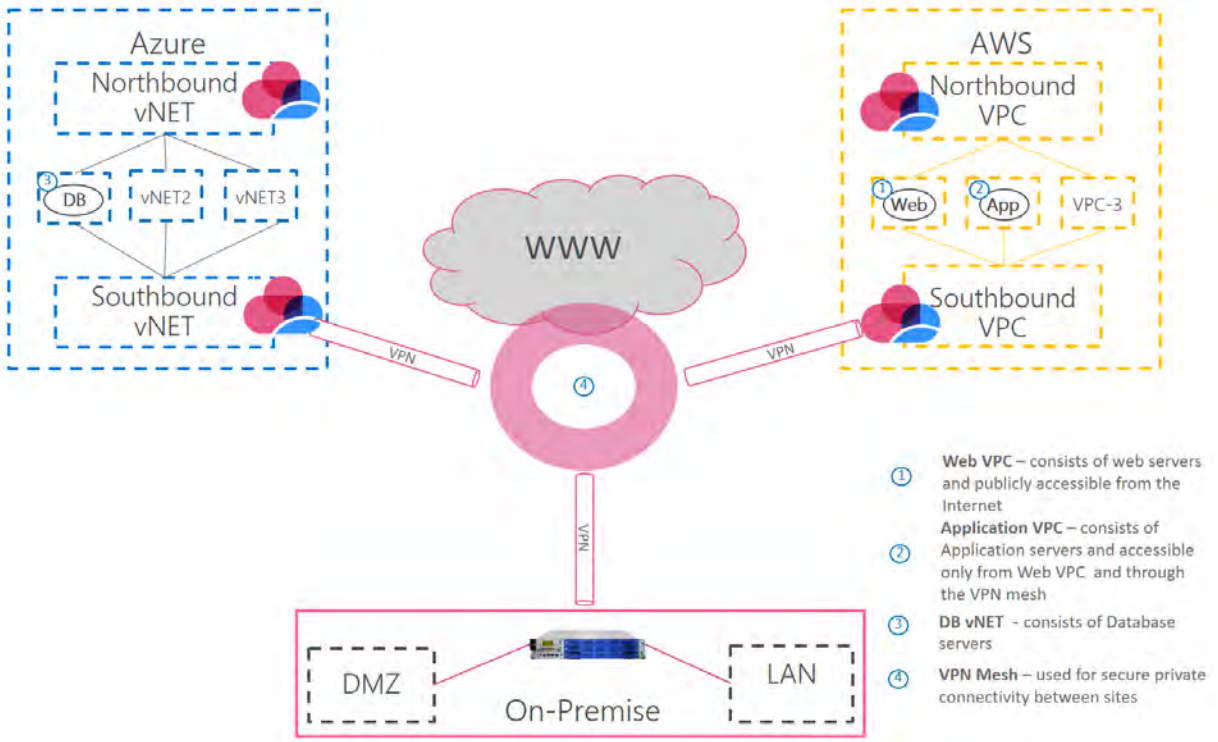

Figure 6: Implementing CloudGuard Network Security Gateways Across Platforms for Location-Specific Traffic Control and Security Policy Enforcement Across Locations

where:

1 = a Web VPC, which consists of web servers publicly accessible from the Internet

2 = an Application VPC of application servers accessible only from a Web VPC and through the VPN Mesh

3 = the Azure MSSQL DB

4 = VPN Mesh that is used for secure private connectivity between sites

The multi-cloud architecture use case illustrated in Figure 6 is for an online gaming company that deploys its services across AWS, Azure and an on-premise data center in a "best of breed" approach where each platform is chosen based on team expertise and technological superiority. In our example the web frontend and application tiers are hosted on AWS across multiple availability zones for redundancy, while identity and authentication is provided by the AD server located on-premise. The database and storage tiers are hosted in Azure.

Implementing CloudGuard Network Security gateways across the different platforms allows us to control traffic in each location specifically, as well as enforce security policies across and between locations.

CloudGuard Posture Management also upholds the borderless principle by delivering and orchestrating its security capabilities across all three leading cloud providers: Amazon Web Services, Microsoft Azure, and Google Cloud Platform (GCP). CloudGuard Posture Management also supports the onboarding of Kubernetes clusters into the CloudGuard Posture Management Cloud Inventory so that compliance assessments can be run on them. The cluster can be on premises or in a cloud environment, including managed cloud environments.

Unified Management

Implementing and operating security in a multi-cloud environment can be challenging, as it involves managing and controlling resources that use different management tools in a variety of locations. Trying to maintain a unified security policy in such conditions is not only tedious and inefficient, but often a source of error. It is also difficult to troubleshoot connectivity issues or quickly and efficiently resolve security events in such an environment.

Blueprint 2.0 supports integrated security management that lets organizations translate their security definitions into a simple set of rules and consistently implement those rules across complex multi-cloud and hybrid cloud environments.

Other challenges often encountered in multi-cloud environments are implementing a unified security policy and gaining end-to-end visibility into security events.

The Check Point unified security management server (SMS) is an integrated security management solution that includes policy, logging, monitoring, event correlation, and reporting. Supporting all leading public and private cloud vendors, the SMS allows organizations to translate their security definitions into a simple set of rules that can be efficiently administered and enforced as a unified security policy. Administrators can also easily identify security risks across the environment.

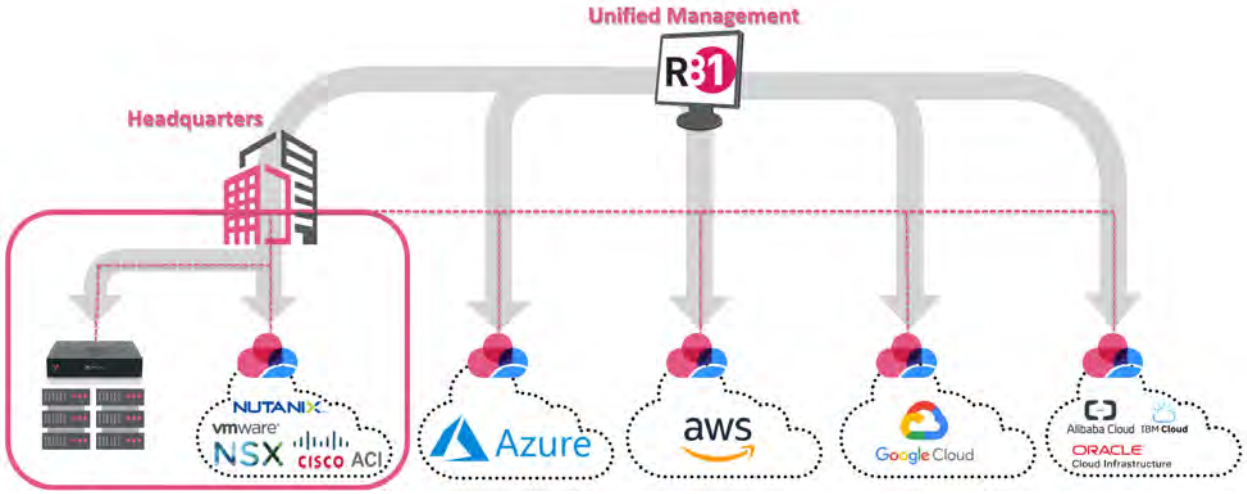

Figure 7: Check Point Security Management Server for Unified Management

The deployment of the SMS is flexible and it can be located anywhere across the environment. It is also possible to set up the management server in high availability mode across platforms (e.g., a primary management server located on-premise with a backup server located in a secondary disaster recovery site).

Unified management is also one of CloudGuard Posture Management's key value propositions, with its centralized interface that simplifies security management and orchestration across all cloud assets.

Summary

Cloud Security Blueprint 2.0 is a design framework with cloud security best practices for building a secure cloud-based infrastructure based on the essential cloud security architectural principles of advanced threat protection across all attack vectors (network, data, identity messaging, users), security by design, segmentation, secure agility, robust automation, and being provider-agnostic.

The Blueprint 2.0 design ensures that all traffic to and from isolated network environments must traverse the security controls of a central broker. Each isolated environment is a segment whose security controls can be adjusted to the type of ingress and egress traffic. Internet-facing segments, for example, will be configured to monitor incoming external traffic for threats or anomalies and can systematically block lateral traffic movement. Private-facing (corporate) segments, on the other hand, can be configured to effectively inspect and secure lateral traffic.

Blueprint 2.0's design also supports business agility. Segment owners, such as different lines of business, have freedom to operate but centrally managed security controls ensure that the organization's security policies are upheld consistently across all platforms and accounts.

Check Point's cloud security capabilities—CloudGuard Network Security, CloudGuard Posture Management, and CloudGuard Intelligence—work together to ensure seamless Blueprint 2.0 implementations.

CloudGuard Network Security, for example, applies advanced perimeter security on the hubs; implements a VPN Mesh for secure connectivity across multiple providers, accounts and assets; and allows organizations to efficiently administer and enforce a rules-based security policy across complex environments. CloudGuard Network Security also supports automation and orchestration at the infrastructure deployment level (using implementation templates) as well as dynamic provisioning of resources during runtime to securely support auto-scaling and load-balancing cloud services. In addition, automation on the policy level allows cloud-native objects to adapt automatically to the organization's security policy. CloudGuard Network Security also supports resilient multi-zone deployments.

CloudGuard Posture Management is a powerful SaaS cloud security posture management (CSPM) solution that visualizes and consistently enforces an organization's security posture across all providers and services. CloudGuard Posture Management quickly identifies and alerts to anomalous traffic anywhere in the organization's environment, ensuring quick responses and, where relevant, triggering automated remediation workflows. Its Compliance Engine continuously monitors for compliance to third-party or corporate requirements, providing rulesets that can be used "as is" or tailored to the organization's specific compliance needs. CloudGuard Posture Management hardens cloud native IAM services to protect sensitive assets and operations with time-limited privilege elevations.

Last but not least, CloudGuard Intelligence is a cloud security intelligence tool that derives actionable insights and context from the cloud providers' network traffic and event logs.

Contact Check Point for more information, or schedule a demo of one or more of the above cloud security solutions to help you to design a secure cloud architecture.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com