CHECK POINT™

BUYER'S GUIDE TO CLOUD NETWORK SECURITY

SECURE YOUR EVERYTHING™

Introduction

Although corporate and internal networks are the most popular (54%) attack vector for hackers, cloud-based environments, ecommerce in particular, are the next most popular targets (44%) (2020 Trustwave Global Security Report). In fact, between four and five of every 10 data breaches (43%) involve web applications. Moreover, a recent study shows that misconfigured clouds were a leading cause of breaches in 2020, and data breaches due to cloud misconfigurations resulted in the average cost of a breach increasing by more than half a million dollars, from $3.86 million to $4.41 million.

As a result, cloud security has become business-critical as organizations expand and deepen their cloud presence. According to the Check Point 2020 Cloud Security Report, 75% of surveyed organizations were either very or extremely concerned about cloud security.

Cloud Security Platform Layers and Hierarchy

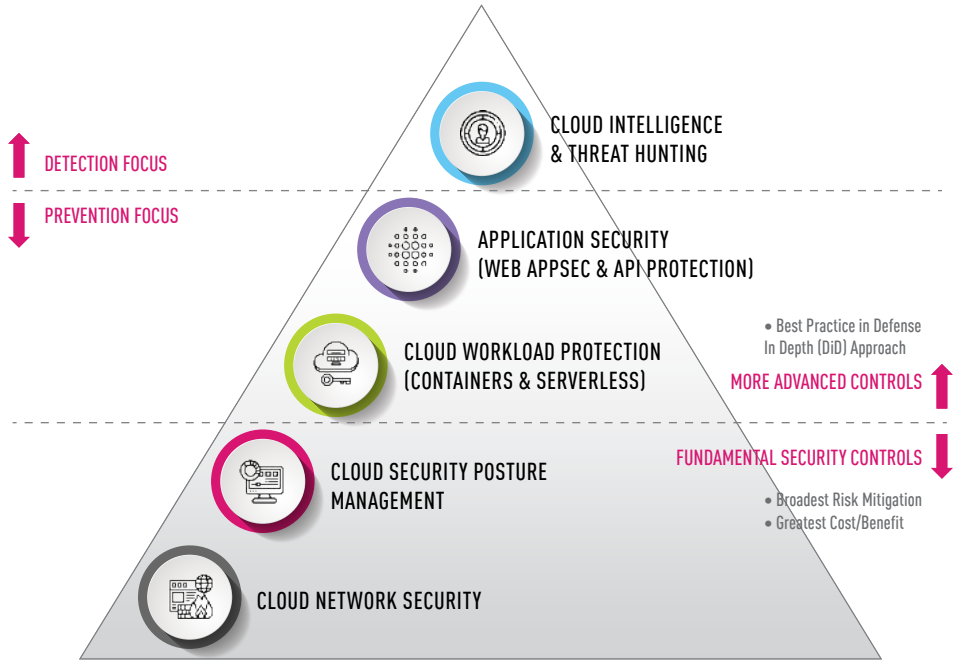


Figure 1: The Multiple Layers of a Unified Cloud Native Security Platform

Figure 1 illustrates the kind of multilayered, yet unified, cloud security platform that organizations should put in place in order to protect their cloud deployments and ensure a robust cloud security posture.

Conversely, a recent Forrester study stated that cloud security confidence is a leading driver for adopting more cloud services.

It's always important to remember that cloud security takes place in the context of a shared responsibility model. At the infrastructure level (IaaS), cloud providers are responsible for securing their compute-network-storage infrastructure resources while users are responsible for protecting the data, apps, and other assets deployed on the infrastructure. The tools and services offered by cloud providers to help users uphold their end of the shared responsibility model are important elements of any cloud network security solution. However, cloud providers are not specialists in security; these cloud provider tools and services must be complemented by partner solutions in order to achieve enterprise-grade network security.

As shown in Figure 1, a key foundational layer is **cloud network security**, where organizations should deploy virtual security gateways to provide advanced threat prevention, traffic inspection and micro-segmentation. Such security solutions use multiple layered security technologies including Firewall, IPS, Application Control, DLP and others.

This guide describes the ten essential considerations a company should examine when choosing its cloud network security platform. Using these considerations, it then compares the relative benefits of the cloud network security solutions provided by leading cloud providers and third-party security vendors in the market today.

This guide discusses the functionality that effective cloud security solutions should have, and how you can make sure that vendor solutions have the capabilities that are important to your organization's success and security.

The Top 10 Considerations for Evaluating a Cloud Network Security Solution

Here are the top ten criteria you should be using to choose your company's optimal cloud network security solution:

1. ADVANCED THREAT PREVENTION AND DEEP SECURITY
2. BORDERLESS
3. GRANULAR TRAFFIC INSPECTION AND CONTROL
4. AUTOMATION
5. INTEGRATION AND EASE OF USE
6. VISIBILITY
7. SCALABLE, SECURE REMOTE ACCESS
8. CONTEXT-AWARE SECURITY MANAGEMENT
9. VENDOR SUPPORT AND INDUSTRY RECOGNITION
10. TOTAL COST OF OWNERSHIP

In order to stay a step ahead of malicious actors, threats must be captured and neutralized ***before*** they penetrate the network.

1 Advanced Threat Prevention and Deep Security

Threat detection is not enough to effectively protect cloud assets in today's complex cybersecurity landscape. You need multilayered, real-time threat *prevention* for both known and unknown (zero-day) vulnerabilities. The solution must deliver deep security through features such as granular and deep traffic inspection, enhanced threat intelligence, and sandboxing that isolates suspicious traffic until it is either validated or blocked. And these advanced capabilities must be deployed on both North-South (incoming/outgoing) and East-West (lateral) traffic.

Why is this important? **Detecting a threat *after* it has breached the corporate network exposes the organization's assets to unacceptable levels of cybersecurity risk. In order to stay a step ahead of malicious actors, threats—including zero-day and other agile exploits—must be captured and neutralized *before* they penetrate the network. This advanced prevention is possible only by deploying a deep security solution that applies advanced methodologies across multiple layers. Most importantly, a deeper and more comprehensive cloud network security solution will reduce the probability of a cloud breach and minimize the impact and damage if and when it occurs.**

2 Borderless

The solution must run transparently and consistently across even the most complex multi-cloud and hybrid (public/private/on-prem) environments. A unified management interface (sometimes called a "single pane-of-glass") should provide a single source of cloud network security truth as well as a centralized command and control console.

Why is this important? **Security teams can *not* deliver enterprise-grade protection with a fragmented stack comprised of vendor-specific or environment-specific security tools. Aside from the challenging range of diverse skill sets this requires, it inevitably creates policy and process gaps through which threats can slip.**

3 

Granular Traffic Inspection and Control

Look for next generation firewall (NGFW) capabilities, such as fine matching granularity that goes beyond basic whitelisting, deep inspection to ensure that traffic matches the purposes of the allowed ports, advanced filtering based on URL addresses, and controls at not just the port level but the application level as well.

Why is this important? **Without deep traffic inspection, organizations are easy prey to evasion techniques that attempt to carry out unauthorized actions through seemingly legitimate access points. And trying to control application activity by blocking URLs and IP addresses is doomed to failure because these protections are easy to bypass; the only solution is application level control as easy as "block Facebook".**

4 

Automation

In order to match the speed and scalability of DevOps, the solution must support high levels of automation, including programmatic command and control of security gateways, seamless integration with CI/CD processes, automated threat response and remediation workflows, and dynamic policy updates that don't require human intervention.

Why is this important? **Any cloud solution that does not enable high levels of automation will be impossible to support and will be abandoned by customers. Legacy security approaches that rely heavily on human intervention cannot scale to meet the volume, velocity and variety of today's cybersecurity threats, Manual processes are also slow and prone to error. As in many other areas of IT, in security as well the only solution is rule-based, adaptive automated workflows.**

5 

Integration and Ease of Use

The solution must work well with your company's configuration management stack, including support for Infrastructure as Code deployments. In addition, the solution has to be deeply integrated with the cloud providers' offerings. In general, your goal should be to streamline operations and promote ease of use by minimizing the number of point security solutions that have to be deployed and managed separately.

Why is this important? **Integration is critical to a number of other considerations described here, such as enabling borderless operations and increasing visibility. It plays an important role in creating a cross-functional cloud security platform that addresses not only infrastructure security but also application security, cloud security posture management, and more. Tight integration also contributes greatly to overall ease of use, allowing configurations and tasks to be carried out with the least number of clicks and minimal navigation through complex interfaces.**

6 Visibility

The solution's dashboards, logs, and reports should provide end-to-end and actionable visibility into events as they are happening. For example, logs and reports should use easy-to-parse cloud object names rather than obscure IP addresses. This visibility is also important for enhanced forensic analytics should a breach take place.

Why is this important? **At the most basic level, you can't secure what you can't see. Even more important, however, is that what you see is both easily understandable and context-aware—correlating across the different signals, events, and data streams that are being monitored.**

7 Scalable, Secure Remote Access

The solution must secure remote access to the company's cloud environment with features such as multi-factor authentication, endpoint compliance scanning, and encryption of data-in-transit. Remote access must also be able to scale quickly so that, during times of disruption such as the COVID-19 pandemic, any number of remote employees can work productively yet securely.

Why is this important? **The work-from-home trend was accelerated by the pandemic, but many analysts are predicting that it will continue to grow even after the crisis is behind us. In a world of highly distributed and mobile work forces, remote access to the corporate network that is both secure and performant is a must-have.**

8 Context-aware Security Management

The cloud network security solution must be able to aggregate and correlate information across the entire environment—public and private clouds as well as on-prem networks—so that security policies can be both context-aware and consistent. Changes to network, asset, or security group configurations should be automatically reflected in their relevant security policies.

Why is this important? **High levels of integration and automation are critical for the intelligent and consistent management of security policies across complex environments. With asset, change and configuration management frameworks playing a central role in vulnerability remediation efforts, your security platform must be able to seamlessly publish changes, and adapt in real-time to all relevant security policies.**

9 Vendor Support and Industry Recognition

In addition to the features and capabilities of the solution itself, it is also important to take a close look at the vendor. Is it highly rated by independent industry analysts and third party security testing companies? Can it meet your SLAs? Does it have a proven track record? Can it provide added value, such as network security advisory services? Can it support your global operations? Is it committed to innovation so that its solution will be future-proof? Is its software mature, with few vulnerabilities, and does it deliver timely fixes?

Why is this important? **Recognition by trusted evaluators has become a key factor in purchasing decisions in general, and certainly plays an important role here as well. Use these impartial recommendations to seek out a vendor that can drive your cloud security strategy forward, with the capacity to adapt and scale to your ever-changing business requirements. Look for a vendor who meets your security needs and can be a trusted cloud security advisor for many years into the future. Remember, an ill-matched vendor can be a constraining factor in achieving enterprise-grade cloud security.**

10 Total Cost of Ownership

The total cost of ownership is determined by a number of factors, all of which should be considered as part of the buying process: the flexibility of the licensing model, the extent to which the cloud security platform seamlessly integrates with and leverages existing IT systems, the level and scope of personnel required to administer the system, the vendor's MTTR and availability SLAs, and more.

Why is this important? **You want your cloud security platform to streamline operations, optimize workflows, and reduce costs while enhancing your security posture. The last thing you want is to be surprised by hidden infrastructure, personnel and other costs that emerge only after the system is up and running.**

The last thing you want is to be surprised by hidden infrastructure, personnel and other costs that emerge only after the system is up and running.

CloudGuard: Advanced Cloud Network Security

Check Point's CloudGuard platform provides unified cloud native security for all your assets and workloads and across your multi-cloud environments, giving you the confidence to automate security, prevent threats, and manage posture.

One of CloudGuard's fundamental capabilities is cloud network security, delivered as a virtual appliance that extends Check Point's advanced threat prevention and industry-leading catch rate to the dynamic and elastic cloud environment. It is adapted and configured specifically for easy deployment on cloud platforms as well as software-defined data centers.

> CloudGuard Network Security is delivered as a virtual appliance that extends Check Point's advanced threat prevention and industry-leading catch rate to the dynamic and elastic cloud environment.

The Key CloudGuard Network Security Features and Benefits are:

1

Enterprise-grade, advanced, multilayered threat prevention:
CloudGuard preemptively protects cloud assets against known and unknown (zero-day) vulnerabilities, leveraging one of the world's largest threat databases, Check Point ThreatCloud, as well as advanced threat extraction and threat emulation technologies.

2

Borderless:
CloudGuard is quickly deployed on and works seamlessly with multiple public cloud service providers and software-defined data center solution providers.

3

Granular traffic inspection and control:
CloudGuard implements deep SSL/TLS inspection for incoming and outgoing traffic as well as for lateral traffic behind the firewall. CloudGuard's next generation firewall supports finely granular matching policies, including exclusions, verifying traffic against port configurations, and application-level blocking.

4

Automated, agile network security at scale:
Cloud-defined elements (asset tags, objects, security groups) are updated in real time and security policies adjusted automatically to changes in the cloud environment. CloudGuard also promotes the automation of threat response, remediation processes, and workflows.

5

Integration with your existing tool stack:
CloudGuard integrates via APIs with the leading configuration management, Infrastructure as Code, and CI/CD tools. CloudGuard is also deeply integrated with cloud native tools and services, as described in more detail below.

6

Visibility:
CloudGuard consolidates incoming log data from the entire corporate infrastructure and substitutes cloud object names for IP addresses in order to enhance network security visibility and forensics.

7

Secure remote access:
CloudGuard ensures that all remote connections to cloud resources are securely authenticated—including two-factor authentication for mobile access. CloudGuard also encrypts incoming and outgoing data-in-transit. On Azure, for example, CloudGuard leverages Virtual Machine Scale Sets (VMSS) to deliver highly scalable and dynamic secure remote access with automatically managed connectivity and load sharing.

8

Context-aware management across cloud and on-prem infrastructures:
CloudGuard's single unified management console is easy to use and customers consistently rank it highly in the regular surveys that Check Point conducts. Security policies can be enforced consistently and security events tracked easily across the entire environment.

9

Industry leadership and global presence:
For 21 consecutive years, Check Point has been named a Leader on the Gartner Magic Quadrant for Network Firewall and has maintained a Recommended rating by NSS labs. CloudGuard benefits from Check Point's industry-leading global support, professional services, partner ecosystem, Incident Response, and more. Check Point operates in 88+ countries, with over 6500 global channel partners and four global TACs (Technical Assistance Centers) which "follow the sun", providing 24x365 global support.

10

Total Cost of Ownership:
Another area in which CloudGuard leads the industry is its low-latency performance, which translates into a lower total cost of ownership since fewer cloud compute resources are needed to achieve the required throughput. The 2021 Forrester Total Economic Impact of CloudGuard Network Security provides an independent study of RoI and cost of ownership.

Check Point operates in 88+ countries, with over 6500 global channel partners and four global TACs (Technical Assistance Centers) which "follow the sun", providing 24x365 global support.

What do customers say?

Customers utilizing security solutions are often hesitant to publicize their choice of vendor and product. They may be concerned that threat actors will use this information as a vector of attack, which is often the case when using security vendors with a high propensity for vulnerabilities in their own products.

As a result, satisfied customers who tell their story publicly are always a good indication of solution and vendor quality.

The table below provides customer stories for the top 10 considerations defined previously.

CONSIDERATION	CUSTOMER STORY	LEARN MORE
1 **Advanced Threat Prevention and Deep Security**	BH Telecom receives all their cloud security needs in one solution, "from firewall filtering to IPS, to content filtering to antivirus. By combining everything, we can join the dots in our service offering."	Customer Story
2 **Borderless**	The US-based global healthcare customer, interviewed in the recent Forrester TEI study of CloudGuard Network Security, is able to manage security across VMware, AWS, Azure, Google Cloud as well as on-premises from a single console and using the same security policies. "Each cloud has its own language. With CloudGuard we use the same set of tags across multiple clouds, and across different accounts and subscriptions. We would have had to manage everything separately if we had done it natively."	Forrester TEI of CloudGuard Network Security
3 **Granular Traffic Inspection and Control**	Paschaolotto ran a comparison using two models in parallel (one with CloudGuard; one without) while under attack by various types of malware. CloudGuard, which protects all network layers, including the application layer (Layer 7), stopped application-based attacks that passed undetected without CloudGuard installed.	Customer Story Watch Video
4 **Automation**	Openlink is very focused on automation and efficiency. "Check Point has always excelled in unified management—whether it's two or two thousand instances. We're currently working through orchestration and scripting to automate as many steps as possible. Our goal is to minimize the human resources needed to deploy new environment and manage the cloud."	Customer Story
5 **Integration and Ease of Use**	NHS Scotland benefits from CloudGuard's seamless integration with their SIEM solution: "That means that we don't have to go and actually start writing and creating configurations, it just links in and just automatically starts to work."	Customer Story Watch Video

CONSIDERATION	CUSTOMER STORY	LEARN MORE
6 **Visibility**	For Avianca, consolidated monitoring, logging and reporting give security teams immediate visibility into status and incidents—whether in the cloud, on-premises or across all environments.	Customer Story Watch Video
7 **Scalable, Secure Remote Access**	Gas South planned to provide secure remote access to a small number of employees in early 2020, but after the first Covid lockdown, needed to support all employees working remotely. Fortunately CloudGuard supported this without any difficulty.	Customer Story Watch Video Blog Post
8 **Context-aware Security Management**	Invitalia no longer has to toggle between different security consoles to benefit from consistent visibility, policy management, logging, reporting, and control.	Customer Story
9 **Vendor Support and Industry Recognition**	X by Orange assessed Check Point against strict criteria: "From an operational point of view, working with Check Point also gave us access to a wide network of first-class support across Spain."	Customer Story
10 **Total Cost of Ownership**	With on-demand cloud and security infrastructure scalability, Xero can confidently ensure that peak usage periods deliver the high performance that customers expect. At the same time, during lulls in activity Xero is not paying for capacity that sits idle. AWS and Check Point enabled Xero to achieve its primary goals of reducing service delivery costs while assuring high service availability.	Customer Story Ebook Webinar with AWS

" Check Point CloudGuard Network Security has been a saving grace for Gas South. It is the only solution that gives us secure, stable, complete access to our critical applications and services in Azure."

– Rajiv Thomas, Senior Systems Engineer, Gas South

How CloudGuard Extends Cloud Native Security

CloudGuard is fully optimized for the cloud environment. It takes just minutes to deploy and configure CloudGuard Network Security gateways using automated cloud provider workflows and templates that can be customized to align with your corporate security ecosystem.

The CloudGuard gateway seamlessly and deeply integrates with cloud native resiliency and scalability features, such as auto-scaling, failover, and high availability across multiple regions.

Each cloud provider offers tools and services to help its customers monitor and secure their cloud resources. The following table provides a sampling of some typical cloud provider tools.

	FIREWALLS	CLOUD MONITORING AND THREAT DETECTION	SECURITY CONSOLE
AWS	Security Groups Network ACLs AWS Network Firewall	Amazon GuardDuty AWS CloudTrail Logs	AWS Security Hub
Microsoft Azure	Azure Firewall Network Security Groups	Azure Defender Azure Advanced Threat Protection Microsoft Defender for Cloud	Microsoft Defender for Cloud Microsoft Sentinel
Google Cloud Platform	Google Cloud Firewalls	Event Threat Detection	Cloud Security Command Center

Table 1: Typical cloud provider tools to monitor and secure cloud resources

CloudGuard Network Security enhances and complements the cloud provider security services

What are the main areas where CloudGuard Network Security enhances and complements the cloud provider security services?

CloudGuard Network Security provides a self-service, automatic, adaptive solution that complements cloud native security constructs in order to **prevent** malicious activity in real time. CloudGuard delivers enterprise-grade security in the cloud, including fine matching granularity and control, deep inspection and advanced evasion protection, and proactive threat prevention against both known and unknown vulnerabilities.

CloudGuard Network Security also provides truly unified and **multi-cloud** management of cloud security and compliance from a single management console. After the initial connection, all cloud assets are automatically imported into the console, and changes to instance/VM attributes, such as IP, name, or location, are updated automatically in CloudGuard security policies and logs. In addition, cloud object names are used in both policies and logs for enhanced visibility and searching.

The use of multiple cloud providers is becoming the norm rather than the exception. The Check Point 2020 Cloud Security Report found that 68% of organizations use two or more cloud providers; in a recent Gartner research more than 80% of respondents indicated that their organization runs workloads in multiple clouds. The Check Point unified security management provides consistent visibility, policy management, logging, reporting and control across all public and private cloud deployments, as well as for on-premises deployments.

CloudGuard Network Security also provides truly unified and ***multi-cloud*** management of cloud security and compliance from a single management console.

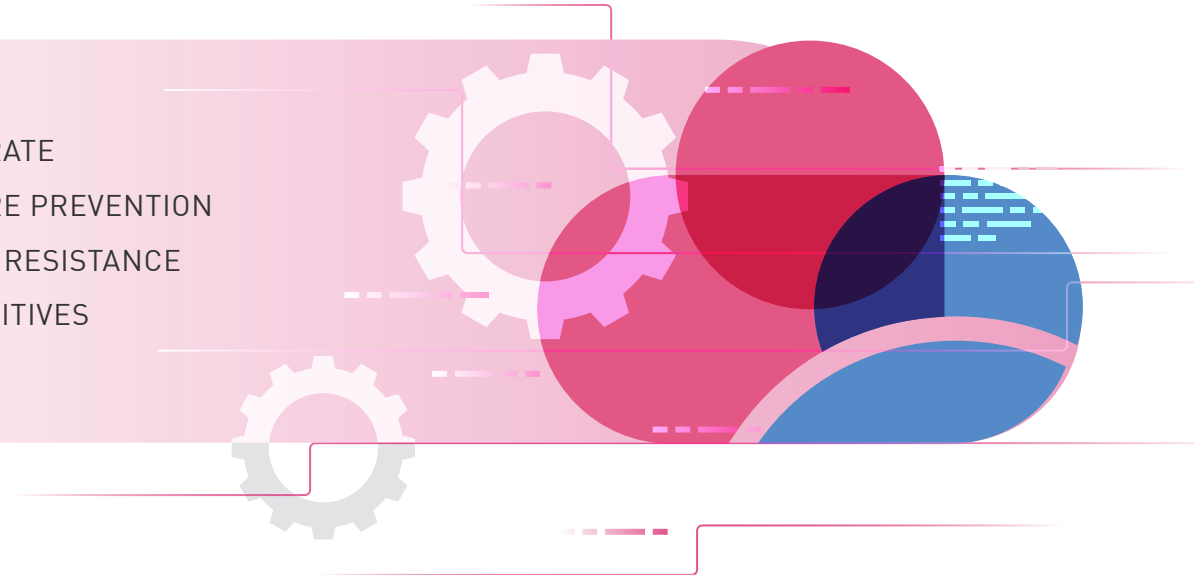
How CloudGuard Compares with the Competition

Table 2 compares CloudGuard and the cloud network security solutions of leading cloud security vendors:

CONSIDERATION	CLOUDGUARD	CLOUD SECURITY COMPETITORS
1 **Deep Security, Advanced Threat Prevention**	Provides enterprise-grade threat extraction and sandboxing, including zero-day threats.	Provide threat extraction and sandbox capabilities but cannot block zero-day threats.
	Check Point detects and prevents against a large number of risky apps and known vulnerabilities.	Competitors detect and prevent against fewer risky apps and CVEs, according to their own online publications.
2 **Borderless**	Supports the broadest range of public and private cloud providers, including Azure Stack, IBM Cloud, Alibaba Cloud, Huawei, Tencent, OpenStack, Nutanix, Microsoft Hyper-V and KVM.	Support a subset of these. Often their integration with some cloud providers lacks depth and functionality (e.g., not integrated with VMware vCenter).
4 **Automation / Integration and** 5 **Ease of Use (Licensing)**	Customer-centric licensing: allows automatic license assignment per used cores in public cloud (BYOL), managed centrally.	Require manual license assignment, with no central management.
5 **Integration and Ease of Use**	Automatically queries cloud provider APIs to import and update asset/object name and tags.	Provides limited dynamic enforcement; objects must be created manually and then linked to a security policy.
	Optimized for how real users work to solve real problems easily and efficiently: Testing shows that CloudGuard Network Security is easiest to use over standard cloud network security use cases.	To complete three standard cloud network security use cases, leading cloud network security vendors require on average 3-4 times longer, 4 times more mouse-clicks and 4-10 more menus navigated than CloudGuard. For details, please refer to the Agony Meter.
6 **Visibility**	Dynamically updated cloud instance names are used in logs, events, and reports. Can search logs by VM/instance name.	Cloud instances in logs, events and reports are identified by dynamic, hard-to-resolve IP. Logs cannot be searched by VM/instance name.
9 **Vendor Support and Industry Recognition**	NSS Labs gave Check Point a Recommended rating 21 times, which is more than all other competitors combined. Check Point also came out ahead in head-to-head comparisons.	Competitors received more Neutral and Caution ratings than Check Point. For more details, please refer to this document.
	Check Point's software is mature, with few vulnerabilities, and delivers timely fixes.	Competitors have significantly more SW vulnerabilities and take longer to fix these.
10 **Total Cost of Ownership**	For organizations with Check Point on-premises security that are migrating to the cloud, CloudGuard provides the easiest, quickest and most secure cloud network security with the lowest total cost of ownership.	

Table 2: Comparison of Cloud Network Security Key Requirements

- 100% BLOCK RATE
- 100% MALWARE PREVENTION
- 100% EXPLOIT RESISTANCE
- 0% FALSE POSITIVES



In summary, CloudGuard stands out from its competitors for the following reasons:

- Most secure threat prevention with industry-leading catch rate of malware, ransomware and other types of attacks: Highest security effectiveness score with 100% block rate, 100% malware prevention, 100% exploit resistance and 0% false positives.
- Recognized as a long-term leader by third-party analysts: 21 consecutive years as a Leader on the Gartner Magic Quadrant for Network Firewall, Recommended rating by NSS Labs, with over 28 years of security gateway intellectual property and cybersecurity technology innovation.
- Real-time detection and auto-remediation of known and unknown vulnerabilities.
- Ease of use when compared with its competitors (based on the three standard use cases that were tested). For more details, please refer to this document.
- Automatic and dynamic enforcement of security policies consistently across complex hybrid and multi-cloud environments using cloud instance objects.
- Very high level of interconnectivity and integrations throughout the enterprise ecosystem, including cloud native services, vulnerability scanners, and SIEM solutions.
- Seamless integration with Check Point's CloudGuard platform of cloud security solutions, including the powerful CloudGuard Posture Management public cloud security and compliance orchestrator, CloudGuard Intelligence, which provides multi-cloud security monitoring and analytics, CloudGuard Workload Protection which delivers full protection of modern cloud workloads, including serverless functions and containers, and CloudGuard AppSec, which automates application security and API protection, powered by contextual AI.

5 Five Questions You Must Ask Cloud Security Vendors

When an enterprise chooses a specialized cloud network security vendor, it expects a solution that is easy to deploy and scalable as well as one that visualizes the entire cloud network security environment, supports single-pane, policy-driven security management, enforces compliance best practices, and provides comprehensive real-time threat prevention and remediation.

With this in mind, here are five questions that you must ask cloud security vendors, or cloud providers with security services, as you consider which specialized cloud security solution is optimal for your organization:

Q1 How do you preempt cyber security attacks before they can harm our cloud assets?

Being able to detect known threats in real time is no longer sufficient to protect cloud assets. Your cloud security solution must also be able to apply advanced threat intelligence, emulation and extraction techniques in order to provide real time detection of unknown zero-day threats. In addition, the solution must be able to demonstrate that it immediately and automatically neutralizes all detected threats (known or unknown) before they can compromise cloud-based applications and services and their data. Lastly, does the vendor have an industry-recognized security track record or are they not cybersecurity experts and relatively new to the security scene?

Q2 How do you support our security posture requirements?

Whether or not your company is subject to formal regulatory laws or standards, compliance with data protection best practices is a critical business requirement these days. Your cloud security solution must make it easy to define security policies and enforce them consistently across your multicloud, hybrid architecture. Further, those policies must be automatically updated, with no need for human intervention, in order to keep pace with your dynamic and elastic cloud environment. Compliance monitoring must be continuous and alert your team to irregularities. And audit reports should be available at the click of a button.

Q3 Can you give us a single source of cloud security truth and a single point of cloud security control?

There are many cloud security stakeholders in your company, from security teams to line of business managers and C-suite executives. The solution must be able to provide a cross-organizational single source of truth of the current cloud security status in a highly visual and easy-to-read format. In addition, security teams must be able to centrally define, implement, and maintain security policies and gateways for all relevant cloud environments—public, private and hybrid—in a single, intuitive command and control interface.

Q4 Are we going to have to disrupt our current compliance and security practices and the tools that support them?

You have invested heavily in your compliance and security programs. You have well-defined best practices and workflows and a well-functioning stack for vulnerability scanning, configuration and change management, asset management, infrastructure provisioning, and more. You need to be sure that your cloud security platform does not disrupt what is already in place but rather extends your current capabilities with deep and programmatic integration.

Q5 How can we be sure that you can continue to meet our cloud security requirements as they evolve over the long term?

You are in it for the long haul and your cloud security vendor has to be a reliable partner. Here you need to look carefully at the vendor's track record in terms of sustained investment in innovative intellectual property over time. They should be security thought leaders who anticipate trends and launch new products and features at the cutting edge. They should be recognized by industry watchers as significant players. And they should have a global support infrastructure that can provide real time responses to specific issues, as well as advisory guidance for your long-term strategies.

Summary and Calls to Action

Cloud services are revolutionizing the way we build and deploy applications.

Cloud migration, which is the process of migrating data and workloads from on-premises to a cloud computing environment, has become a major task for IT teams. As part of this process, each organization must consider carefully how it will uphold security requirements in the cloud environment, especially their cloud network security.

For organizations evaluating cloud network security solutions, this Buyer's Guide explains the top ten considerations with explanations why each consideration is important. The document introduces Check Point's CloudGuard Network Security and describes how it answers the top ten considerations and provides examples from customer stories and testimonials relevant to each consideration.

The cloud providers offer some tools and services to help their customers monitor and secure their cloud resources; the Buyer's Guide explains how CloudGuard Network Security enhances and complements these solutions.

The document then compares CloudGuard Network Security with the cloud network security solutions of leading cloud security vendors.

Finally, the Buyer's Guide provides five questions that organizations must ask their security vendors, preferably before the solution is chosen and implemented.

Organizations using Check Point on-premises security gateways and in the process of migrating to the cloud with CloudGuard receive unified and consistent security management of all their on-premises and cloud environments and experience the most secure, easiest and quickest cloud migration, with lowest total cost of ownership.

Contact Check Point for more information or to discuss your cloud security needs with a cloud security engineer, or schedule a personalized demo of CloudGuard Network Security to understand the best and easiest way to protect your cloud assets.

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