
CHECK POINT™
CLOUD WITH CONFIDENCE
RE-IMAGINE CLOUD SECURITY
YOU DESERVE THE BEST SECURITY

THE CLOUD SPRAWL

The use of the cloud drives multiple business benefits, including decreased time to market, increased security, and business growth. Widespread recognition of these benefits had led to broad cloud adoption. In fact, according to Flexera's Annual State of the Cloud Report for 2020, 90% of those surveyed said they are using at least one cloud service in their organization.

While public cloud providers dedicate extensive efforts to security, customers retain responsibility for how they use those services, including the data that is stored in them, and how it is shared and accessed. There are many different ways to protect your data in the cloud, and organizations are failing to do the vast majority of them. Gartner research has found that, through 2022, at least 95 percent of cloud security failures will be the customer's fault.

The Rising Complexity of Multi-Cloud and Cloud Sprawl

The cloud is the single most disruptive technology to enterprise IT since the internet itself. It's easy to see how growth is accelerated by functionality such as enabling workers to collaborate and easily share files with external parties. While cloud service providers expand their service offerings and organizations benefit from adding more workloads into the cloud, security must cope with the growing challenges.

In 2020, multi-cloud is the norm. Most organizations leverage a myriad of SaaS apps as well as public and private clouds, further increasing complexity. According to Flexera's Annual State of the Cloud Report for 2020, of those organizations using cloud services, 93% have a multi-cloud strategy that combines multiple public and private clouds. 62% of organizations using public cloud are using more than one public cloud. More than half of organizations (53%) are using multiple public and multiple private clouds, followed closely by 33% using a single private cloud and multiple public ones. The 2019 SANS State of Cloud Security Survey listed challenges including inadequate API and automation options for managing the multi-cloud environments that companies increasingly find themselves navigating.

Additionally, while needing to secure a rising number of total services, the complexity within each service is also rising. For example, AWS added approximately 1,800 features in 2019, compared to about 28 features the first year it launched. You must support the rapid pace of deployment within your own organization, as well as the rapid release of new features and functions from your service providers resulting in yet more sources of potential for misconfigurations.

Of course, we should expect cloud security complexity to only increase in the future. It is likely that at least one new groundbreaking technology will become a standard that you will need to quickly support for both developers and customers, resulting in additional security challenges.

Unique Challenges of Cloud Security

Security professionals are now faced with the challenge of securing everything across multiple clouds. Of course, it is impossible to copy and paste security strategies from on-premises to cloud (or even from one cloud to the other). Cloud is no longer one parameter. You must secure access, manage identities, and constantly audit and govern accounts, to name just a few.

Security professionals must keep pace with the ever-increasing velocity of agile software deployment. Additionally, difficulty obtaining visibility and the lack of end-to-end context around risk further inhibit your ability to secure the cloud. With increasing sprawl of workloads across multiple public and private clouds, getting control of it all grows ever more difficult. These challenges are only exacerbated by the security gaps inevitable with disparate solutions. Questions that appear simple can now be difficult to answer, such as:

- How many accounts do we have?
- Did the developers add machines, new functionality, or connect to the outside world?
- Who put that there?
- Is it configured properly?
- Does it have vulnerabilities?
- Can I stop them before it hits runtime environment?
- How do I detect attacks?

You Installed it... But Did you Configure it Correctly?

In its 2020 Data Breach Investigations Report (DBIR) Verizon Enterprise showed that errors constituted one of the top causes in the data breaches it examined. Verizon's researchers attributed 21% of those incidents to misconfigurations. In total, human error accounted for 22% of all breaches. According to Symantec's *2019 Internet Threat Report*, in 2018 (AWS) S3 buckets emerged as an Achilles heel for organizations, with more than 70 million records stolen or leaked as a result of poor configuration.

While organizations recognize that misconfigurations occur, most grossly underestimate their prevalence. In fact, many misconfigurations go unnoticed.

Not only are organizations unclear about the misconfigurations inside their cloud environments they don't even know what cloud environments they are leveraging.

Some good news: It is within your control to prevent this from happening.

The reality is that most attacks are not sophisticated. By merely exploiting simple mistakes, they are able to succeed and start the kill chain of events in an attack.

More bad news: maintaining control is very difficult.

The Need for Automated, Unified Security Solutions

Getting control of your cloud environment far exceeds the limits of human multitasking. No matter how large the team, you cannot scale to keep pace with the automated attacks we are all facing. You cannot delay every new software deployment in order to manually configure security.

You need to keep things in check in an automated manner that controls everything, everywhere.

It is hard for security to be proactive, but you still must maintain control, governance, and observability across your cloud environment.

Cloud breaches are getting even more common. Hackers are getting more sophisticated, and what they stand to gain only increases, as accessing your cloud means accessing more data. In a carefully planned attack involving lateral moves, it only takes one attack vector, one vulnerability, one open and unconfigured resource, left unchecked for a sequence of kill chain events to take place before a breach. Continuously checking, and rechecking your entire cloud landscape at scale and speed is humanly impractical without automation.

Cloud Native Security for All Your Assets and Workloads with Check Point CloudGuard

Check Point CloudGuard's Native Security platform protects assets in the cloud from advanced threats with dynamic scalability, intelligent provisioning, and consistent control across physical and virtual networks, from CI/CD to production. CloudGuard seamlessly integrates with the largest number of cloud platforms and cloud-based applications to instantly and easily protect any cloud service.

With CloudGuard's flexible rules engine and Global Security Language (GSL), you can easily make customizations. Build your own rule sets and customize your own settings such as tags and specific regions. CloudGuard also provides customizable dashboards, including custom widgets as well as out of the box dashboards for any type of KPI.

Additionally, you can support any downstream process with APIs and integrations. In fact, CloudGuard supports more API calls than any other vendor, and provides continuous automated analysis of security posture from CI/CD to production with automatic remediation.

With CloudGuard, you can attain complete protection against malware and zero-days, and share security context to protect workloads during development and runtime.

DEVELOPERS AND DEVOPS ARE MOVING FAST

Many organizations are now developer-centered, incentivizing developers to develop and deploy faster to market. The time difference between when a piece of code is written and when it runs is shortening. Typical application development time and time taken before deployment into cloud have transitioned from months, to multiple times a day. Security is trying to keep up but often lags behind. Sid Sijbrandij, CEO and cofounder at GitLab stated, this year's Global DevSecOps Survey shows that there are more successful DevOps practitioners than ever before and they report dramatically faster release times, truly continuous integration/deployment, and progress made toward shifting both test and security left.

Even the functions of individual jobs move quickly. Github's Fourth Annual DevSecOps Survey uncovered how roles across software development teams have changed as more teams adopt DevOps. The survey found that rising rates of DevOps adoption and implementation of new tools has led to sweeping changes in job functions, tool choices and organization charts within developer, security and operations teams.

And it is only getting faster. The scope of the threat landscape is accelerating at the same time we are accelerating cloud adoption.

- The number of devices has grown exponentially every year and is likely to accelerate.
- Vulnerabilities increase daily.
- Nearly 60% of companies report deploying multiple times a day, once a day or once every few days.
- With increasing network speeds, an org's entire database can be exfiltrated in the blink of an eye.

Additionally, developer's modern toolbox has many resources, such as APIs, modern delivery techniques, and multiple clouds. They are also able to leverage the wisdom of others with open source. ***Security must cope with the challenges this brings.*** Organizations must figure out how to work with developers and the DevOps automation culture in order to still deliver secure, continuous release cycles — and quickly; security automation, everywhere is key.

Security Must Maintain That Speed

Application developers are encouraged to move very fast. While some degree of mistakes are acceptable, for developers as they will be resolved as part of continuous iteration and release cycles, security teams are faced with the pressure to always be right. When you are not right, you need to be wrong in the right direction. While some false positives are acceptable, you must have zero false negatives. And you must accomplish this while not impacting the developers.

Unfortunately, impacting the developers has become common enough to be the expectation. According to the Oracle and KPMG Cloud Threat Report 2020, Collaboration with the cybersecurity team is perceived as threatening to throttle speed.

No is not an option.

Cloud security must get developer-friendly, integrated and transparent. While it would certainly make your job easier to simply delay deployments, security professionals have to figure out how to enable developers instead of saying, no, or wait. Echoing this sentiment, Brian Jensen, Managing Director, Oracle Practice, KPMG LLP, described the need for IT and security leadership organizations to be nimble and help enable while balancing protection.

With developers releasing updates so quickly, they are also distributing risks immediately. Security protections must follow the same automated path and self-publish. Those protections must take the same path and speed as development, working with development toolchains that automatically enable posture checks and protections without slowing things down.

Complexity within Your Organization

Dennis Gaughan, Distinguished VP Analyst with Gartner, described the need to replace the phrase, shadow IT with citizen innovation. Gaughan suggested IT professionals think about how to leverage the capabilities of the broader population of the organization. Shadow IT is happening for a reason and you need to understand why it is happening. Shadow IT happens because either implementation of what is needed is restricted or unavailable from IT, or IT is taking too long to implement it.

Adopting this view for software development, aim to embrace the speed at which your colleagues in development are moving. Rather than attempting to restrict momentum and impose delays, aim to empower their velocity, because if you do not, they will find a way around you.

Build Trust Internally and Shift Security Left

It is important for security professionals to build trust with developers and DevOps. To accomplish this, you must understand their working procedures, specifically the speed with which they deploy code and progress to the next iteration and the DevOps tools they use to do this. You need to deploy solutions that live inside this context.

It is vital to shift security *left* in the software development lifecycle, implementing security during development, rather than waiting for deployment, or worse, *after* deployment. Make developers part of the process rather than resisting. For example, conduct vulnerability scanning at the point of deployment check-ins by integrating with their development orchestration tools e.g. Jenkins or Maven. Offer developers self-service functionality to assess security of a stack they are about to deploy. More than 70% of applications are developed using open source components, which is notorious for vulnerabilities and *poison the well* attacks. Use Software Composition Analysis (SCA) tools to provide risk analysis of open source components to developers early in the development process, so vulnerabilities are caught early

As Qualys Marco Rottigni tells Computer Business Review, Developers should be empowered with plugins that trigger security and compliance controls at every step of the DevOps process, exposing the results right within the tools they commonly use to enable rapid remediation of the vulnerable code.

Automate remediation. Do not create tickets to solve things that could be resolved in an automated way. Enable developers to do their jobs, with security ingrained, and without adding an overhead to their work. Provide tools to automate tasks, such as generating permissions for Lambda functions. ***Take steps to remove friction.***

Automation is Crucial

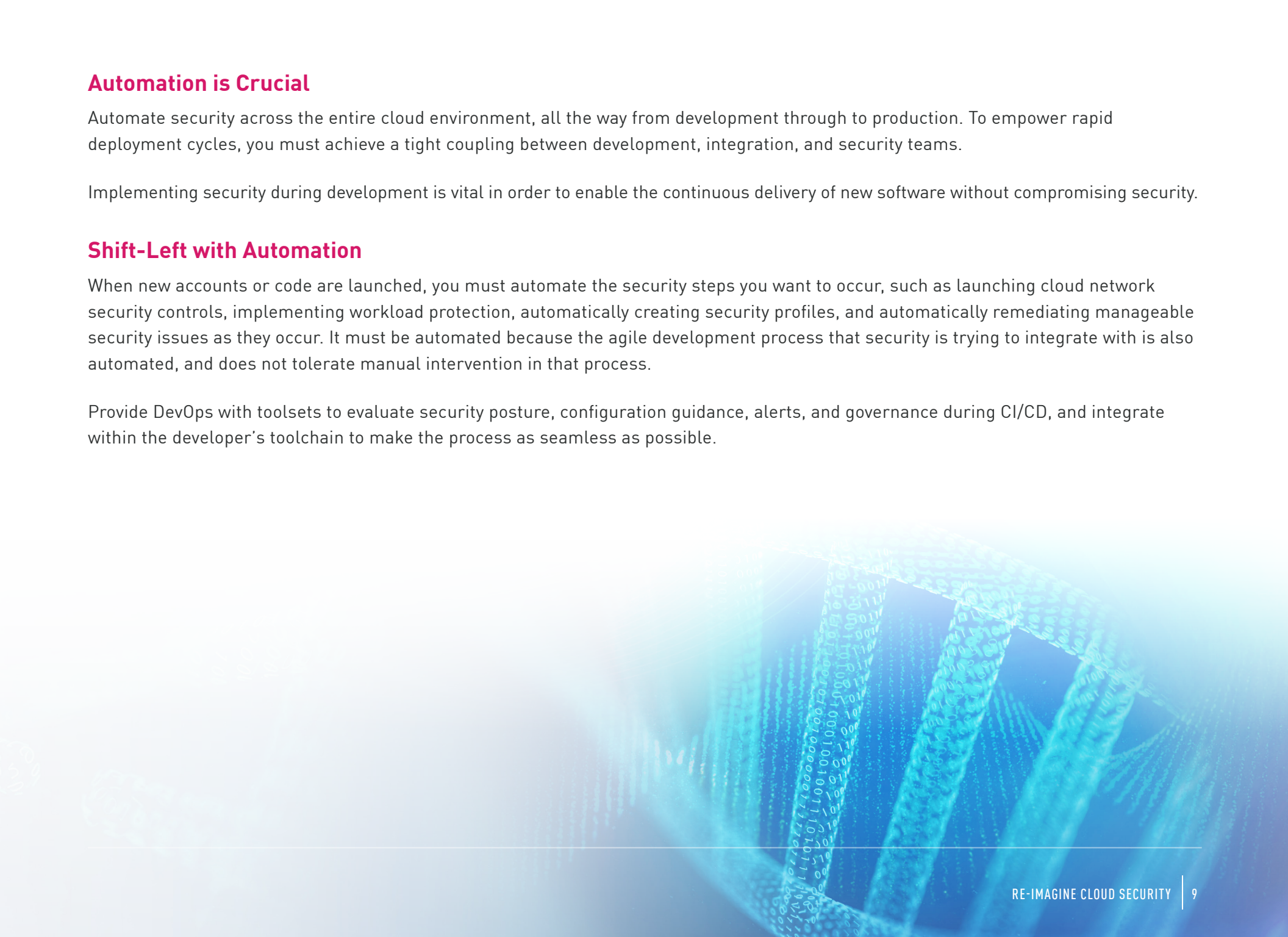
Automate security across the entire cloud environment, all the way from development through to production. To empower rapid deployment cycles, you must achieve a tight coupling between development, integration, and security teams.

Implementing security during development is vital in order to enable the continuous delivery of new software without compromising security.

Shift-Left with Automation

When new accounts or code are launched, you must automate the security steps you want to occur, such as launching cloud network security controls, implementing workload protection, automatically creating security profiles, and automatically remediating manageable security issues as they occur. It must be automated because the agile development process that security is trying to integrate with is also automated, and does not tolerate manual intervention in that process.

Provide DevOps with toolsets to evaluate security posture, configuration guidance, alerts, and governance during CI/CD, and integrate within the developer's toolchain to make the process as seamless as possible.



CloudGuard Lets You Shift Left and Automate Security at the Speed of DevOps

Security needs to work within the operational context of your environment and that means fast deployments. Only Check Point supports single-click and agile deployment models that align with the dynamic nature of cloud services, making adoption and expansion of cloud services seamless.

Check Points Cloud Native Security Platform — CloudGuard — ensures your security protections keep pace with all changes to your cloud through advanced features such as auto-provisioning and auto-scaling along with automatic policy updates.

Seamlessly integrate protections and controls into your CI/CD tools, like CloudFormation, Ansible and Terraform, and evaluate security posture pre-deployment and scale across hundreds of thousands of cloud assets. In addition, automatically profile and define application behavior, and enforce zero trust boundaries between cloud workloads (e.g. containers and serverless) during production.

CloudGuard's High Fidelity Posture Management (HFPM) empowers security to shift left. CloudGuard provides continuous enforcement of regulatory compliance standards and security best practices with the most comprehensive compliance engine. HFPM help you prevent critical cloud security misconfigurations and keep up with evolving posture management security and compliance best practices, including auto remediation. More so, it helps organizations comply with regulatory and industry standards, such as HIPAA, CIS Benchmarks, NIST CSF/800-53, PCI-DSS, with the most contextual cloud security across, 300+ native cloud services.

THE PROBLEM OF THE SECURITY GAPS

The Oracle and KPMG Cloud Threat Report 2020 shows that trust has continued to grow in both public cloud infrastructure and business-critical applications as a service. However, 92% of companies surveyed have a "cloud security readiness gap" between their current and planned cloud usage and the maturity of their cloud security programs. More than 40% report a wide gap, while 48% say the gap is moderate. 70% of those surveyed report too many tools are needed to protect public cloud environments. On average, each uses more than 100 discrete security controls. Multiple security vendors, providing disparate solutions, blocking on different attack vectors all results in gaps. And those gaps create access points for attackers.

- Too much cloud complexity +
- Too many different security solutions +
- Solutions not cooperating =
- No shared intelligence or architecture, gaps, and risk.

To overcome these gaps, it is imperative to implement tools and resources to help simplify the security management of the cloud and take control of security.

Visibility and End-to-End Context are Vital

It is important to understand how resources should behave and so you can observe when that behavior deviates. This requires a complete picture of your environment and context around all your cloud log and event data, so you know what to expect, and can more effectively detect and visualize threats.

Additionally, visibility is vital in order to map to regulatory requirements and achieve compliance with laws and relevant industry standards. It can be difficult to understand where you have sensitive information within your infrastructure, particularly with ever-expanding cloud sprawl.

Visibility also requires context to be useful. Viewed without context, cloud ephemeral events can be hard to piece together - especially when there is a lot of data to look at.

Without consolidated dashboards, it is very difficult to identify and act on threats in a timely manner.

Visualize and Assess Security Posture Across a Broad View

With CloudGuard, you get complete visibility into all assets, workloads, and security policies across virtual networks, regions, and accounts on public clouds & K8S. You also gain a broad view across multiple public clouds and across all data types (user, network, cloud logs).

Additionally, you can visualize and assess security posture, detect misconfigurations, model and actively enforce gold standard policies. CloudGuard protects against attacks and insider threats and empowers you to leverage cloud security intelligence for cloud intrusion detection.

Machine learning incorporates multiple data sources across different cloud assets, determining typical use to effectively detect anomalies. CloudGuard can create rules and readily identify threats and unnecessary exposure. You can access detailed forensics and assess the level of exposure, and drill down to see malicious activity against specific assets.

So, What to Do?

Enabling growth and maintaining security can be conflicting objectives. While no one wants to sacrifice either, the office of the CISO must retain control.

You have to complement compliance tools with a remediation process.

With the endless number of configurations and options in most modern multi-cloud infrastructures, your cloud security approach should be multi-layer.

Get the Visibility and Context You Need to Automate Security

The Check Point CloudGuard platform provides cloud native security for all your assets and workloads in your public, private, hybrid, or multi-cloud environment. CloudGuard enables you to automate security everywhere at the speed of DevOps, with unified security management.

Get the visibility you need along with the context that is crucial to make sense of data. Understand the connections between virtual networks, resources and workloads, with enriched graphical representation of logs. Visibility is further enhanced by high fidelity, enabling you to access detailed forensics behind what is occurring. Assess the level of exposure and determine if alerts are critical, as well as detect incidents and respond fast.

IMAGINE HARMONIOUS CLOUD SECURITY

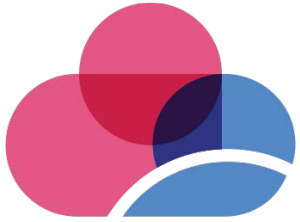
While organizations are benefitting from the use of the cloud, gaps in security, errors, and misconfigurations are prevalent. Disparate solutions bring security gaps. Your ability to secure the cloud is further inhibited by difficulty obtaining visibility and the lack of end-to-end context around risk. Additionally, the duty is becoming perpetually more challenging with increases in both cloud sprawl and the velocity of agile software deployment. And no one wants to sacrifice growth or speed for security.

The answer is harmonious security that works at scale and moves at the speed of cloud. Meeting the challenge of securing modern multi-cloud infrastructures requires sharing security context under one cloud security platform, and shifting security left while also automating it. Imagine Harmonious Cloud Security with Check Point CloudGuard.

Cloud with Confidence. Check Point CloudGuard. Security Automated Everywhere

Check Point CloudGuard's Cloud Native Security Platform is designed for advanced threat prevention, multi-vector cyberattacks targeting enterprise cloud services. Effectively secure the sprawl with one unified cloud native security platform that automates security posture at scale, preventing advanced threats and giving you visibility and control over all of your workloads, across any cloud.

Deliver zero trust, advanced threat prevention with workload protection, including security hardening, runtime code analysis, web and API security and prevent threats. Only CloudGuard offers High Fidelity Posture Management (HFPM) to prevent critical cloud security misconfigurations and keep up with evolving security and compliance best practices, with enriched vulnerability management findings to better identify, prioritize, and auto-remediate events based on public exposure.



CloudGuard

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

www.checkpoint.com