Are you exposed and unprotected in cloud environments?

Hosting workloads in the cloud offers enterprises agility, speed, efficiency, and reduced costs. CheckPoint CloudGuard protects your unprotected environments with advanced, multi-layered threat prevention security and provides secure remote connectivity to all your cloud resources.

With benefits like increased agility, improved efficiencies and lower overall fixed costs, it’s no surprise that nearly 95% of businesses are now using the cloud. In conjunction with this rapid adoption, Microsoft users of cloud services are experiencing a 300% increase in cyber-attacks targeting their cloud environments (*Volume 22, Microsoft Security Intelligence Report*).

CloudGuard is the only advanced threat prevention for all leading public and private cloud platforms including: Amazon Web Services, Google Cloud Platform, Microsoft Azure, Cisco ACI, OpenStack, VMware NSX, VMware Cloud on AWS, VMware ESX, Alibaba Cloud, KVM, Hyper-V and more.

Cloud providers protect their infrastructure, cloud fabric, hypervisors, services and tenant environments. They are NOT responsible for
protecting any assets or data that customers place on their networks. It is imperative for businesses to understand that they are responsible for protecting all data, workloads and assets that reside in the cloud. This is what cloud providers refer to as the “shared security responsibility” model. The security controls cloud providers offer are port filters or access control lists (ACLs) that allow clients to segment their environment and control both inbound and outbound traffic.

Beyond that, there is no native mechanism in place to determine whether traffic flowing in or out of a customer environment is benign or malicious. Bottom line; don’t be lulled into a false sense of security. Cloud-based applications provide several access inroads into customer networks and cybercriminals only need to find a way to get in. The rush to the cloud should not outweigh the due diligence required to keep your environment secure.
CloudGuard provides industry-leading advanced threat protection and single pane of glass management for easily extending advanced security protections to cloud environments. CheckPoint ensures that your cybersecurity strategy aligns with your business goals while delivering consistent protections for all corporate data – both on-premises and in the cloud.

CloudGuard SaaS prevents advanced persistent attacks (APTs) and unknown zero-day malware from infecting SaaS applications, using real-time sandboxing; and ransomware protection that are powered by integrated, real-time cloud-based threat intelligence to identify new threats. To prevent account takeover of SaaS-based applications,
CloudGuard SaaS uses ID-Guard technology, which identifies and blocks illegitimate users from accessing SaaS accounts, and blocks unauthorized users and compromised devices. CloudGuard SaaS also ensures consistent policies are enforced across CheckPoint security gateways and SandBlast Mobile solutions, enabling consistent security and management across the enterprise via a unified security management platform.

**IPSec and CheckPoint can help your organisation protect unprotected cloud environments.**

For more information you can also visit the following resources:

- CloudGuard Solution Overview
- CloudGuard SaaS Overview
- IPSec – CheckPoint Real Time Detection & Incident Response Press Release
- Preventing Gen V Cyber Threats > watch the video
- 2017 Cloud Breach Examples
- Checkpoint 2017 Cyber Attack Trends Report

For more information or if you’d like a demonstration of IPSec’s capabilities please contact your IPSec account manager.

1300 890 902

enquiry@ipsec.com.au