PUBLIC SECTOR NETWORK

September 2022

# Cloud Security: A Guide for Government Decision-makers

Sponsored by CHECK POINT™

# Table of Contents



# >> Introduction

**Cloud is helping to modernize government services and transform citizen interactions. But cloud security hasn't kept up with the pace of cloud adoption. Ensuring a secure, compliant environment in the cloud is critical—particularly for public-sector organizations that collect, store and manage highly sensitive data on behalf of their citizens.**

Governments are stewards of citizen data, from social insurance numbers to healthcare records to financial data. Maintaining security, privacy and compliance is crucial to maintaining trust with the citizens they serve, but governments also need to provide seamless digital services to keep pace with the private sector—albeit with fewer resources.

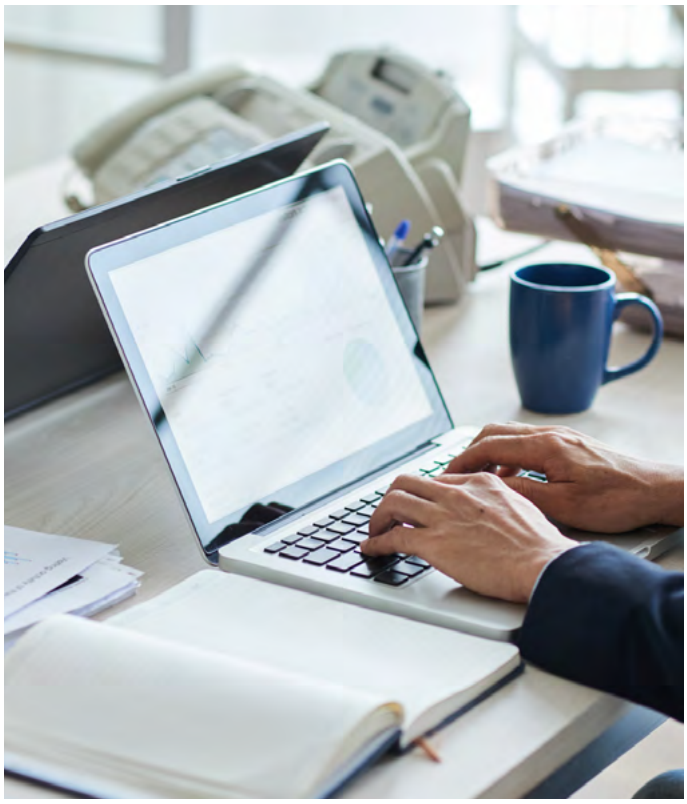
Many government departments and agencies operate in silos and still rely on legacy infrastructure, though the COVID-19 pandemic forced many to transform their operations and start migrating at least some of their workloads to the cloud. Government employees continue to work from home, at least part of the time, which has greatly expanded the network edge.

This makes it easier for bad actors to target the public sector with malware and ransomware, as well as social engineering attacks. Add to that an acute talent shortage for skilled IT workers and cybersecurity professionals—where government often can't compete with their private-sector counterparts—and it's clear why cloud security is such a pressing issue in the public sector.

# >> Understanding the Cloud Landscape

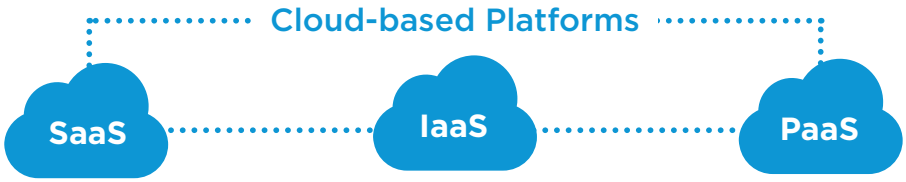
Organizations are continuing to rely on multi-cloud solutions, according to Check Point's 2022 Cloud Security Report. A survey of 775 cybersecurity professionals found that 76% are using two or more cloud providers, compared to just 62% from the previous year. And 35% have more than 50% of their workloads in the cloud, with 29% stating they anticipate moving this number up to 75% in the next 12-18 months.

Understanding the cloud landscape, however, means understanding the different types of cloud deployments. A private cloud is controlled by a single organization, while a public cloud offers shared infrastructure in a multi-tenant environment. The big difference? With private cloud, the onus is on the organization to manage and support that infrastructure, similar to on-premise equipment. It's secure, but less scalable, agile and flexible than public cloud.



With public cloud, the organization is a customer of the public cloud provider—such as Amazon Web Services (AWS), Microsoft Azure or Google Cloud, among other smaller players. While the leading cloud platforms offer cloud-native security features and services, customers also bear some responsibility for securing their workloads.

Hybrid cloud is a combination of both private and public cloud (and may include edge computing and the Internet of Things), while multi-cloud is a combination of public clouds—which is becoming much more commonplace, as noted in the 2022 Cloud Security Report.




Most cloud-based platforms use a combination of SaaS (Software-as-a-Service) and IaaS (Infrastructure-as-a-Service), along with PaaS (Platform-as-a-Service). Here's how they work:

- **SaaS** makes software available over the Internet, typically for a monthly subscription fee
- **IaaS** provides cloud-based alternatives for on-premise infrastructure, such as storage, networking and virtualization
- **PaaS** provides a framework—including servers, storage and networking—that allows developers to build their own apps and software, managed by a third-party provider

**A Unified Approach to Cloud Security -**
https://www.checkpoint.com/infinity-vision/

## >> *Cloud Computing Benefits*

Public-sector organizations have tended to lag behind their private-sector counterparts in the adoption of cloud services, in part due to the challenge of changing leaders and administrations. Previously, investments in cloud were often piecemeal, resulting in a "patchwork of cloud utilization without the organizational foundations needed to realize its full benefits," according to a paper by Deloitte Insights.

That changed during the pandemic, when public-sector organizations turned to cloud to solve some of their most pressing challenges, such as enabling remote work and providing virtual access to government services. But the key to an ongoing successful shift to cloud, says Deloitte, is shifting how governments use cloud—not just rehosting existing services to cut costs, but applying the unique properties of cloud to improve government services.

Public, hybrid and multi-cloud strategies free up government IT resources, so they can focus on the business of government instead of managing data centres. Moving workloads to the cloud can reduce time to market for new programs and services, scale those programs and services as demand increases and provide faster recovery if applications go down. It also offers low up-front costs, can help to control costs over time and can even create new revenue-capturing opportunities.

But cloud security hasn't kept up with the pace of cloud adoption. Ensuring a secure, compliant environment in the cloud is critical—particularly for public-sector organizations that collect, store and manage highly sensitive data on behalf of their citizens.

## >> *Managing Cloud Risk*

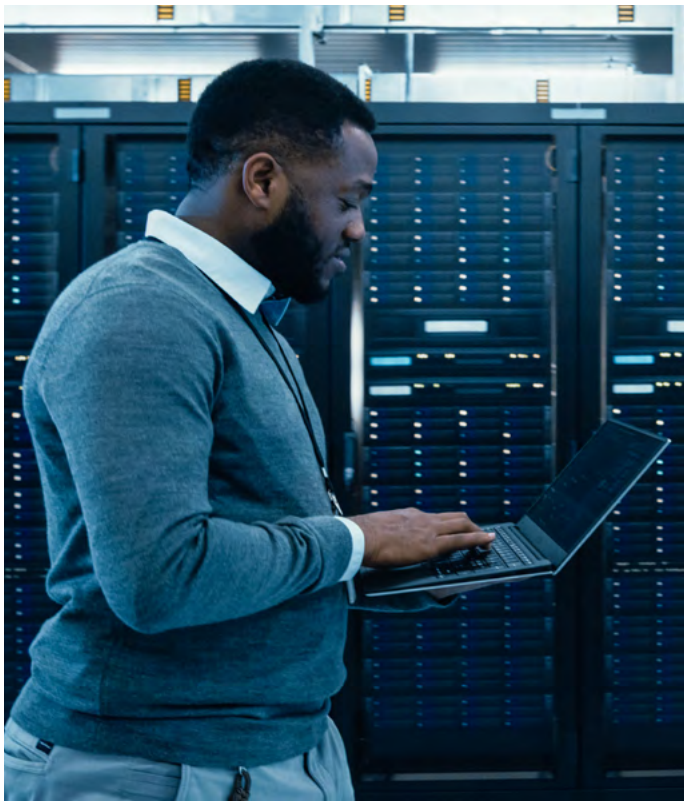
The *2022 Cloud Security Report* found that a quarter of organizations (27%) had experienced a public cloud security incident, with misconfigurations clinching the top position of security-related incidents—surpassing 'exposed data by user' and 'account compromise.' Indeed, managing multiple cloud vendors has created greater complexity than first anticipated.

**27%**

had experienced a **public cloud security incident**

At the same time, not all public-sector organizations fully understand the shared responsibility model of public cloud. But cloud security—which refers to the technologies, policies, controls and services that protect cloud data, applications and infrastructure from threats—is a responsibility shared by the cloud provider and the customer.

The cloud provider is responsible for safeguarding the infrastructure, as well as patching the physical network. The customer, however, is responsible for managing user access privileges, safeguarding cloud accounts from unauthorized access, protecting cloud-based data assets and managing compliance, among others.



Since governments collect, store and manage sensitive data on behalf of their citizens, they need to ensure that any workloads they're migrating to the cloud adhere to configuration and hardening standards, including GC cloud security risk management procedures. While leading cloud providers are aligned with the most well-known accreditation programs—such as PCI 3.2, NIST 800-53 and GDPR—customers are ultimately responsible for ensuring that their workloads and data processes are compliant.

This is even more challenging in a hybrid or multi-cloud environment, and when adopting modern cloud approaches such as automated Continuous Integration and Continuous Deployment (CI/CD) methods, distributed serverless architectures and ephemeral assets like containers or Functions-as-a-Service.

# >> Cloud Security 101

Creating a security-first culture means striking a balance between the use of cloud services and protecting sensitive data and transactions. But traditional security tools aren't effective in a flexible and dynamic environment such as cloud. Managing security across hybrid and multi-cloud environments requires tools that work across public cloud providers, private cloud providers and on-premise deployments, and offer edge protection in geographically distributed organizations.

Supplementary third-party solutions are critical in achieving enterprise-grade cloud workload protection from breaches, data leaks and targeted attacks in the cloud. But multiple, disjointed solutions inherently have gaps in visibility and integration complexities, which creates more work for DevSecOps teams. Automation and machine learning will be critical to cloud security strategies going forward, as will security 'platforms' over point solutions.

For example, the Cloud-Native Application Protection Platform (CNAPP), originally defined by Gartner, emphasizes the need to focus on cloud-native security solutions that provide a complete lifecycle approach to application security as opposed to a patchwork of tools. CNAPP encompasses Cloud Security Posture Management (CSPM), Cloud Service Network Security (CSNS) and Cloud Workload Protection Platform (CWPP) in a single holistic platform.

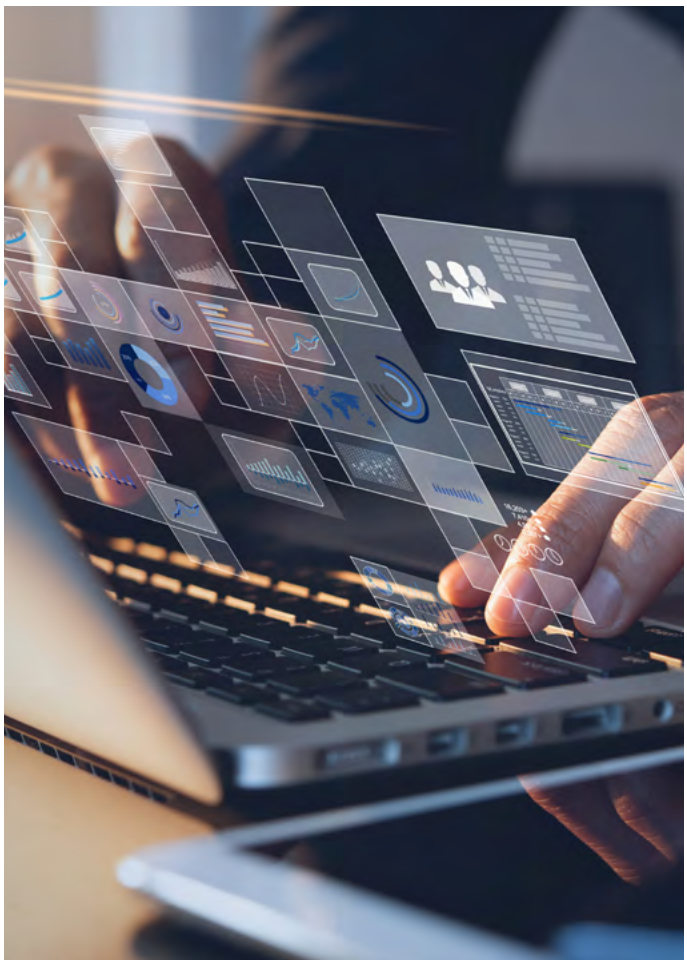
https://www.checkpoint.com/cloudguard/cloud-security-posture-management/

# >> Cloud Tools for Your Technical Team

Check Point CloudGuard is an enterprise CNAPP that provides unified threat prevention and automated security across private, public, hybrid and multi-cloud environments—ensuring the security and compliance of your network, workloads and applications from development through runtime. It includes:

- **CloudGuard Posture Management:** Provides cloud-native security posture management and account-level threat detection across multi-cloud environments
- **CloudGuard Network Security:** Delivers cloud-native network security to macro- and micro-segment assets across cloud providers and on-premise infrastructure
- **CloudGuard Workload Protection:** Integrates with CI/CD pipelines and protects workloads running on virtual machines, containers and serverless platforms
- **CloudGuard AppSec:** Automates application and API security using AI analysis to deliver up-to-date threat protection—without the need for constant human intervention
- **CloudGuard Intelligence:** Achieves a deeper layer of security and insight with intrusion detection, threat hunting and remediation

https://www.checkpoint.com/cloudguard/cloud-security-solutions/



# >> *Four Keys to a Successful Cloud Journey*

While cloud offers a path to digital government, it can also translate into greater complexity for IT teams who now have to manage and maintain security across multi-vendor as well as private, public, hybrid and multi-cloud environments. Four keys to a successful—and secure—cloud journey include:

1. **Understand the shared responsibility model:** When migrating workloads to public cloud, it's important to understand your security obligations alongside the cloud provider's security obligations for the specific type of cloud deployment.
2. **Understand the business drivers for security:** The attack surface changes when workloads are moved to the cloud. Business drivers for security reflect the vectors most likely to be exploited—and should therefore be protected vigilantly (for example, lack of proper identity management in the public cloud IaaS).
3. **Establish cloud security policies:** Written guidelines should specify which data can be stored in the cloud, which security tools and technologies will protect that data and who is permitted to access it. Automation will be key to ensuring policies are continually enforced; zero trust is a security framework that can help with policy enforcement.
4. **Augment cloud service providers' native controls:** Take a multi-layer approach to cloud security that leverages automation, machine learning and artificial intelligence. Third-party solutions should work across any cloud and any workload, and provide continuous analysis of your multi-cloud security posture—from CI/CD to production.

CHECK POINT™

## About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from 5th generation cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers multilevel security architecture, "Infinity" Total Protection with Gen V advanced threat prevention, which defends enterprises' cloud, network and mobile device held information. Check Point provides the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

Find out more about Check Point's cloud security solutions for government:

https://www.checkpoint.com/

PUBLIC SECTOR NETWORK

# About Public Sector Network

Public Sector Network is a research company that represents public sector professionals across Australia, Canada, New Zealand, and the USA. It develops roundtables, seminars, and conferences to suit current areas of interest to government agencies and their suppliers.

Public Sector Network's growing community spans across federal, state, and local government departments, healthcare, and education, allowing members to share information, access the latest in government innovation, and engage with other like-minded individuals on a secure and closed-door network.


**CANADA**
**P** +1 (647) 459 8904
**E** contact@publicsectornetwork.co

**USA**
**P** +1 (647) 969 4509
**E** hello@publicsectornetwork.com

**AUSTRALIA / NEW ZEALAND**
**P** +61 2 9057 9070
**E** info@publicsectornetwork.co