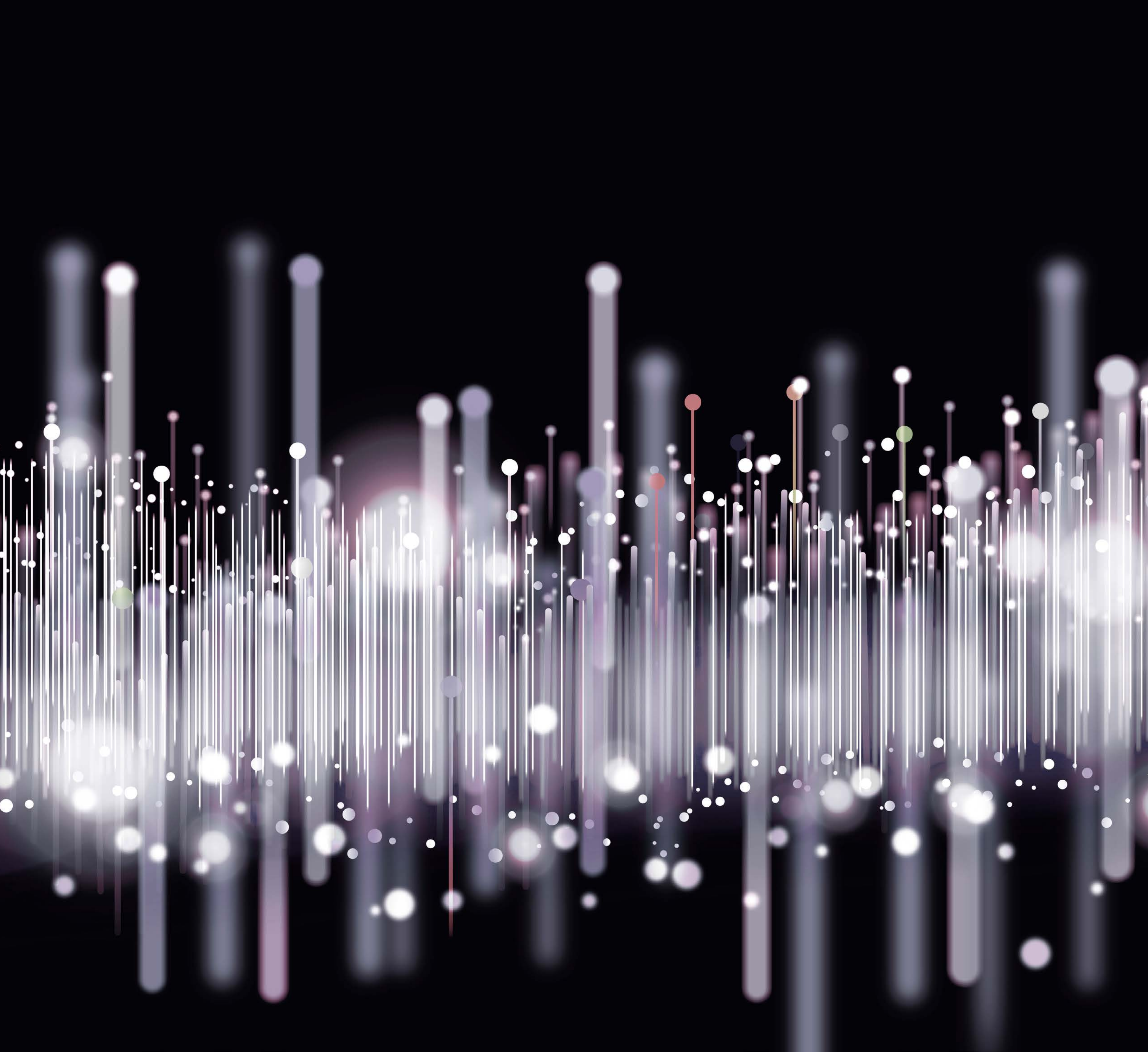


Better Cloud Adoption Through Better Security

MARKET TRENDS REPORT

govloop

Check Point
SOFTWARE TECHNOLOGIES LTD.

Introduction

Today in the public sector, the popularity and benefits of the cloud are more than apparent. Cloud offers flexible computing options at a fraction of the cost and time, and agencies can conveniently improve data storage and server processing or use Software-as-a-Service (SaaS) products through this adoption. Additionally, government mandates like Cloud Smart and security requirements like the Federal Risk and Authorization Management Program, or FedRAMP, are further driving agencies toward cloud adoption.

It's clear that cloud computing has become an integral piece of today's IT government infrastructure. Its "try before you buy" and "pay as you go" models provide agencies with the ability to test the technology, and integration with the cloud is fast and usually requires virtually no organizational downtime.

Much like other newer technologies, however, the cloud can be abused or misused. Shared responsibility, lack of visibility, internal risks, advanced cyberattacks and more are at play for agencies that move their sensitive data and applications to the cloud. In short, the complexity of security in the cloud can make it difficult for agencies to move forward.

This analysis paralysis and fear of data breaches or hacks is normal, but agencies need to progress. That means it's imperative to know cloud's vulnerabilities –especially holes in security.

To better understand how agencies can take a proactive, holistic approach to security in their cloud platforms, GovLoop partnered with Check Point Software Technologies LLC, a leading provider in cybersecurity solutions, for this report. In the following pages we break down the top security challenges with cloud and solutions for overcoming them, and gain insights from Jeremy Castleman, Federal Cloud Security Consultant at Check Point.

BY THE NUMBERS

Cloud and Security Today

65%

of IT professionals underestimate the damage caused by attacks on the cloud.

Source: Check Point Security Report Threat Prevention Research Among IT and Security Professionals, November 2018

$49.2 billion

The government cloud market is set to grow to $49.2 billion by 2023.

Source: P&S Market Research

"Commercial cloud capabilities have improved dramatically in recent years, affording federal agencies a wide variety of paths to cloud adoption. Because of that, no two moves to the cloud are the same, and agencies shouldn't just heedlessly look to replicate what they see elsewhere in government."

– Federal CIO Suzette Kent

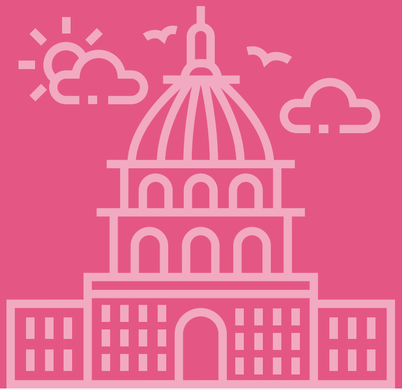
"Cloud Smart equips agencies with actionable information and recommendations gleaned from some of the country's most impactful public and private sector use cases. The new strategy is founded on three key pillars of successful cloud adoption: security, procurement, and workforce."

– 2019 Federal Cloud Computing Strategy

16%

of government leaders voiced a lack of confidence about security in environments that combine on-premise data centers, private clouds, SaaS applications and public cloud IT infrastructures.

Source: CDG



THE CHALLENGE

Achieving Security in a Complex Cloud World

Today in government, process efficiencies and increased network agility are driving SaaS, IaaS and platform-as-a-service (PaaS) technology adoption at a rapid pace. And while many agencies are adopting cloud at different rates and for different purposes, it's top of mind for nearly all government leaders.

Agencies of all sizes are rapidly migrating workloads and data to public cloud environments to improve efficiencies, drive innovation and increase responsiveness to market conditions. This new adoption, however, is also presenting agencies with a unique set of security challenges.

Below are some of the main challenges that highlight the complexity of cloud security in government today.

1. Shared responsibilities between agencies and vendors in terms of security: Cloud service providers are not responsible for securing agencies' applications and data in the cloud. They manage security of the cloud and its global infrastructure – but not what's in the cloud. Agencies still must secure their network, data and applications – and this can be difficult given limited budgets, time and skills.

2. Dynamic ever-changing workloads across multiple cloud platforms: There are multiple teams working in an agency's cloud environment, from different departments to contractors and other third parties. These users are constantly changing the cloud environment in multiple cloud platforms. This makes it difficult to implement a consistent and simultaneous security posture across a dynamic cloud environment.

3. Minimal visibility across workloads: Another obstacle to implementing a consistent and simultaneous security posture in a constantly changing environment is not having full visibility. It's critical that agencies have a tool that provides full visibility into workloads, applications and assets across multiple cloud platforms in real time. Without this visibility, they will not be able to implement continuous compliance and maintain their security posture.

4. Internal risks: Even with the best of intentions and protocols, there are benign human errors and misconfigurations that happen in the cloud. This could be a result of staff lacking expertise, having multiple management platforms or not having automation and auto-scaling available. Having to repeat processes multiple times across multiple platforms increases the likelihood of inconsistencies and configuration errors. An overwhelming majority of incidents are the result of misconfigurations, and organizations having weak identity, credential and access management. Of course, there are also the usual malicious insider threats of disgruntled employees, and the constant struggle that security teams have with shadow IT.

5. External threats: Today's attackers know that there is this new increased attack surface and that organizations are not investing enough in advanced threat prevention for their cloud infrastructure. They are relying on organizations to misunderstand the Shared Security Model, to lack visibility into their environment and to ignore misconfigurations. These vulnerabilities were not present in traditional data centers, and provide a more attractive target. This leads to large-scale, multi-vector mega attacks using advanced tools.

6. Governance, risk and compliance (GRC): Agencies need to comply with multiple regulations and compliance standards. These can be federal, state, industry or customs requirements. Furthermore, they need to be able to provide audit ready reports showing that their public cloud infrastructure conforms to these regulatory requirements.

Given these challenges, agencies need a holistic security strategy for moving to a world where complex cloud solutions are a necessary reality.

THE SOLUTION

A Holistic Security and Cloud Platform

Security is continually cited as a key barrier to widespread enterprise cloud adoption, yet traditional security approaches don't fit the dynamic nature of the cloud, leaving agencies and their data exposed.

It's time for a new security model; one that delivers a complete architecture focused on preventing attacks, provides true ease of operations and stays aligned to the dynamic nature of cloud environments.

The solution is moving toward a more holistic cloud security approach and platform. "With these challenges, we have to rethink how we approach security," said Jeremy Castleman, Federal Cloud Security Consultant at Check Point. "We have to change the way it is implemented in the cloud and ensure that we prevent advanced threats."

Cloud security tools must be flexible and agile, meaning that your platform needs automation and the ability to scale up and down securely. The security design of the platform must include the ability to secure all assets, enforce all compliance disciplines and enable business through automated deployments and adaptive policies.

This will help organizations maintain that security posture across multiple public cloud platforms. They need to be able to visualize and assess that security posture, detect misconfigurations, model and actively enforce gold standard policies.

This will go a long way toward protecting against attacks and insider threats, and will offer security intelligence for cloud intrusion detection, while helping with compliance with regulatory requirements and best practices.

BEST PRACTICES

Creating Holistic Cloud Security

☑ **Be aware of your responsibility in the cloud:** "I see many agencies that are not aware of where their responsibility lies when securing the cloud," Castleman said. "You must know that the basic explanation of this is that your cloud provider will secure the general cloud infrastructure, but anything inside the cloud you must still work to secure."

☑ **Watch out for data breaches:** It's imperative not to be lulled into a false sense of security when moving to the cloud; it's your responsibility to protect any assets and data you place in the cloud. Native tools provided by cloud platforms are not enough. To keep your cloud environment protected, it's highly recommended to deploy an advanced threat prevention solution to inspect all traffic entering and leaving your cloud to prevent attackers from targeting your assets.

☑ **Watch out for hijacked accounts with extra security levers:** Implement the use of multifactor authentication, as well as good key management practices when utilizing public cloud environments.

☑ **Train your workforce:** "Proper training and alignment of all disciplines is more critical than ever when migrating infrastructure to the public cloud," Castleman said.

☑ **Focus on encryption:** As a rule when using public cloud services, make sure to trust no one and encrypt everything. "This is true of any data stored in the cloud, but should also be true of any data transmissions to and from the cloud," Castleman said.

☑ **Deploy the right platform with a trusted vendor:** From the constant threat of malware to malicious users and misconfigurations, there are a number of specific challenges organizations face when moving data, assets and workloads to the cloud. It's important to not only understand these risks but also to identify a vendor with the technology and techniques to properly secure your cloud environment.

CASE STUDY

Mitigating Security Concerns in the Cloud

DataStream Connexion is a premier technology consulting and web application development agency. Formed in 2000, it has built web applications for the federal government, USDA, FDA, the Homeland Security Department, healthcare organizations, Fortune 500 companies and small businesses.

With the introduction of AWS GovCloud in the U.S. in 2011, the DataStream team recognized the opportunity to the cloud presents users while hosting highly regulated workloads. The newly introduced Amazon GovCloud was a perfect fit for its customers, supporting the common AWS security controls and compliance standards, but in an isolated, dedicated region designed specifically for sensitive government agency data.

In the early days of the public cloud, however, there was still pushback from DataStream Connexion's federal customer base, which was unsure of securing data in AWS.

As with every new technology adoption scenario, there were challenges that had to be worked out along the way.

With the CloudGuard Dome9 platform by its side, DataStream Connexion was able to address and mitigate each of these challenges.

The CloudGuard Dome9 service played a critical role in helping DataStream Connexion mitigate the security challenges of a cloud-based environment. With it, owner and president Eric Hoffman and his team has complete visibility into all configurations, holes, inconsistencies, vulnerabilities and any setting that has been modified.

"I want my staff to be nimble and empowered to do their work, where I can trust them to keep moving forward," Hoffman said. "I have the ability at any time, in real time, to assess why a port may be open. CloudGuard Dome9's logs and alerts are really important to me and enable my employees to be agile and work in the fashion they need to."

HOW CHECK POINT SOFTWARE TECHNOLOGIES HELPS

Effective cloud security requires a centralized and consolidated platform that is built from the ground up for the cloud and gives administrators complete visibility and active control of their cloud environments.

Check Point's CloudGuard Dome9 offers end-to-end control over the security posture of public cloud environments from a centralized console. This solves the challenge of not having visibility into a dynamic and ever-changing multi-cloud environment.

CloudGuard Dome9 provides several prevention and detection capabilities to protect cloud environments from security exposures caused by misconfigurations and breaches. With CloudGuard Dome9, organizations can automate regulatory compliance process requirements, as well as produce ongoing audit reports within seconds.

This innovative service provides a broad set of security and compliance controls, deep visualization, cloud assets management, identity and access management, and policy automation for verifiable and comprehensive security management.

"We just added a new module to CloudGuard Dome9 called Log.ic," Castleman said. "It uses cloud logs, built-in rules, threat intelligence feeds, configurations, AI and machine learning to provide traffic flow and user activity analysis and threat-hunting capabilities."

CloudGuard Dome9 also uses anomaly detection algorithms to spot potentially unauthorized or malicious activity within your cloud environments, including serverless applications. This can provide real-time policy violation and intrusion detection alerts to your security team based on user-defined criteria.

"In short, our platform helps minimize your attack surface and protect against vulnerabilities, identify theft and data loss," Castleman said.

Conclusion

While public sector cloud adoption is accelerating due to clear benefits and government mandates like Cloud Smart, security remains a key concern for many. Traditional security approaches don't fit with the dynamic nature of the cloud, and leave agencies exposed to a host of new threats. A holistic platform that helps agencies deal with the complex nature of security in the cloud is the way forward. It will enable both cloud security resiliency and scalability while minimizing the need to configure the same policy across an agency's cloud resources as it moves into the future.

ABOUT CHECK POINT SOFTWARE TECHNOLOGIES

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to corporate enterprises and governments globally. Its solutions protect customers from 5th-generation cyber-attacks with an industry leading catch rate of malware, ransomware and other targeted attacks. Check Point offers a multilevel security architecture with our new Gen V advanced threat prevention that protects all networks, cloud and mobile operations of a business against all known attacks combined with the industry's most comprehensive and intuitive single point of control management system. Check Point protects over 100,000 organizations of all sizes.

Learn more here: https://www.checkpoint.com/

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop