# Adaptive Security in a Complex Cloud Environment

**RESEARCH BRIEF**

Check Point SOFTWARE TECHNOLOGIES LTD

Swish

govloop

# Executive Summary

Government is undertaking a massive migration of on-premises resources — IT, data and workloads — to dynamic and complex architectures erected on public and private clouds. Propelling the shift are tantalizing prospects for agencies: streamlined operations, more responsive applications, better user experiences, improved data management, integrated automation, artificial intelligence (AI) and superior attainment of mission goals.

Yet digitally transformed environments, supported by multi- and hybrid cloud solutions, also change cybersecurity. Data and applications that were well-defended now exist in sprawling, complex and dynamic environments. The potential attack area is larger, and the bad guys are smarter; visibility into operations can be murky.

For organizations leaning into the digital future, the challenge is making sure cybersecurity protocols — prevention, detection and remediation — adapt to and match the dynamism and complexity of modernized IT landscapes and emerging cyberthreats.

To learn more about these challenges, GovLoop partnered with Swish Data and Check Point Software Technologies to conduct a survey about agencies' strategies against cyberthreats. It yielded a community snapshot of 50 federal employees who shared the current state of cloud security at their agencies, their pain points when handling cyberthreats and what they look for in a cloud security solution.

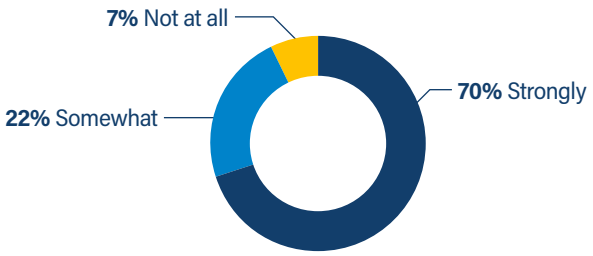
In this report, you'll learn about our survey responses and hear from Check Point and Swish experts about how federal agencies can effectively match their cybersecurity protocols against the increasing complexity of IT landscapes and cyberthreats. Check Point provides IT security products and Swish provides technology and engineering services and solutions.

*Please note that in some charts, the numbers do not add up to 100 due to rounding.*

# The Challenge of Cybersecurity

Within the government IT community, the consensus is that cybersecurity has become more challenging, a trend that is expected to continue. Survey respondents overwhelmingly agreed, with 70% saying cybersecurity will be more complex in the future than it is today (See Figure 1).

***Figure 1:** To what extent do you agree with the following statement: "In the future, cybersecurity will be more complex than it is today."*



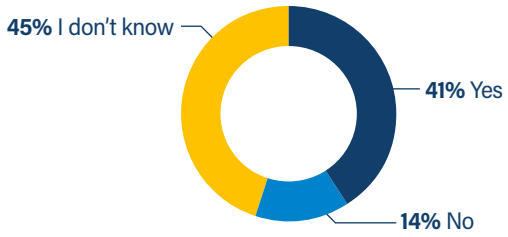

"It's becoming more complex due to the complexity of advanced technologies and the types of threats and attacks," said Glen Deskin, Check Point's Head of Engineering for the Mid-Atlantic region. "They're becoming more complex because of multi-cloud environments, multiple risks from the internet of things, mobile devices, traditional data centers and desktops. The attack surface is increasing exponentially. Data is moving everywhere…and that makes the security challenge more complex."

At the federal level, agencies are consolidating assets across data centers, which is producing more shared services, typically in a private on-premises cloud environment. In some instances, one entity could host many organizations in its cloud environment.

"Security really matters," said Sean Applegate, Chief Technology Officer (CTO) at Swish. "There's a lot more aggregation points where people are mixing different desktops and differing levels of control or security that might be using the same applications."

Agencies are adopting public cloud at an accelerated rate, with varieties such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service and Software-as-a-Service (SaaS) containing multiple levels of trust. Nearly three times as many respondents said their agency uses a multi-cloud or hybrid cloud environment (41%) as those that didn't (14%) (See Figure 2).

***Figure 2:** Does your agency use a multi-cloud or hybrid-cloud environment?*




With multiple clouds, security is more complex. During the COVID-19 pandemic, the sharp rise in teleworking has increased traffic on the internet, a low-trust environment. Organizations might have shared services in a high-trust environment on premises in a private cloud. Simultaneously, an agency might use a medium- to high-trust cloud environment through a service provider.

"The ability to control the security, whether it's in SaaS or IaaS or an on-premises cloud, is very challenging," Applegate said. "It's not just setting the regulations and the policies and checking for compliance. It's enforcing the controls in a consistent manner across those properties."

Moving to the cloud highlights several security challenges:

**Data breaches**
Security measures used to protect on-premises networks don't work as well in the cloud, if at all. Inspecting all traffic entering and leaving clouds can prevent breaches that otherwise could spread to other off-premises assets.

**Compromised accounts**
To get at cloud assets and data, hackers use many tools, including scripting, keylogging, spear phishing, brute force attacks and exploitation of weak passwords.

**Insider threats**
To adequately protect data in the cloud, security solutions must account for the behavior of potential insider threats, both purposeful and unintentional.

**Poorly secured APIs**
Application programming interfaces (APIs) are used to customize cloud services. When compromised, they can be used to manipulate cloud environments.

**Encryption**
Inadequate encryption of data in the cloud can compromise the integrity of critical information, a problem that grows as more workers use personal devices.

Agencies need a way to consolidate and consistently deploy security policies into a central business-centric engine. It should be readily applied at the right technical level across multiple environments and applications in public, private and hybrid clouds.

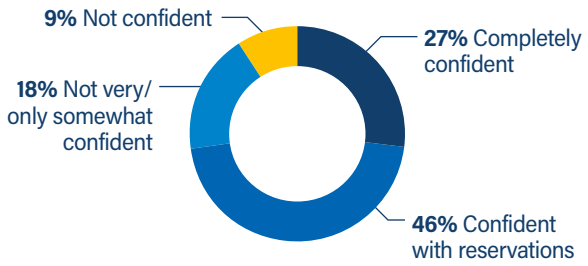
*"There's a lot of education that needs to take place to let customers know that 'shared responsibility' means you're responsible for your own data and the information you put in those cloud environments."*

**- Glen Deskin**, Head of Engineering for the Mid-Atlantic region, Check Point

# The Enemy is Everywhere

As organizations contend with new cyber vulnerabilities, uncertainty about who is responsible for protecting IT assets is impeding those efforts. In particular, the prevailing "shared responsibility" model of cloud security has caused confusion. In the survey, 73% of respondents expressed some level of confidence that sharing responsibility for security with cloud providers is "sufficiently comprehensive" (See Figure 3).

***Figure 3: How confident are you that the responsibility for security that you share with your cloud provider is sufficiently comprehensive?***



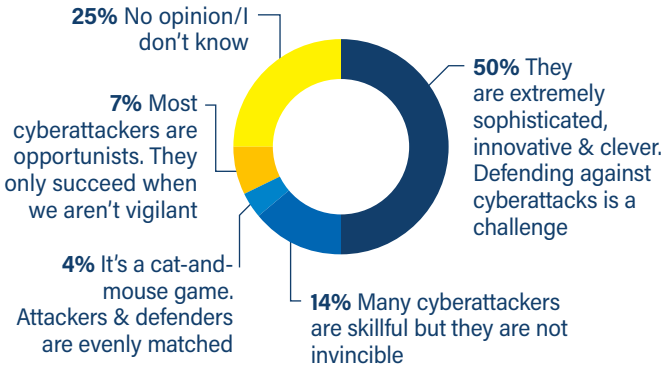

That confidence might be misplaced. What looks like sufficient security could be ignorance and vulnerability. Some users mistakenly believe that their providers are responsible for securing everything in their cloud. In reality, "shared responsibility" divides security obligations between agencies and the vendors who serve them.

"It's definitely a misconception that, 'It's in the cloud, therefore it's not in my data center,' equates to an assumption that someone else is responsible," Deskin said. "The reality is that [cloud service providers] are responsible for protecting their own infrastructure."

When those misconceptions create false security, they diminish agencies' abilities to thwart cyber attackers. "There's a lot of education that needs to take place to let customers know that 'shared responsibility' means you're responsible for your own data and the information you put in those cloud environments," Deskin said.

There is greater clarity about cyberattacks and their perpetrators. Half of survey respondents agreed that cyber adversaries "are extremely sophisticated, innovative and clever," and that defending against them is a challenge. Indeed, cyber attackers and defenders are engaged in something of a cyber arms race, with both sides trying to gain the upper hand (See Figure 4).

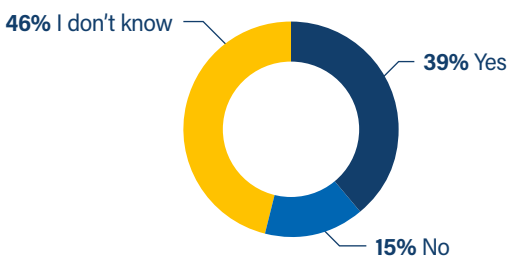
***Figure 4: Which statement best characterizes the sophistication of entities behind cybersecurity threats?***




"As the sophistication of attacks increases and our defenses get stronger, adversaries are having to lend more resources and stronger skillsets to keep up with their competitors, resulting in larger attack organizations getting involved," Deskin said.

Further motivating cyber attackers is their record of success in breaching targets. For every major breach in the federal government that makes the news, hundreds or thousands go undetected or are not publicly reported. In the survey, nearly 40% of respondents reported a security breach at their agency in the past two years, compared to 15% who said they hadn't had one. A plurality of respondents (46%) said they didn't know if their agency had experienced a breach (See Figure 5).

***Figure 5: Has your agency had a security breach within the last two years?***

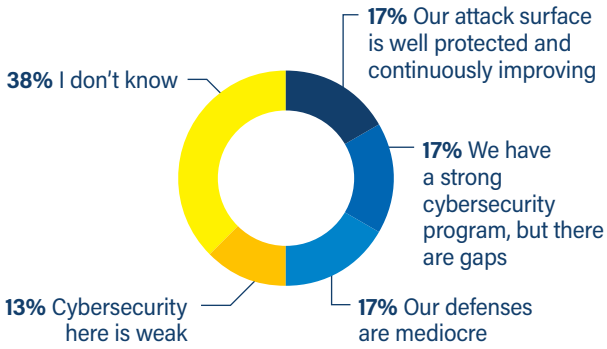



"If they are saying they don't know, that typically means they probably had an incident," Deskin said. "Government is a big target. It's No. 1."

On the question of agencies' ability to repel cybercriminals even as attack surfaces grow, there was no consensus among respondents. Matching the variety of those responses is the amount of technologies used to protect their network components. Driven by culture, procurement rules and bureaucracy, large agencies have tended toward patchwork security, putting in place separate solutions for cloud, network security, mobile, operations and endpoint security.

"If you've got an enterprise architecture, there are opportunities to consolidate some of those technologies into a more tightly integrated platform that's more policy focused, with AI across different properties and trust zones," Applegate said.

***Figure 6: The attack surface of IT systems has expanded in recent years. Which statement best describes your organizations ability to repel threats coming from all directions?***

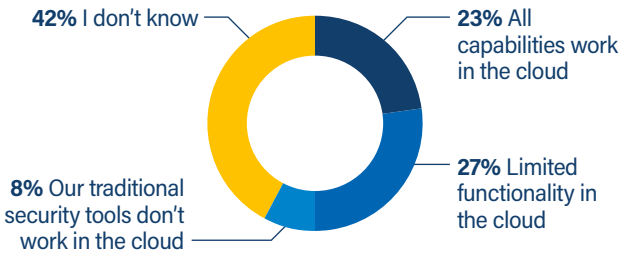



# Solving Cyber Complexity

Beneath sprawling attack surfaces are layers of complexity that further complicate efforts to repel threats and preserve network integrity. The modern data center, for example, relies on virtualization to separate workloads and pool resources that can be dynamically allocated as needed. Many organizations have adopted software-defined networking, which makes it possible to configure, manage, secure and optimize networks. Additionally, more agencies are moving to software-defined data centers, which deliver full infrastructure — networking, storage, central processing unit and security — as a service.

Those advanced technologies deliver far greater agility, flexibility and efficiency, but they also introduce new security challenges. In this environment, security must match the dynamism of applications that deploy quickly, scale to needs automatically and roam the data center for maximum efficiency.

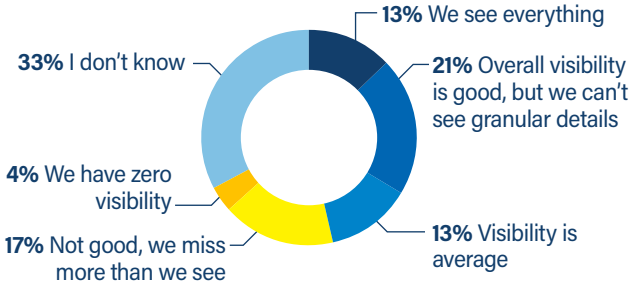
***Figure 7:** How well do your traditional security tools work in the cloud environments?*




Enforcing security policies in a virtual environment requires automation and visibility into traffic that moves laterally among data centers' virtual machines. In response to a question about the level of visibility at their organizations, about a third of respondents said visibility is good or excellent; about a third said it is average, not good or nonexistent; and a third didn't know (See Figure 8).

In multi-cloud environments that have on-premises assets, "the challenge is having a single, consolidated view of the complete environment in a single pane of glass," Deskin said. "We've got to have visibility into both the cloud and traditional networks."

***Figure 8:** Which statement best describes the level of visibility your organization has into internal system communications, network traffic and data transfer and other internal processes?*




The survey also revealed that federal IT staff have many concerns related to the new security environment. Chief among them are compromised or hijacked accounts, data breaches and external data sharing, and malware and ransomware. Their concerns are justified.

"As soon as you post data [in the cloud], automated robots know it's there, and they start hitting it within seconds, so there's not a lot of time to respond before some of the data might be compromised if you do it wrong," Applegate said.

For agencies, reverting to the status quo isn't an option because legacy security solutions are largely ineffective in the current environment. For example, traditional network segmentation was used in the past to subdivide legacy assets and limit cyberintruders who had breached perimeter defenses. Segmentation worked much like a ship's bulkheads prevented it from sinking if its hull was breached.

Manually configuring the segments is a labor-intensive process, however, and recreating them in virtualized environments compromises functionality. Agencies need a solution that segments networks by application.

***Figure 9:** What do you see as the biggest threats in a multi-cloud environment?*

| #1 | #2 | #3 |
|---|---|---|
| Compromised or hijacked accounts | Data breaches or external sharing of data | Malware/ ransomware |

# The X Factor: People

In the era of legacy computer systems, security was largely hands-on. The complexity of modern enterprises and the sophistication of cyber attackers who seek to infiltrate them require tools that use automation, AI and other advanced technologies to fend off attacks.

"We're used to doing things with people and processes that were manual, but at the 'pace of cloud,' those things break down, and so they have to shift to leveraging automation and AI in their security operations," Applegate said. "That allows them to become much more efficient and adapt in real time to changes in the cloud."

A good cloud security solution allows an organization to deploy security policies easily and consistently. That's important because many agencies have an IT skills gap at a time when their operations are increasing. Ultimately, making it easy for workers to create and deploy policies is important.

When asked to name their biggest operational headaches, respondents cited keeping up with changes to new and existing applications. Compliance issues and setting consistent policies rounded out the top three (See Figure 10).

Workers who spend the most time managing legacy systems sometimes experience more challenges dealing with security issues emerging from transformative network technology.

"As we move to cloud, people are used to those old methodologies and old technologies. Now we have serverless functions, containers and different things that are constantly changing and may live for minutes or seconds and then go away," Deskin said. "The cloud is dynamic and elastic, so how do you put security around that? In a traditional environment, you put up borders and you're done. In the cloud, there is no border."

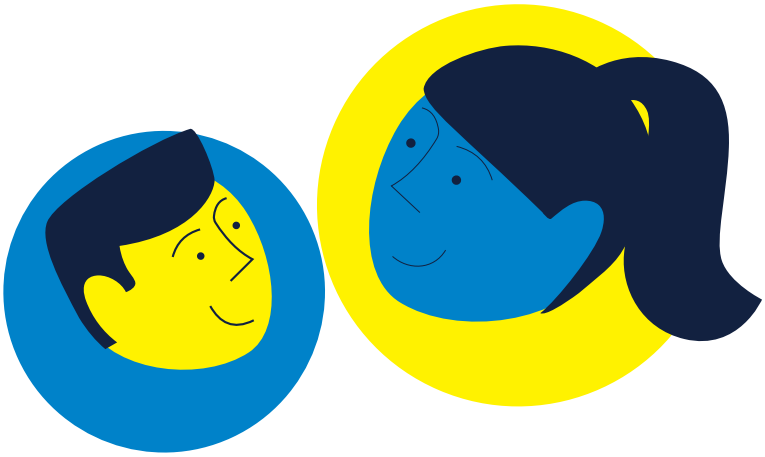
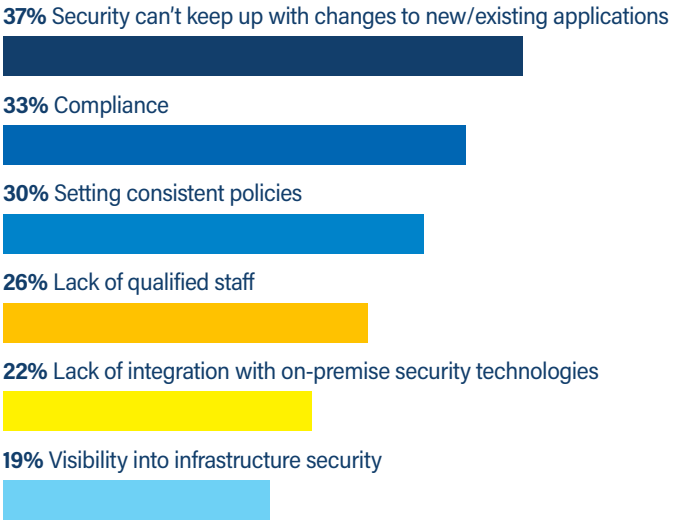
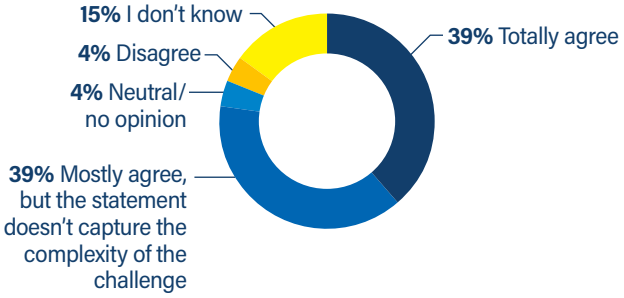


***Figure 10:** What are your biggest operational, day-to-day headaches trying to protect cloud workloads? (choose 2)*




Survey respondents overwhelmingly agreed with that view. Almost 80% said cybersecurity must be dynamic and automated to effectively thwart cyberattacks, including advanced persistent threats that attack multiple fronts simultaneously using automated scripts and AI engines to crack open an entry point.

***Figure 11:** Which of the responses best describes your reaction to the following statement: "Cloud environments have evolved to be dynamic and automated, therefore effective cybersecurity must be dynamic and automated as well."*

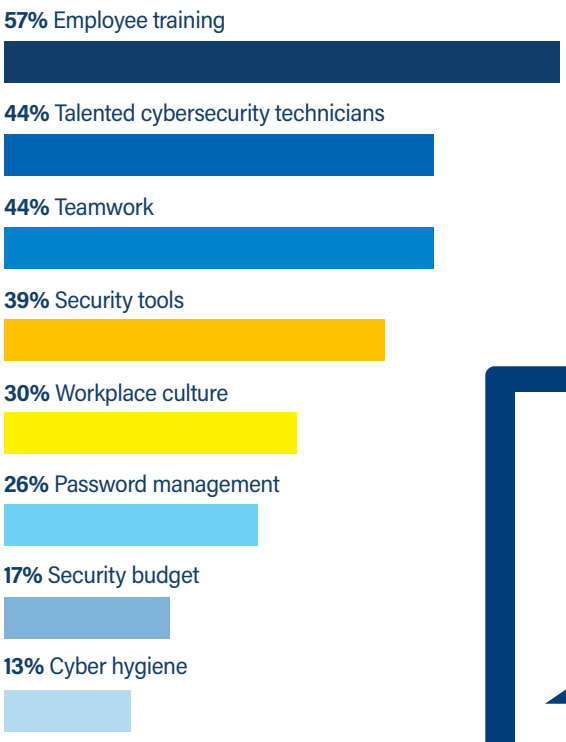


"When they get a beachhead, they go laterally across the organization. And it's not a matter of if they're going to get in, it's a matter of when," Applegate said. "AI helps us compare millions or billions of dependencies and policies automatically — something a human just can't do."

"It allows us to leverage algorithms to do what they're very good at, and it lets humans focus on the response once we find somebody that shouldn't be where they are," Applegate said.

Indeed, the survey makes clear that in the war against cyber attackers, the most effective strategies combine advanced technology and outstanding IT security teams. Asked to name the most important factor when evaluating cloud security solutions, almost 61% of respondents chose "great support and training." And asked to name the factors that most contribute to robust cybersecurity, the top three answers, in order, were employee training, talented cybersecurity technicians and teamwork (See Figure 12).

***Figure 12: Which factors most contribute to robust cybersecurity? (choose 3)***




## How Swish and Check Point Can Help

Swish and Check Point are partnered to deliver the most comprehensive cybersecurity solutions available for digitally advanced organizations in multi-cloud or hybrid cloud environments. End-to-end security architectures incorporate high-performance network devices and real-time, proactive protections for all network traffic.

Built-in flexibility and custom-fit security enforcements provide maximum protection for the modern data center. Swish and Check Point use automation, AI and other advanced tools to prevent attacks by increasingly sophisticated adversaries. An adaptive and highly responsive approach to threat vectors protects networks without compromising their flexibility, elasticity and dynamism.

For more information, visit: swishdata.com or checkpoint.com

# Conclusion

Security is the bane of IT modernization.

Take cloud computing. At many agencies, digital transformations rely on cloud. Seeking greater agility, flexibility and scalability, organizations are shifting data and applications from on-premises environments to multiple off-site platforms. Cloud-enabled IT enterprises benefit from numerous improvements, including faster provisioning of applications, improved data management, improved user experiences and more efficient operations.

But security is a challenge — more so than when legacy systems kept IT assets locked behind a defensive perimeter. In the new environment, there is no perimeter. Attack surfaces are larger, networks are more dynamic and more complex, and cyber attackers are more sophisticated. Having visibility into a system, including network traffic, is critical, but seeing operations at a granular level and in real time can be challenging, as well.

In the rush to roll out new capabilities, organizations can overlook security. They mistakenly assume that legacy security solutions will work in the new environment or that their cloud provider will handle security issues. Such oversights can prove costly. An inadequately secured system can provide virtually unlimited opportunities for invaders to move throughout a network.

With so much at stake, well-managed modern IT enterprises require the most robust security available.

## About Swish Data

Swish is a 10 year old veteran-owned solutions provider, with a focus on high-quality outcomes for our clients. Our experienced and certified engineers search out the most innovative technologies, and then develop full lifecycle solution offerings to ensure our clients realize maximum operational value. Swish ensures your digital service capabilities, performance and security exceed your mission requirements. Working together, we build long term relationships focused on value, sharing our insights and ideas to help our clients succeed.

To learn more visit swishdata.com.

## About Check Point Software Technologies

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

To learn more visit checkpoint.com.

## About GovLoop

GovLoop's mission is 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 the public sector.

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

www.govloop.com | @GovLoop

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

P (202) 407-7421 | F (202) 407-7501
www.govloop.com
@GovLoop