Adaptive Security in the Cloud

The federal government holds a massive amount of data, more and more of which is being stored on public and private clouds. Cloud has a ton of benefits – like improved operations and cost savings – but it also opens up the attack surface and makes security more complex.

Think of a federal agency like a bank. To serve more customers and grow profits, a bank opens a few branch offices. Deposits, loans, and members increase, and along with that so do their challenges. With more staff and money to manage across locations, security becomes harder and robbery becomes more likely. In the same way, as government use of cloud grows, so do their threats. So how can agencies stay secure?

To better understand the current state of cloud security at federal agencies, GovLoop partnered with Swish Data and Check Point Software Technologies to survey nearly 50 government employees.

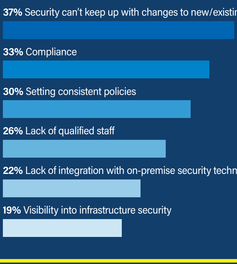
Cybersecurity – Complexity and Challenge

Growth of sprawling multi-cloud and hybrid-cloud environments continues to enlarge the attack surface that agencies must protect, much the same way that a large bank with many branches must protect more tills and vaults from bank robbers.

Does your agency use a multi-cloud or hybrid-cloud environment?

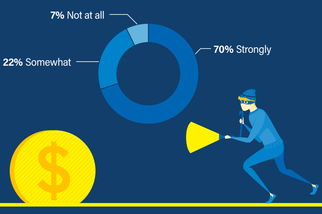
IT security is an ever-present concern, according to survey respondents.

What are your biggest operational day-to-day headaches trying to protect cloud workloads?



Cyberattackers target government agencies for the same reason that bank robbers hold up banks. That's where the money is, bank robber Willie Sutton allegedly said. For cybercriminals, "the money" is data and the control or disruption of IT operations.

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



Cybersecurity Expands Along Multiple Parameters

Trends point to escalating threats, costlier remediation and the need for more robust prevention.

60% of U.S. federal agencies reported in 2019 that they have been breached at some point

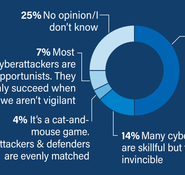
$150 million is the average projected cost of a data breach in 2020

$18.8 billion was proposed for fiscal 2021 spending on federal cybersecurity

Threats: The Enemy is Everywhere

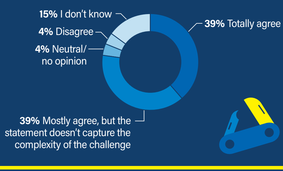
Even as agencies try to protect a larger and more complex IT environment, nation states and other adversaries seeking to breach those defenses are becoming more sophisticated. It's as if a bank had to defend against robbers armed with advanced military weapons and vehicles.

Which statement best characterizes the sophistication of entities behind cybersecurity threats?



Respondents acknowledged the importance of having the sophistication to operate in a dynamic cloud environment – and the firepower to defeat adversaries and protect assets. Bringing a knife to a gunfight is pointless.

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



Cyberattackers are using automated tools and artificial intelligence to defeat agencies' defenses. IT staff at federal agencies reported a range of security concerns related to cyberattackers' capabilities and the new security environment. Chief among them are:

Compromised or hijacked accounts

Data breaches

External data sharing

Malware and ransomware

A Need for New Insight

To meet the security challenge, agencies must

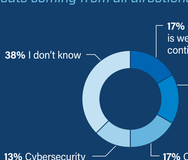
- **Adapt to new environments and adversaries**
- **Prevent security breaches**
- **Increase visibility into internal system communications**
- **Prepare to stop the lateral spread of intrusions**

Enforcing security policies in a virtual environment requires automation and visibility into traffic that moves between data centers' virtual machines.

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

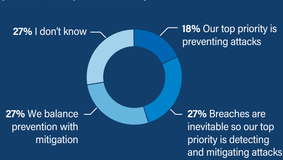
Trying to protect IT assets without visibility is like trying to foil a bank robbery while blindfolded.

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?



In the war against cyber attackers, effective strategies combine advanced technology and outstanding IT security teams, yet agencies at times struggle to allocate limited resources.

Which statement best describes your agency's approach to cybersecurity?



How Swish and Check Point Can Help

When it comes to the security of precious metals, Fort Knox is the gold standard. In the world of cybersecurity, Swish and Check Point deliver the most comprehensive security 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 and networks without compromising flexibility, elasticity and dynamism.

For more information: checkpoint.com and swishdata.com.

Check Point SOFTWARE TECHNOLOGIES LTD | Swish | govloop