3 ways to strengthen SECURITY *seamlessly with* CLOUD

statescoop

Microsoft Azure Government

With a focus on organizational accountability, identity and device security, state and local governments are turning to cloud to streamline and strengthen their cybersecurity efforts.

By StateScoop Staff

There has been a pivotal shift over the last half-decade in how state and local government are approaching cloud computing.

In fact, it's more than just a shift — it's a complete reversal of course, Stuart McKee, Microsoft's State & Local Government CTO, says.

“Roughly five years ago, no one was moving to the cloud because they were worried about security and compliance,” McKee says. “Today, it's completely the opposite.”

Government agencies, the CTO says, are inspired to move to cloud because of the investment that private sector cloud providers have made in building security and compliance structures into their products.

In California, Chris Cruz — the state's deputy chief information officer — said some of the cybersecurity components included in government clouds were “very significant” in protecting the state's networks.

“We have the highest level of security, standards and postures in place now that align with federal standards and recommendations,” Cruz said on a state general assembly hearing on cybersecurity oversight. “[That helps us] in protecting and procuring the state's most mission critical data.”

On the vendor side, it's important for cloud providers to not only adhere to compliance structures, but to exceed them.

“You can fundamentally measure that in a compliance framework,” McKee says. “You can measure it against compliance standards, and you can also, to a lesser extent, measure that against security outcomes and commitments.”

It's that key phrase of “commitments that McKee says goes furthest. Government and the vendors who support it have a tendency to treat things like compliance as a checkbox and not as a commitment. For government agencies with troves of sensitive data, compliance needs to be more than just checking a box — instead, compliance must be a stepping stone to an even deeper conversation about security.

That deeper conversation can help avoid a large percentage of cyberattacks, McKee says. In fact, according to a 2016-2017 Gemalto study, more than 70 percent of breaches on public sector agencies came from malicious outsiders. Those attacks predominantly come from phishing and other email-borne attacks. And the numbers reported in the study — and studies like that across the globe — don't include unreported attacks, McKee says. “Unfortunately, reported attacks are just the tip of the iceberg. There are a lot more cyberattacks that are not reported than are reported.”

Through a mix of organizational accountability, a focus on identity and an increased focus on the security of physical devices, McKee says, state and local government agencies can protect themselves from a large number of these attacks. The security and compliance wrapped within a cloud infrastructure make that even more seamless.

Organizational accountability

In some cases, the very structure of how government makes decisions and spends money can be its own harbinger of difficulty when it comes to security.
According to a 2016 report from the National Association of State Chief Information Officers and Deloitte, cybersecurity is increasingly becoming a part of the fabric of government operations; however, 45 percent of survey respondents said a lack of documented processes make it hard for them to operate at full capacity.

"It's a real struggle," McKee says. "There are lots of complex questions an agency must stop and consider. For example, does leadership prepare for an attack? Do they have the ability to figuratively cut the wires if necessary during an attack? Do they have an organizational structure in place that can effectively respond and deal with it?"

If done properly, streamlining that structure isn't an expensive or difficult process to do, McKee says. Through a cloud provider that has built-in security and compliance included, state and local government agencies have access to the configurations to enable accountability across the organization.

"We're not talking about a huge outlay of capital," McKee says. "We're not talking about deviating major resources. Establishing this vital structure requires a small, but critical investment well within state and local government decision makers control."

In Texas, Todd Kimbriel, the state's chief information officer, says the state's long-term embrace of cloud has helped meet his team meet and exceed compliance goals, especially with a focus on regulated data.

"We've been leveraging cloud for quite a few years now, we had very early adoption and most of our agencies have adopted some measure of cloud services," Kimbriel says. "We've done due diligence on the govcloud environments for our selected providers and we're very happy with the security they've provided us."

The structure present in cloud has allowed Kimbriel and the team to make streamlined security and data management decisions and have the flexibility to move around sensitive data across multiple environments.

"[The] providers in the cloud space do have a strong sense of security," Kimbriel says.

Identity

"Identity is the new firewall," McKee says. "We still need to secure our facilities — large door locks still matter, but the key thing is the bad guys are not entering through the front door or the backdoor. They're not showing up physically at our locations. They're attacking us virtually."

State and local agencies need to start thinking about protecting data — and to do that, they need to consider identity. It starts with knowing who and what is on the network and how they are behaving. The analysis of these behavioral trends gives security leaders a window into what may look like normal behavior but could actually be a bad actor performing an abnormal function.

With a secure and compliant cloud, agencies can unlock “a vast amount of capabilities and features that are really important,” McKee says, like advanced threat analytics, an intelligent security graph and more.

“We’re actually able to monitor active threats happening in the moment, predict potential threats, and develop a feedback loop that increases the accuracy of our intelligence continuously. We share this intel with our customers on a real-time basis,” McKee says.

Device security

If identity is the new firewall, then devices are the new perimeter, McKee says.

While knowing who and what is on the network is important and essential for threat monitoring and analytics, good device security — from mobile devices and Internet of Things technology to computers — can help prevent bad actors from even making it to the network in the first place.

“The physical devices and things that we either have in our hand, or the laptops that we carry, or the computers installed in cop cars, or the scanners that are in water district workers’ hands, or the traffic cameras that are deployed on street lights,” McKee says. “The physical devices are the new perimeter, and we can’t be lackadaisical about understanding that any access point on our network is a potential attack vector.”

With the security and compliance capabilities on the cloud, agencies can have a deeper look at the identity present on their devices. Most cloud-based enterprise mobility suites also allow organizations to manage devices and physical objects regardless of the platform they are based on.

By tightening the security on individual devices, agencies can cut down on attackers’ ability to get access to a device that would give them access to the network. In some ways, device security can be the first line of defense, before identity and other security protocols have to attempt to stop an attacker in their tracks.

A stronger security stance

With focuses on organizational accountability, identity and individual device security, state and local government agencies will be more poised to take on bigger cybersecurity challenges as the large percentage of external threats are filtered out. This stronger and more focused approach helps in an ever-growing cybersecurity threat environment.

“Historically, you’d see an attack, and it’d spread and then people would create mitigation capabilities, address it, stop the flow and then go back and fix it and clean up systems that were infected,” McKee says. “Today, we’re seeing the idea of polymorphic viruses. Viruses that are actually changing almost real-time.”

With cloud, agencies can take advantage of “an almost unlimited amount” of computer power to take those changing threats on and protect their government agencies.

“Not all clouds are created equal,” McKee says. “What makes our cloud invaluable and unique is its hyperscale capability, it’s this idea of massive compute, massive storage, at your fingertips. The good news is our customers can take advantage of that.”

To learn more about Microsoft Azure Government, visit azure.com/gov.

This article was produced by Scoop News Group, for and sponsored by Microsoft, and distributed via StateScoop.com

statescoop Microsoft Azure Government