SMARTER SECURITY FOR A BETTER PROTECTED GOVERNMENT

IT decision-makers are faced with tough funding choices. Between operations, modernization, security and other programs, there's never enough money to do it all. Unfortunately, data security is often one of the least funded elements of state and local governments, allowing sophisticated hackers and cybercriminals to accelerate their aim at government networks. According to a 2019 report from the U.S. Conference of Mayors, there have been more than 170 recorded ransomware attacks against state and local government entities since the malware first appeared in 2013.

Data security threats are a serious concern for any organization, but the risks are potentially greater for government agencies because their systems often store personal information such as Social Security numbers; birth certificates; and driver's license, bank account and credit card numbers for millions of people and businesses. Meanwhile, many government agencies still rely primarily on perimeter-based security controls such as firewalls, intrusion detection systems, antivirus software, etc. — tools that are no longer adequate in today's heightened threat environment.

Government organizations are often understaffed and working to maintain antiquated systems. Those that don't modernize their IT systems will continue to be highly vulnerable targets. To strengthen their security posture, government IT leaders must focus on automating security practices using modern capabilities such as next-generation cloud solutions with autonomous capabilities.

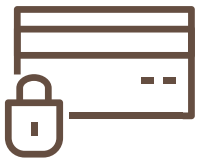
Enter Next-Gen Cloud

A few years ago, concerns about data security and privacy prevented some government organizations from adopting cloud-based business models. But cloud has matured. The next-generation cloud infrastructure available today is built around multiple layers of security and defense. These advances allow organizations to bake in better security than they can obtain in their own data centers.

"Next-generation cloud enhancements enable users to strengthen all aspects of security and build a stronger, more resilient overarching infrastructure," says Jerry Niemeyer, director, Product Management, Oracle Public Sector, who heads a team supporting Oracle's next-generation cloud infrastructure: Oracle Cloud Infrastructure, Generation 2. "Today, governments that migrate to cloud have an opportunity to improve their overall security posture at the same time."

Next-generation cloud includes layered controls that provide exceptional resiliency, so if a vulnerability is discovered and exploited in one layer, the unauthorized user will be confronted with another security control in the next layer. In addition, the highest security bar is set by default. For example, cloud administrators must explicitly grant access to each aspect of their network rather than starting with a default open network and restricting access as needed. These types of security refinements go a long way toward hardening the broader infrastructure, but most importantly, next-gen cloud also enables organizations to employ advanced technologies such as AI-based applications, machine learning-integrated security, automated analytics and autonomous capabilities.

GIVEN TODAY'S GROWING THREAT ENVIRONMENT, STATE AND LOCAL GOVERNMENT AGENCIES MUST FOCUS ON HARDENING THE INFRASTRUCTURE RATHER THAN JUST SECURING THE PERIMETER.



Autonomous capabilities are critical when it comes to helping government agencies strengthen security. An autonomous database uses machine learning to automate database tuning,

security, backups, updates and other routine management tasks traditionally performed by administrators. Unlike a conventional database, an autonomous database performs all these tasks and more without human intervention.

"The ability to address threats in near real-time is something government has always struggled with," says Niemeyer. "But the speed of the threats we see today makes it impossible for humans to keep up. There are not enough security personnel, skills and training that can mitigate these emerging vulnerabilities. This is not something government can hire its way out of. If they're going to invest, autonomous is the answer."

Artificial intelligence is the key to end-to-end automation. For example, failing to apply a patch or security update can create vulnerabilities. Failing to apply a patch correctly can weaken or eliminate security protections altogether. The autonomous database handles patching automatically, acting as a security force multiplier and freeing IT personnel to focus on value-added tasks. This is critical as government faces an ongoing IT labor shortage and limited IT security budgets.

"Do you want to spend your time patching a server, an application or an operating system? Do you want to spend a lot of time learning how to implement new features, or do you just want to use them?" asks Niemeyer. "Autonomous services take care of all that automatically, enabling your team to focus on things like delivering new services to citizens and employees while ensuring a high level of security at the same time."

These same capabilities help agencies enhance disaster recovery capabilities, providing them protection from unplanned disruptions, both physical and virtual. An effective disaster recovery plan can be costly due to the need to establish, equip and manage a remote data center. Next-gen cloud and autonomous capabilities provide an alternative for agencies that do not have a disaster recovery site or who prefer not to deal with the cost or complexity of managing a remote data center.

Building on a Secure Foundation

Given today's growing threat environment, state and local government agencies must focus on hardening the infrastructure rather than just securing the perimeter. Doing so effectively means leveraging the benefits of next-generation cloud, including the automation it enables to improve security, reliability and operational efficiency.

Once an agency's infrastructure is strengthened, it's time to start looking at how to get value out of data. We'll examine that topic next.

ENHANCING SECURITY WITH ORACLE'S GENERATION 2 CLOUD INFRASTRUCTURE

Oracle's Generation 2 cloud infrastructure represents a fundamental re-architecture of the conventional public cloud. Security is baked in from core to edge to set agencies up for cybersecurity success. Oracle Cloud is the only cloud built to run Oracle's Autonomous Database, the industry s first self-driving database.

Users of Oracle Cloud get unparalleled control of and transparency into their cloud-based applications, including:

Customer isolation that allows you to deploy your application and data assets in an environment that is fully isolated from other tenants and Oracle's staff. This also enables internal segmentation of access to ensure only authorized individuals and processes have access to sensitive data.

Always-on encryption that protects customer data at-rest and HTTPS-only public Application Programming Interfaces (APIs).

Easy-to-use security policies that allow you to constrain access to your services and segregate operational responsibilities to reduce risks associated with malicious and accidental user actions.

Comprehensive log data that allows you to audit and monitor actions on your resources, helping you to meet your audit requirements while reducing security and operational risk.

Identity federation that allows you to use your existing user and group definitions in the cloud.

Support for third-party software solutions to further protect customer data and resources in the cloud.

Separate fault domains that enable high-availability scale-out architectures that are resilient against network attacks, ensuring constant uptime in the face of disasters and attempted breaches.

Rigorous internal processes and use of effective security controls in all phases of cloud service development, operation and maintenance.

Adherence to strict security standards through third-party audits, certifications and attestations. Oracle helps customers demonstrate compliance readiness to internal security and compliance teams, their customers, auditors and regulators.

For more information on Oracle next-gen cloud solutions, visit **oracle.com/stateandlocal**

ORACLE