BUILDING SECURITY-AS-A-SERVICE MODELS AT THE STATE GOVERNMENT LEVEL

SECURING YOUR STATE'S DIGITAL TRANSFORMATION

Like many enterprises, state governments are attempting to drive digital transformation to reduce costs, improve operational efficiency, and drive innovation opportunities. A recent report from Deloitte asked the question, "What if government services worked like cloud services?" Yet, at the same time, the report revealed that many state government officials believe that their digital capabilities lag behind the private sector.[1]

Nonetheless, state governments are slowly but surely moving to the cloud: 28% already have a cloud migration strategy in place, and 55% have one under development.[2] Cloud now ranks as the number-two priority of state IT leaders, surpassed only by security.[3]

Digital transformation efforts can pay big dividends for states, but as data moves between agency silos, decentralized networks, legacy applications, mobile apps, and multiple clouds, attack surfaces grow far beyond agency walls, rendering traditional peripheral security insufficient.

As state governments consolidate IT services with cloud solutions, an opportunity is emerging to deliver Security-as-a-Service (SECaaS) to agencies and departments. However, to maintain transparency and control, a comprehensive and unified approach to security is essential. In a recent survey by the Center for Digital Government, those states that received an "A" grade for their digital transformations also had a strong focus on cybersecurity.[4]

#1: Security
#2: Cloud Services
top priorities of state IT leaders

83% of states have a cloud migration strategy in place or under development.

56% of public-sector organizations use cloud-enabled cybersecurity solutions.

WHITE PAPER

SECURITY AS AN ENABLER FOR CHANGE

Because state governments and their agencies store a massive amount of data about citizens—often more than the federal government—their networks and databases are attractive targets for cyber criminals. For years, states have reported a far higher rate of cybersecurity incidents than the private sector, and 56% of public sector organizations now use cloud-enabled cybersecurity for services such as real-time monitoring and analytics, threat intelligence, advanced authentication, and identity and access management.[5]

Compliance is a growing factor as well, ever changing and always increasing in scope. At least 19 states now have specific statutory requirements around data security policies and measures for state government agencies to follow.[6]

To make matters even more complex, the Internet of Things (IoT) is here to stay and gaining momentum, bringing new security requirements with it: 43% of state CIOs feel that IoT will be the most impactful emerging IT area in the next three to five years.[7] In the not-too-distant future, all states will be connected by sensors and devices in hospitals, traffic intersections, and government offices—all of which will need to be secured.

But fear not—change is bringing tremendous opportunities. Security should be an enabler, not an inhibitor, helping state governments drive change by allowing them to move to cloud or use cloud services and IoT devices securely. A centralized, automated approach to security also helps to address the shortage of cybersecurity skills, which are always in high demand in state government.[8] But states won't succeed with their digital transformations unless they think differently about security and integrate it from the ground up.

Applying layers of security as an afterthought is a sure way to fail. Disparate point products increase complexity and reduce visibility, making your organization less efficient and security less effective. Security layers must be thoughtfully architected to include advanced threat protection across the entire attack surface.

> *"The CISO's role has moved from being viewed as the barrier to being the enabler. We must enable the mission, reduce organizational risk, protect reputation, and reduce cost."*
>
> *— Agnes Kirk, CISO, State of Washington*

SERVING MANY STAKEHOLDERS

State governments must serve a broad swath of agencies and constituents—some with strict compliance and security requirements. From the attorney general's office to corrections to education, all state agencies have significant and diverse technology requirements. In a recent survey cited by Deloitte,[9] state IT personnel and decision-makers identified the most critical areas needing better digital capabilities that are ripe for transformation:

Health and human services. States spend more on healthcare than anything else except for elementary and secondary education.[10] State hospitals can greatly improve efficiency and effectiveness using mobility solutions and IoT-enabled devices. However, with personal information and lives at stake, security has never been more important.[11]

Motor vehicle offices. With improved digital capabilities, departments of motor vehicles (DMVs) can provide better, faster service. But as providers of state IDs and stewards of millions of Social Security numbers, DMVs are prime targets for cyber fraud and data theft.

Employment services. Using cloud integration and mobile apps to bring data together from disparate sources and match jobs to job seekers, states can reduce unemployment and save taxpayer money. But even as states offer more flexible employment services, cyber fraud is on the rise: "Advances in technology have made it easier for multi-claimant scams to financially impact state agencies. The proliferation of organized crime efforts takes advantage of specific state vulnerabilities using stolen personal claimant identification and the anonymity of the Internet."[12]

Public safety. For police and fire agencies, timely and detailed information equals faster and more effective responses. Whether accessing real-time information about a crime scene on mobile devices or analyzing signals from IoT devices to determine the characteristics of a fire, public safety agencies need to be sure the information is secure. Additionally, state law enforcement agencies must be empowered to enforce cybersecurity laws where they apply.

All of these agencies can benefit from a SECaaS model to reduce costs and improve management efficiency. For example, the state of Washington offers state agencies a set of common security services that includes perimeter security, logging and monitoring, forward proxy services, a secure single sign-on portal to state applications, and vulnerability management, covering the cost through an internal transfer process.[13]

FOLLOWING FEDERAL FRAMEWORKS

Although state laws around data retention and security vary, many states are adopting a federal cybersecurity framework and model for information exchange to achieve a higher level of maturity in securing their digital transformations. Recognizing that the U.S. government is leading the way, states are seeking to comply with the same regulations to increase their security resilience:

U.S. National Institute of Standards and Technology (NIST). In 2013, President Obama issued Executive Order (EO) 13636 on Improving Critical Infrastructure Cybersecurity and directed NIST to develop a cybersecurity framework. When NIST released the framework a year later, it invited state and local CIOs and CISOs to learn about the framework and prioritize their cybersecurity efforts. Since then, Virginia, Nebraska, and other states have adopted the NIST framework, which encourages the sharing of threat information to enhance security. The 800 series of publications by NIST provide helpful definitions for security controls that states can easily leverage.

The Brookings Institution recommends that states "closely examine and adopt standards, policies, and procedures enacted by nationally respected groups like NIST in order to jump start their cybersecurity planning."[14]

National Information Exchange Model (NIEM). A common vocabulary that enables efficient information exchange across public and private organizations, NIEM can save states time and money by providing consistent, reusable data terms and definitions, as well as repeatable processes that can be used across borders.

National Governors Association (NGA) Resource Center for State Cybersecurity. The NGA provides valuable resources as well as a "Governor's Guide to Cybersecurity" to help states confront the growing cybersecurity challenge.

HOW STATES CAN IMPROVE SECURITY TODAY

At present, most state security solutions are spread out across agency silos and not unified. Application modernization and cloud adoption require a different security model—one that can easily be offered and consumed as a centralized service. To achieve this objective, states need a unified security fabric that satisfies the following requirements:

Integration. Lack of integration leads to manual processes, taking staff time away from important strategic initiatives. Instead of deploying multiple, disconnected point products, look for security solutions that complement each other and share data to detect advanced threats.

Performance. Securing applications and data across an expanded attack surface should not come with any degradation in performance. Beware of security solutions that present multiple "choke points" that slow network traffic.

Scalability. A digital transformation is an ongoing process, and security solutions must scale and adapt in order to be useful and cost-effective in the long run. Look for solutions that can scale to provide the security services each state needs five years from now.

Flexibility. As previously mentioned, security solutions should enable, and not inhibit, the application modernization process. As states' digital transformations evolve and new cloud services are deployed and more IoT devices are added, securing the entire information chain—from IoT to cloud—will be essential. The ability to integrate with third-party solutions to create a connected ecosystem is also critical.

Visibility. To enable centralized, automated, and effective policy controls, states need visibility into their entire security infrastructure. Security information and event management (SIEM) tools are needed to prioritize threats, and these should be utilizing artifical intelligence and automated threat-prevention protocols.

> ***"Data management and analytics, cloud solutions, and security are demanding our attention. Unification of services will drive the need to improve data management discipline, enterprise governance, and optimization."[15]***
>
> ***— Bo Reese, CIO, State of Oklahoma***

HOW STATES CAN MOVE TO A SECAAS MODEL

For most states, the transition to delivering SECaaS will be a gradual one. Both from a fiscal and a practical perspective, it makes sense to lay the foundation for SECaaS with a core security capability and build on that to deliver all of the capabilities mentioned above. The maturity models presented below offer a general guide to developing an increasingly robust state SECaaS:

MODEL 1: NOC-BASED ON-PREMISES SERVICES

The core SECaaS capability focuses on threat prevention, using agency-sited or cloud-based next-generation firewalls (NGFWs) that are managed and monitored around the clock from a multi-tenant network operations center (NOC). Because the NGFW serves as the core of the SECaaS operations, it is important to choose an advanced and well-supported technology with a range of form factors to suit the variety of clients the SECaaS provider will serve.

MODEL 2: ADVANCED SERVICES WITH A SECURITY FABRIC

After NGFWs, the next most critical capabilies are web application security—namely, protection from attacks to web applications from known and unknown exploits—and sandboxing. Unprotected web applications are the easiest point of entry for hackers, and they are vulnerable to a number of different types of attacks.

With sandboxing, the SECaaS provider begins to expand its competence from threat prevention to advanced threat protection, which includes threat detection and rapid mitigation. With today's threats rapidly evolving to evade traditional defenses, sandboxing is a critical component of network security. Sandboxing quarantines suspicious programs or code before it can cause damage and tests them in a safe environment to determine whether they are dangerous.

Typically, web application firewalling and sandboxing are delivered through additional customer premises equipment (CPE). However, some advanced NGFWs include web application firewall and sandboxing support; it's simply a matter of remotely turning on these security functions in the CPE when the SECaaS provider—whether the state or a third-party managed security services provider (MSSP)—is ready to manage them. This requires less capital expenditure and provides easier adminsistration.

A more forward-looking approach would be to deploy web application security and sandboxing capabilities as centrally managed services in the NOC. This approach would allow providers to deploy more streamlined devices on the client premises (or none at all—see Model 3) while reducing the administrative burden in the NOC.

State security operations centers (SOCs), both those run by the state and those delivered through an MSSP, can improve their efficiency and efficacy by adding more advanced management, analytics, and SIEM tools. These enable states, including individual agencies, to gain greater visibility into the operation and effectiveness of the CPE or cloud-based firewalls.

MODEL 3: ON-DEMAND, INTEGRATED SERVICES

The premise of SECaaS is to deliver greater cost and operational efficiencies than if the security services were delivered by individual agencies and departments themselves. But it's a challenge due to a security skills shortage and constant budget pressures. At this stage in their development, SECaaS providers should focus on improving their operational agility through technological approaches such as software-defined networking (SDN) and network functions virtualization (NFV).

Rather than deploying physical CPE at client sites, providers can provision virtual CPE through the cloud. Virtualization abstracts the administrative functions from the security functions, enabling security services to be provisioned quickly from any location—a boon for providers in larger states. To more rapidly scale their services, providers should work toward automated security provisioning, based on threat activity and continuous intelligence feeds. Staff can then be better allocated to monitoring the provisioning and making strategic and critical decisions. Some SECaaS providers may also want to allow clients to self-provision security functions on demand.

The guidelines above should be taken as a rough outline of possible progress. Each state and each SECaaS provider will find the optimal path for delivering services that provide a secure path to digital transformation for all constituents.

[1] William D. Eggers and Steve Hurst, "Delivering the digital state," Deloitte Center for Government Insights, 2017.

[2] "Technology Forecast 2018: What State and Local Government Technology Officials Can Expect," National Association of State Chief Information Officers (NASCIO), Accessed on Feb. 26, 2018.

[3] "State CIO Priorities for 2018 - State Technology Leaders make Security and Cloud Services Top Priorities," National Association of State Chief Information Officers (NASCIO), Accessed on Feb. 26, 2018.

[4] "How Digital is Your State?" Government Technology, Sept. 2016.

[5] "Public Sector Remains a High Target for Cyber Attacks highlights Bitdefender researchers," The DQ Week, Sept. 25, 2016.

[6] "Data Security Laws - State Government," National Conference of State Legislatures, Jan. 2017.

[7] Jon Oltsik, "Research suggests cybersecurity skills shortage is getting worse," CSO from IDG, Jan. 11, 2018.

[8] "Essential digital services survey," Center for Digital Government, Feb. 2017.

[9] "State Health Care Spending," The Pew Charitable Trusts and the John D. and Catherine T. MacArthur Foundation, May 2016.

[10] "A Security Fabric for Digital-Age Healthcare," Fortinet, Dec. 11, 2017.

[11] "Schemes to Swindle State Unemployment Agencies on the Rise," First Nonprofit Group, An AmTrust Financial Company, Accessed on Feb. 26, 2018.

[12] David Raths, "States and Localities Consider Security as a Service," Government Technology, Aug. 31, 2015.

[13] Gregory Dawson and Kevin C. Desouza, "How state governments are addressing cybersecurity," Brookings Institution, March 5, 2015.

[14] "State CIO Priorities for 2018 - State Technology Leaders make Security and Cloud Services Top Priorities," National Association of State Chief Information Officers (NASCIO), Accessed on Feb. 26, 2018.

[15] Dan Lohrmann, "State Chief Security Officers Share Current Plans," Government Technology, Jan. 28, 2017.

FORTINET

www.fortinet.com