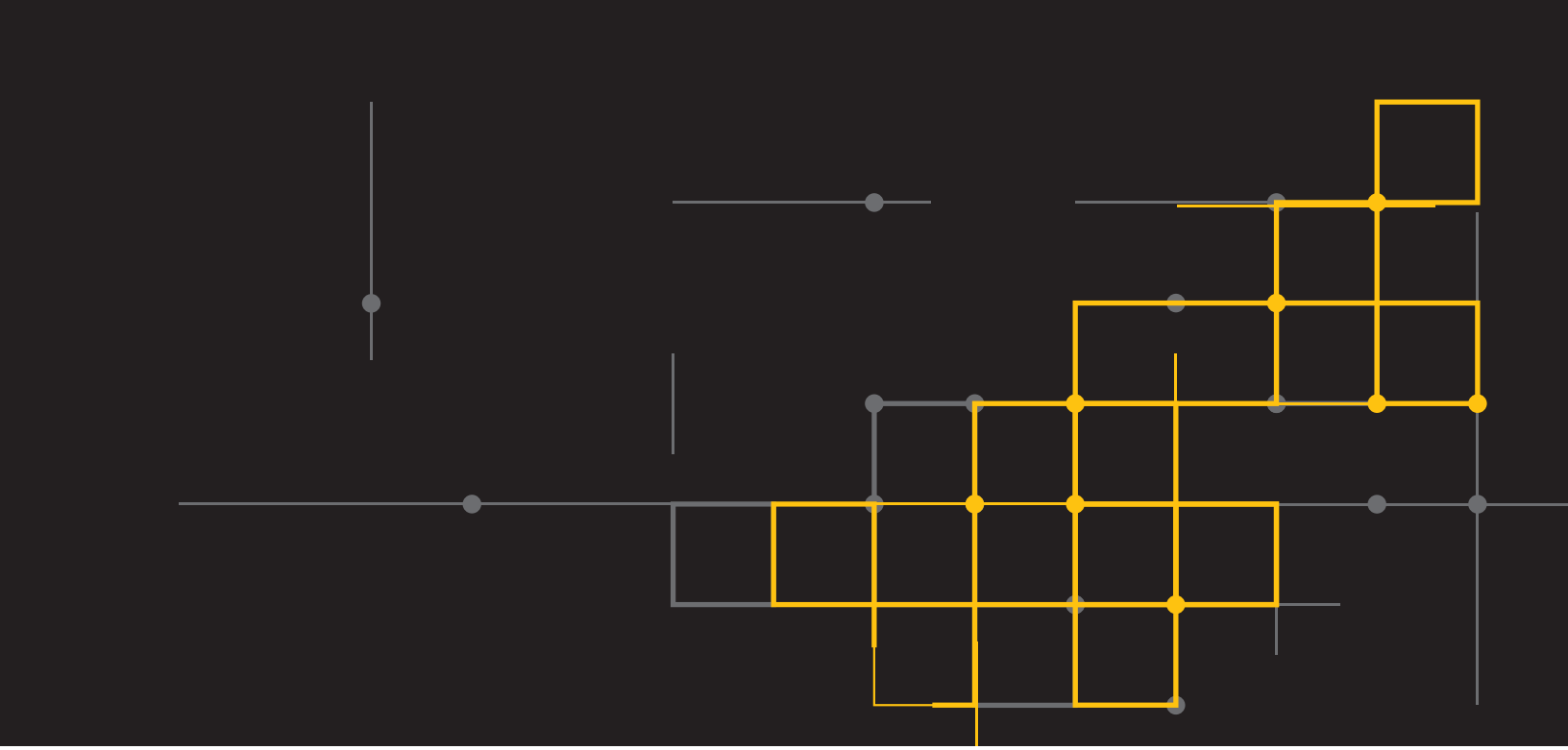

# State and Local Government: Security for the Cloud Generation

White Paper | April 2017

Symantec

## End-to-end solutions allow agencies to take advantage of the cloud with confidence

There are more than 89,000 local governments spread across the United States and each one is in a different place in their cloud computing journey, if they have started at all. Along with the 50 state governments, these entities face perhaps the most difficult public sector security challenge in the nation: Keep citizen and government information secure with less money, less staff and less resources than their counterparts in the federal government or the private sector.

State and local governments, by and large, have just begun leveraging cloud computing solutions. However, using cloud-based email and productivity systems like Office 365, agencies are getting a first-hand look at the cost, efficiency and ease-of-use that the cloud provides.

As more and more of these agencies begin to use or expand their use of the cloud, security will remain a top priority – for all the benefits cloud provides, it quickly loses its value if it is not secured properly. The good news for state and local governments is that the security posture of today's cloud environments is better than ever, as organizations can purchase end-to-end solutions that keep data safe no matter where it is in its lifecycle.

## The Cloud Generation

Today, state and local employees use multiple devices and connect to many applications through a variety of networks. It is impossible to secure this ecosystem with the methods of the past. As this generation of workers has come to learn how to take advantage of the convenience and ubiquity of the cloud for increased efficiency, productivity and accessibility, they often do so with little regard for security.

Additionally, state and local employees already use the cloud, both in authorized and unauthorized ways. While the government itself might offer select services via the cloud, employees are using the cloud applications they use outside of work on the job. This is also true for state and local governments that have not fully embraced cloud computing. While the agency itself may not sanction cloud capabilities, employees are regularly using the cloud at will. It is no longer about technology leaders choosing cloud computing – the cloud has ultimately chosen them. State and local technology leaders must rethink their cloud security strategies.

So what are governments to do? With employees forcing them toward the cloud, state and local governments need solutions to stay protected. While there might be fear about this transition, state and local technology leaders can rest easy. With recent advances in integrated security solutions, cloud security no longer has to be about fitting different pieces of the security puzzle together. Instead, agencies can take advantage of security technologies built to protect the cloud generation that enable the users to be productive, while the information remains protected.

## The Challenges of Securing the Cloud

The benefits of cloud computing are well-known. Agencies do not have to make large capital investments in infrastructure, but can still get the same, or enhanced, versions of the applications they previously hosted. This can all be done at a lower cost, allowing customers to either save or reinvest that money in other mission-oriented activities.

Employees can access applications from everywhere, providing them with the same productivity tools they have access to in the office while on the go. This all makes for a more efficient work environment and a more cost-effective one for agencies, but securing the cloud poses more unique challenges than before, including:

- **Explosion of new endpoints.** More connected devices—from desktops, laptops, tablets and smartphones to smartwatches, connected eyewear and the Internet of Things—makes securing people and data through just the endpoint no longer realistic.
- **Evolving traffic and connectivity.** Encrypted traffic via SSL now represents between 50 and 70 percent of data flows, creating blind spots for traditional security products. As users

access information through Wi-Fi or 4G and bypass fixed networks, large amounts of data can be accessed at blazing speeds without administrators having proper visibility.

- **Application blending.** Agencies no longer just have applications on on-premises solutions, but a mix of on-premises and cloud applications. As agencies adopt products like Google Drive, Office 365, Salesforce and Slack, they will need a new security model built to handle both types of application delivery.

These challenges are common in an environment where agency leaders know what cloud applications their employees use, but the reality is that employees often use cloud applications their agencies are unaware of, resulting in a sprawl of shadow IT. It is not uncommon for a technology leader to believe their employees use only a few dozen cloud applications only to learn later that number is a few hundred. As computing changes, both from technology to habits, so must the security strategies and techniques to support that change.

State and local governments are at an increased challenge as it can be more difficult for these agencies to provide enough resources to effectively impact cybersecurity. With enhanced solutions, new security products can make it easier for state and local governments to secure data without a large investment. A solid cloud computing framework has been shown to reduce the costs governments face in cybersecurity as they avoid the hefty prices that come with cleaning up a major breach – the average cost of a data breach in the U.S. in 2016 was more than $7 million. Take into consideration that nearly 50 million records of Californians have been breached between 2012-2015, with the majority of these breaches resulting from security failures (according to the California Data Breach Report) and agencies can see huge implications and liabilities that result from a breach.

## The Path Forward

For state and local government, the long answer to cloud security has focused on patching together a range of security products to oversee each part of the process. This resulted in agencies picking individual purpose-built solutions that were not intended or developed to work with one another, which created a patchwork, and often incomplete, security infrastructure.

While this process made sense at the time, the proven approach for cloud security is now to use a unified, network-based platform with a flexible security architecture that can manage the ever-changing cloud environment – from the endpoint through the data transmission pipe to the cloud and back. This comprehensive approach of integrating solutions together to protect data through the entire process was simply not available…until now. Agencies can now unify access governance, information security and threat protection across cloud platforms and on-premises security infrastructures – offering the same level of protection that agencies are used to in their own physical networks.

An integrated, end-to-end cloud security environment can be structured like the following:

- **Apply policy universally.** The first step of an effective cloud security program is to establish the policies that will govern the agency's people and processes. This includes ensuring the proper people have access to only the data they need. By better managing the users and identities that have access to specific data, agencies can improve the risk vectors that threaten their data and strengthen their overall security posture.

  Additionally, the ability to extend those existing policy sets universally – across the entire enterprise – provides a more comprehensive structure and increased oversight over the entire program. The ability to manage policies across all delivery mechanisms—appliances, virtual appliances, IaaS/PaaS and cloud—ensures that policies are consistently applied on-premises, in the cloud and at the endpoint. Agencies that can produce this level of policy enforcement set themselves up to have an effective cloud security program. The next steps in the process combine these policies with appropriate technologies to lock down data and applications no matter where they reside.

- **Protect information everywhere.** Network security solutions can serve as a way to complement the focus of endpoint security solutions. With network-based email and web gateway technology, delivered either in the cloud or on-premises, agencies can increase policy enforcement along with inspecting the activities of any device. Agencies have the ability to identify where data is stored across cloud, mobile, network, endpoint and storage systems, classify that data, monitor how the data

is being used, and protect the data from being leaked or stolen. This ensures that the routes of all valuable traffic are seen and monitored for anomalies.

It would also be ideal if every employee used a secure network, but that is not always the case. Whether it is at home or at an airport or a coffee shop, valuable data can be transferred over less-than-ideal networks, bringing into focus the power of encryption. Encryption capabilities ensure secure data transfers start by incorporating technologies that positively identify a user with a dynamic, second factor of authentication that cannot be predicted or stolen. This enables agencies to deliver secure remote access to the agency network and its resources/applications regardless of where the employee is accessing it.

- **Protect applications everywhere.** The cloud has enabled agencies to use a wider-variety of applications than ever before, but each of these applications comes with different risks. With the right cloud security tools, agencies can rest assured that their data remains protected no matter the type of application that uses it.

  Data Loss Prevention (DLP) capabilities will further help agencies uncover data loss blind spots in both sanctioned and unsanctioned cloud applications—both on–premises and to the cloud—by detecting and preventing unauthorized data exfiltration. Integrating Cloud Access Security Brokers (CASBs) can extend an information technology department's reach to protect users and data as they interact with cloud applications and services, providing visibility and control directly over the use of an application.

## Why Symantec?

Our job at Symantec is security. As the computing model has changed so have we. Symantec's comprehensive cloud security portfolio is the industry's only end-to-end solution, allowing agencies to unify access governance, information security and threat protection across cloud and on-premises infrastructures. This results in stronger protection, greater visibility and integration across the entire enterprise. The cloud generation is already here. We'll help you make sure your agency can get the most out of it, while delivering the most advanced capabilities in data security, threat protection and encryption. Symantec can provide a comprehensive cloud solution that prevents, detects and reports on unauthorized attempts to exfiltrate data from the internal network, mobile devices and the cloud, as well as:

- Prevent insider threats or hostile outsiders from exfiltrating data via the cloud
- Reduce risk of fraud, data loss and inadvertent violation of security policy and data exfiltration from the cloud
- Create an improved security posture
- Prevent violation of data security and privacy laws, regulations and policies

Visit: symantec.com/theme/symantec-cloud-security

## About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

**Symantec Corporation World Headquarters**

350 Ellis Street

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com


# SYMC_wp_Cloud_Gen_Government_EN_v1a