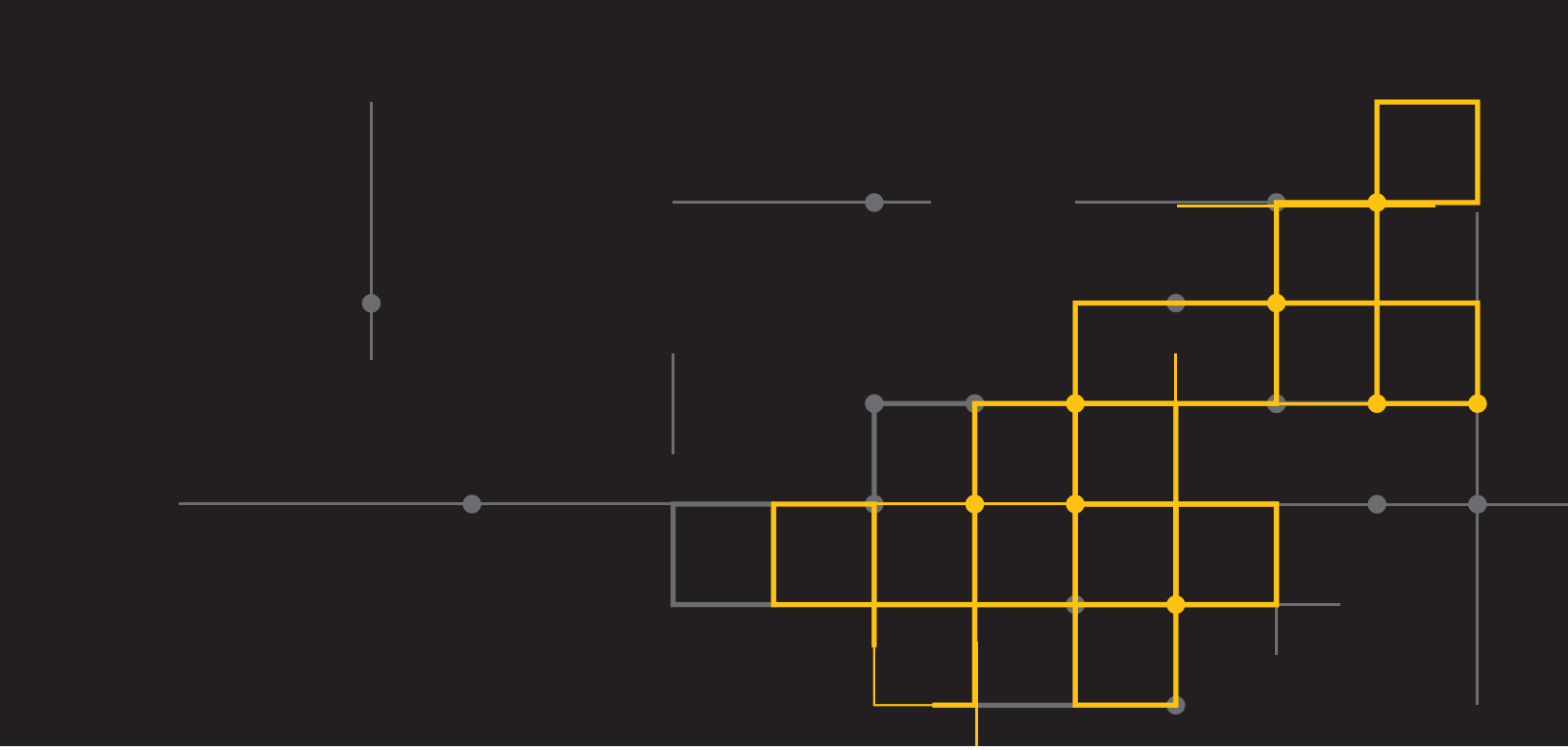

Rethinking Federal Cybersecurity for the Cloud Generation

White Paper | May 2017

Symantec

Welcome to the Cloud Generation

Data security was once a simple concept, especially for federal agencies. Employees used one device to access data through a single network. The goal for technology providers was to secure this infrastructure at all costs. If the infrastructure remained secure, so did the data.

Those days are long gone in government. Now if an employee wants to share a large file with a co-worker, and email can't handle it, the employee looks for other options such as putting it in their personal Dropbox account. A seasoned federal employee might think better about doing something like this since it is more than likely not an authorized agency application, but younger employees, who grew up using the cloud—the cloud generation—see it as a way of being more productive.

While the agency itself may not sanction cloud capabilities, or approves just a small amount, employees are using unauthorized cloud services at will, resulting in a growing issue known as Shadow IT. The employee is not trying to be malicious – instead just doing their job effectively – but it requires federal technology leaders to rethink their security strategies. It is no longer about technology leaders choosing cloud computing – the cloud has ultimately chosen them.

So, what are agencies to do? With employees forcing them toward the cloud, federal agencies need solutions to stay protected. With recent advances in integrated cloud 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 is protected.

The Changing Face of Government Technology

As the cloud has changed how employees work, the government is poised for changes as well. With a new administration that has announced cuts to government spending, agencies must continually look for greater efficiencies and cost savings. The cloud already offers some of the capabilities the new administration seeks: more business-oriented outcomes.

As such, agencies are in transition mode—combining on-premises, hybrid and cloud solutions into their environment—but this transition isn't occurring overnight. Agencies are still concerned with the proper security of the data flowing between these various environments. But, with the National Institute of Standards and Technology's Cybersecurity Framework (CSF), agencies now have a roadmap to feel more confident in their use of the cloud.

With the emergence of enterprise-wide cloud security, agencies can find these efficiencies while operating with a more business-oriented approach. Agencies can feel confident that their data is being protected throughout the entire lifecycle.

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 agencies to either save or reinvest that money in other mission-oriented activities.

This is true for authorized cloud applications only. The benefits of the cloud tend to diminish—or at least become murkier—when dealing with Shadow IT and the resulting information drift. The use of unauthorized cloud applications adds to the security challenge, along with:

- **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 that sprawl of Shadow IT. It is not uncommon for an agency technology leader to believe their employees use only a few dozen cloud applications only to learn later that number is a few hundred. With all of these challenges, agencies must rethink security. As computing changes, both from technology to habits, so must the security strategies and techniques to support that change.

The Path Forward

For the federal government, the historical 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 to extend on-premises policies into the cloud. This allows agencies to follow best practices they have used for years, but with a focus on the cloud. In addition, with proper solution integration, agencies can get enhanced visibility across all endpoints, improving the overall security posture. Agencies can take that a step further by applying 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 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 can 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.

Benefits of a CASB

CASB is a set of new cloud security technologies that addresses the challenges posed by using cloud apps and services. These new CASB solutions are designed to help organizations enable the productivity gains offered by cloud apps and services by providing critical visibility and control of how these services are being used. They help information security teams:

- Identify and evaluate all cloud apps in use (Shadow IT)
- Enforce cloud application management policies in existing web proxies or firewalls
- Enforce granular policies to govern handling of sensitive information, including compliance-related content
- Encrypt or tokenize sensitive content to enforce privacy and security
- Detect and block unusual account behavior indicative of malicious activity
- Integrate cloud visibility and controls with broader security solutions for DLP, access management and web security

Improving Visibility

The ultimate goal of these solutions and any cloud security network is to improve visibility. When information technology leaders lose sight of what their data is doing and where it is going that is when problems begin.

This is especially true in the age of encryption. Agencies have smartly turned to encrypting data as the default. This ensures that data stolen from government sites cannot be read by malicious actors, and is a huge benefit for government, but one that comes with an associated challenge. Administrators do not always have a clear line-of-sight into what data—when encrypted—is moving around the network. This creates a gigantic blind spot that encompasses nearly two-thirds of all government information.

This is where end-to-end cloud security systems can shine. Since government agencies are responsible for protecting data once it is in the cloud—not the Cloud Service Provider that is housing the data—government agencies can use modern cybersecurity solutions to track this encrypted data as it travels to other applications. In addition, it ensures the agency maintains the encryption keys so they are the only ones who can unlock the data. This visibility is paramount to keeping it protected. IT administrators will know who has accessed what specific data without leaving it vulnerable.

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
Email: federal_government@symantec.com

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