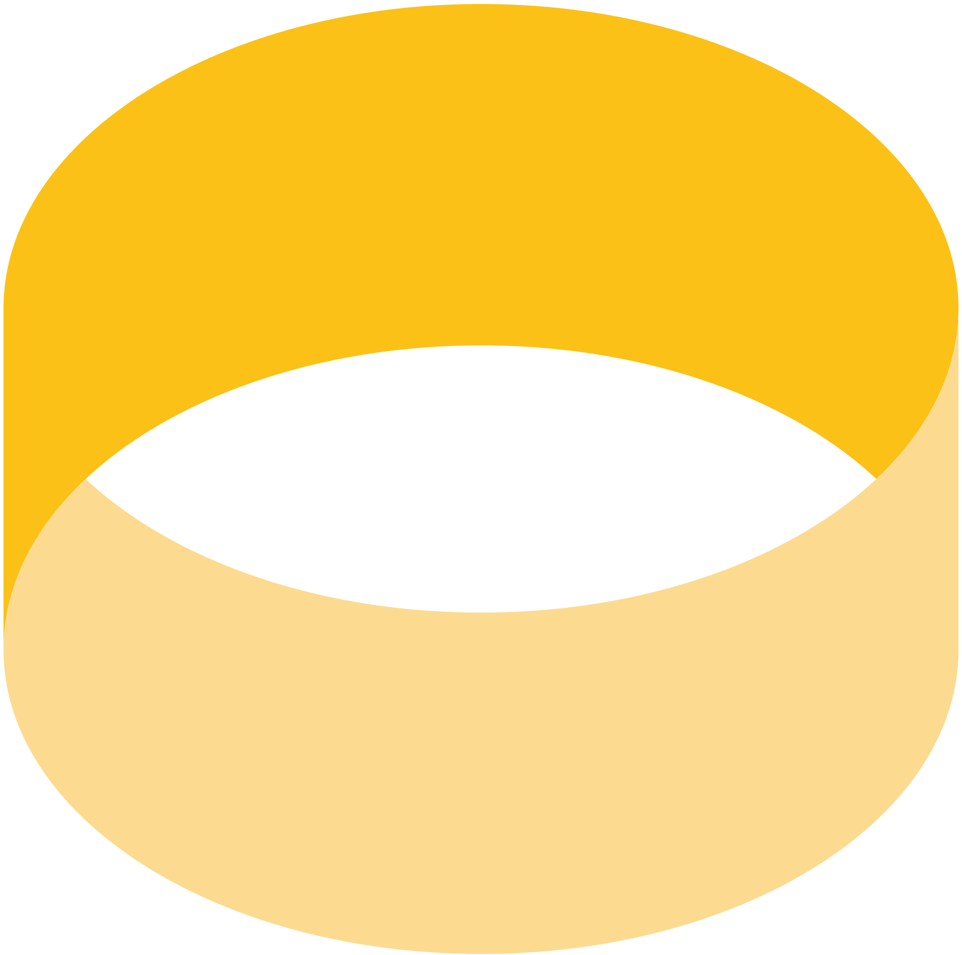

Modernization Needs to Start with Security

WHITE PAPER

Symantec™

The Modernizing Government Technology (MGT) Act, which was signed into law as part of the 2018 National Defense Authorization Act, offers agencies an unprecedented opportunity to improve the security of their systems, applications and data.

The legislation creates a $228 million fund to help federal agencies modernize outdated information technology (IT) systems. The goal is to reverse a trend in which agencies have spent a growing portion of their IT budgets just maintaining old and outdated systems, rather than investing in new technologies and services. In recent years, the federal government has spent as much as 80 percent of its IT budget on maintenance, rather than new investments.

But the modernization push is not just about new technology—it's also about better security.

Not only are legacy systems incredibly expensive to maintain, they are also difficult to secure, especially given the patchwork nature of the existing IT infrastructures at most agencies.

The surge in funding provided by the MGT Act, along with the vision outlined in the Report on Federal IT Modernization, offers the federal government a chance to reset the cybersecurity baseline and to create a framework for maintaining their cyber posture in the years ahead.

The Legacy Challenge

The burden of maintaining legacy systems was made clear by a May 2016 report from the Government Accountability Office. Most notably, 5,233 of the government's approximately 7,000 IT projects are being funded simply for operations and maintenance purposes. Such spending has increased over the past seven fiscal years, which has resulted in a $7.3 billion decline from fiscal years 2010 to 2017 in development, modernization and enhancement activities.

"Federal legacy IT investments are becoming increasingly obsolete: many use outdated software languages and hardware parts that are unsupported," GAO writes. "Agencies reported using several systems that have components that are, in some cases, at least 50 years old."

These legacy systems require employees with special knowledge to maintain, do not integrate well with modern systems and feature security gaps that can be exploited by bad actors. They also do not provide the federal government with the functionality that newer systems can typically offer, while creating a less efficient work environment.

With the new funds from the MGT Act, federal agencies are expected to focus first on replacing those systems that come with high risk and high maintenance costs, then modernizing other systems as more funding becomes available.

Embracing Enterprise Security

It's not enough simply to update or replace old systems. As the Report on Federal IT Modernization makes clear, the goal is to approach security from an enterprise perspective—building architectures that allow improved visibility into network activities, avoids potential blind spots that hackers can infiltrate and ensures data protection in a world where traditional security borders no longer exist.

The federal government found itself overburdened with legacy systems, in part, because of a penchant to purchase "best-of-breed" technologies. While these point solutions were seen as the best in their sector, they were not built to integrate with one another. This has been called the "shiny object" theory. Agencies purchase point products with the hopes it fixes a problem, only to later realize the technology created new vulnerabilities.

Think about it in terms of a football team. A coach could assemble a team with the best players in the NFL, but if they never practiced together, had a cohesive game plan, or understood the strengths and weaknesses of their teammates, the players would struggle to beat a less talented team that had those things in place.

Going forward, agencies instead need to take an enterprise approach to security, focusing on technologies that can work together seamlessly, eliminating the visibility issues that plague today's environments.

An enterprise security approach improves overall visibility and general security, while reducing the resources needed to secure larger systems. It is not that these technologies are not seen as best-of-breed, but they are designed with an enterprise mentality. It's like assembling the best team of football players—but doing so with an overall game plan in mind.

Federal agencies need to plan now for how security fits into their modernization plans. While they will surely want to replace the most outdated systems they must ensure that any new solution fits within the larger security architecture. By not doing so, agency leaders risk creating new security problems that counter the intended effects of their modernization initiative.

Integrated Cyber Defense

Federal IT leaders planning their modernization efforts need to think about an integrated cyber defense approach, one that reflects the complexity of today's IT enterprise, with its mix of cloud and on-premise solutions. With this approach, the focus shifts from the perimeter to the data.

Perimeter defense was the most popular form of cybersecurity for many years. But with cloud, mobility and related trends, the infrastructure has evolved, and a perimeter defense alone is no longer a viable strategy. In short, the perimeter is wherever the data is.

Practically speaking, that means the perimeter encompasses information, users, devices, applications, websites and messaging platforms. By looking at how data flows from one platform to the next, along with the paths in between, agencies can ensure there will never be a time where they cannot view how data is being used. This includes cloud security solutions to govern access, protect information, defend against advanced threats and protect workloads as they move to – and from – the cloud.

Specifically, agencies need to consider four key areas for an integrated cyber defense approach, including:

- **Access governance** – as agencies continue to move critical data, applications and systems between on-premises and cloud environments, effectively managing access becomes more critical. This includes establishing multi-factor authentication, enforcing uniform policies, maintaining full compliance and better managing shadow IT to deter unsanctioned usage.
- **Information protection** – information in motion is information at risk, meaning that agencies need to look at protecting data. This includes eliminating blind spots through data loss prevention policies; ensuring compliance to defend intellectual property; controlling endpoints across the ecosystem; and safeguarding data through encryption and policy enforcement.
- **Advanced threat protection** – the movement of data beyond traditional IT controls has led to a huge increase in security vulnerabilities, requiring the ability to unmask every threat. This is accomplished by layering protection to include the endpoint, network and the cloud; harnessing multi-vector telemetry; and preventing attacks through a preventative architecture.
- **Workload protection** – migrating to the cloud is a quick and cost-efficient approach to accelerating agency modernization efforts. Cloud security, however, requires agencies to protect their workloads by deploying trusted security controls, monitoring across public clouds, private clouds and across on-premises data centers, as well as automating compliance assessments.

This approach can happen only if agencies consider security at every stage and how these pieces work together. Government has suffered from a complexity problem more than anything. They have created systems that are so intricate and with so many non-compatible parts that there are gaps in coverage. These gaps provide vulnerabilities and enable hackers to more easily breach these systems. An enterprise approach to cybersecurity can close those gaps.

Conclusion

Federal technology leaders need to seize the opportunity created by the MGT Act. These funds provide a respite from legacy systems and allow technology leaders to make sound investments in their agency's technology future.

It seems fitting that of the 13 agencies looked at in the GAO's report, 11 agreed with the recommendations. The other two made no comment. There is a feeling in government that these changes are needed. The Trump administration has made IT modernization a key priority, especially as leaders look to make significant changes to overall department budgets.

Federal agencies will always have a need for IT. To spend on outdated systems that are hard to maintain, difficult to use and do not provide adequate security is both wasteful and dangerous. Federal technology leaders need to make these changes.

The biggest concern is that federal agencies will receive these funds and use them to create new problems further down the road. This is the government's opportunity to get technology correct. Federal leaders are being called on to be innovate, daring and, ultimately, successful. An integrated cyber defense approach with a focus on the entire enterprise and data security is the way forward.

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.
350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | **www.symantec.com**