White Paper

# Security Connected from McAfee: Comprehensive, Cost-Effective Security

intel Security

## Table of Contents

Even before the effects of the sequester, the overall US Federal IT budget was predicted to drop from $121.7 billion in 2012 down to $115.5 billion in 2013, according to the Professional Services Council.[1] This reduction is part of what US CIO Steven VanRoekel calls "doing more with less," an initiative to drive IT efficiency and effectiveness across government while spurring innovation, rooting out waste, and streamlining and consolidating agency operations.[2] At the same time, VanRoekel and other leaders recognize that federal cybersecurity efforts must not suffer. If anything, cybersecurity requirements for government agencies have increased, as illustrated by the upcoming publication, *Security and Privacy Controls for Federal Information Systems and Organizations* from the National Institute of Standards and Technology (NIST), a catalog of security technologies that help agencies meet FISMA and other requirements.[3]

With federal budgets trending downward and both cyberthreats and mandates heading upward, the question becomes, "Can you get comprehensive cybersecurity that provides real-time threat visibility and protection at a reasonable cost?" The answer is yes. Not only can you achieve comprehensive security in a cost-effective manner, but doing so with the Security Connected framework from McAfee—now a part of Intel® Security—provides better security by applying integration, real-time threat intelligence, correlation, and speed to achieve stronger security at a lower price than alternative and point solutions. The same framework that delivers stronger security delivers operational efficiencies to also meet VanRoekel's objective of streamlining and consolidating IT.

We designed the Security Connected framework to help customers integrate multiple products, services, and partnerships for centralized, efficient, and effective mitigation of security risk. Mike DeCesare, president of McAfee, described the need for such a framework—and the challenge the security industry faces—in a 2012 talk at the White House: "We must unify, simplify, and strengthen the way we provide security by utilizing a framework for integrating potentially disparate technologies—building bridges between security 'islands' to close coverage and technology gaps. At McAfee, we call this approach Security Connected."

Built on more than two decades of proven security practices, the Security Connected approach helps agencies and programs of all sizes—across all geographies—improve security, optimize security for greater cost effectiveness, and align security strategically with government initiatives.

Security Connected resources and tools provide a clear path from the concept of security to its implementation and can adapt to an organization's unique risks, infrastructure, and objectives. And significantly, the systems are scalable, making them optimum for deployment in the smallest programs as well as enterprise-wide in the largest agencies.

Most importantly, Security Connected provides resilience—the ability to operate through a cyberattack. Resilience requires:

- Speedy action to defend or respond.
- Agility to either adopt new enabling technologies or rapidly add capability in response to a new threat.
- As dependencies increase, stimulate collaboration with a community of interest.

**Security Connected Reference Architecture**

The Security Connected framework provides a platform and a best practice architecture to build resilience into government infrastructure:

- Battlefield command and control systems.
- Continuous monitoring.
- Critical government digital services.
- Cyber-readiness.
- Intelligence-driven response.
- Secure information sharing for joint operations.
- Secure mobility.
- Security operations centers.
- Shared service data centers.
- Secure virtualized infrastructure.
- Tactical network environments.

The Security Connected platform delivers the capability to resist and be resilient to the advanced threat, the ability to respond at network speed, and a framework that enables the addition new capabilities. Coupled with our McAfee® Security Innovation Alliance partner program, the framework provides unrivaled alignment to government cyberdefense requirements and unprecedented levels of scalability, survivability, and integration to protect challenging government environments.

How is this framework cost effective? The answer lies in the cost savings of using commercial off-the-shelf (COTS) software.

## COTS Is Superior to GOTS

We develop COTS software: the research, development, maintenance, and perpetual update costs are absorbed by McAfee and spread across a large number of commercial users. The reason that COTS has been mandated across many government and business programs is that COTS products offer significant savings in procurement, development, and maintenance. The solution costs are lower than with custom software, and the advantages are often greater.

Contrast this to customized government off-the-shelf (GOTS) solutions. In the cybersecurity arena, the government has issued solicitations for specialized security tools that require custom development, are untested in field environments, and are expensive to operate and maintain. Sometimes these specialized tools don't even get deployed, but the funds are allocated so the money gets spent. The US Department of Homeland Security's Risk Assessment and Management Program (RAMP) program offers a noteworthy and cautionary $57 million tale of well-intended funding unwisely spent.[4]

The proposals sound like answers to real problems, but, in reality, the systems might not be compatible with others in the network environment or they might not work on the large scale the government requires. A solution might work perfectly well in the lab where it was developed, but put it in a real-world environment with real threats, and you may find unanticipated problems. If a solution can't be operationalized effectively, it doesn't matter how well it performs in the lab. That great tool might be effective in a network of 50,000 endpoints, but how well does that scale to 500,000 or a million endpoints?

In 2012, a whistleblower revealed that the US Veteran's Affairs Office of Information and Technology (OIT) had deployed only 16% of the 400,000 endpoint encryption licenses they had purchased despite repeated data breaches. The subsequent investigation determined that: "OIT did not install and activate all of the licenses due to inadequate planning and management of the project. Specifically, OIT did not allow time to test the software to ensure compatibility with VA computers, ensure sufficient human resources were available to install the encryption software on VA computers, and adequately monitor the project to ensure encryption of all VA laptop and desktop computers."[5]

The ratio of cost-to-value for GOTS tools doesn't work out favorably either. Consider the following:

- Individual point solutions require individual management controls and individual people to operate them.
- They end up siloed and isolated from one another, and information sharing consists of trading spreadsheets, each of which contains volumes of information, producing not true security, but "swivel chair" security.
- This integration-by-spreadsheet approach is very labor intensive and inefficient, especially when you consider that at many organizations, 70% to 80% of the IT budget may go toward operating costs.

To reduce IT costs in a budget challenged environment, you have to look at solutions that reduce that 70% to 80% of operating costs. The Security Connected from McAfee framework fits the bill.

Another reason COTS is superior to GOTS is that the private sector is generally better equipped to develop the most up-to-date IT solutions in a rapidly changing environment. This is especially true in cybersecurity, where the speed and volume of threats is so intense that security companies are constantly innovating to be able to deter them. By the time government requirements are translated into customized solutions, the threats have already morphed and the requirements might be suited to deter yesterday's threats rather than tomorrow's. Government's role should be in enabling basic cybersecurity research, not applied research that ends up in product development.

## Simplicity Versus Complexity: The Platform Approach

While it might seem counterintuitive, the simple approach to security is more effective than a complex approach. In fact, as Howard Schmidt said while transitioning from government security service back to the private sector, complexity is the enemy of security—and it certainly costs more. Having one framework or suite of products that can meet all your needs makes eminent good sense. This simple approach is far superior to a collection of tools that might not connect with each other and that make reporting complicated. And there's no longer a need to seek coverage from multiple security vendors to cover all the threats—as long as you have the right vendor with a comprehensive approach. The Security Connected platform provides core capabilities as well as an open environment to cover a full range of current and emerging security needs with maximum efficiency.

With the McAfee portfolio of products available through Security Connected, your network defenses learn as they protect, becoming producers and consumers of threat information from your own network. They create an ecosystem that leans toward resilience, removing much of the noise and focusing on the most complex threats for best use of limited resources. Since solutions automate protection tasks while simultaneously managing policy, there are fewer alerts, events, and administrative details to distract administrators. The items that remain are the ones that matter the most and will benefit the most from human attention.

This ecosystem is informed by the McAfee Global Threat Intelligence (McAfee GTI) service, which is integrated into our solutions, feeding them real-time, real-world threat research to enable continual situational awareness. McAfee GTI serves as an immune system, protecting against attacks by electronically detecting and correlating, at machine speed, behavioral data that is identified as harmful from worldwide sources. In milliseconds, McAfee GTI assesses changes, assigns risk levels, and distributes protection recommendations to products covering every threat vector at every tier.

The Security Connected platform combined with McAfee GTI makes security management easier for organizations of all sizes, so that integrating relevant protections and controls and establishing a baseline and escalation process for key risks become simpler undertakings. With the Security Connected approach, you have an integrated platform of intelligent solutions that leverage threat intelligence. Such solutions provide greater accountability and build trust into information systems such as laptops and PCs as well as tablets, smartphones, and embedded systems that use, reside in, or create their own clouds and traverse between networks. With McAfee you also get breadth of coverage with far fewer contracts and less complexity, so you really can do more with less. You can get 35 to 40 different NIST-certified controls in a single platform rather than through 35 to 40 different contracts.

And with Security Connected you have additional choices. Through the McAfee Security Innovation Alliance, you can benefit from the most innovative security technologies not only from McAfee but also from thousands of developers that can integrate with our extensible management platform. Today more than 150 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance. Their tools can snap into the Security Connected framework as well. The Security Innovation Alliance enables you to leverage investments you've already made, bringing strategic tools together, and augmenting them where necessary.

## Customers Have Seen the Value

From our perspective, value is not just in the improvement of security and the reduction of risk. We see the value we bring as twofold: the improvement of security *combined* with operational cost reduction. We've made it a point to study customers who have implemented our integrated platforms and are finding that customers are seeing and realizing the downstream effect of Security Connected in a bigger and broader way. Here are some examples of what we've found:

- A major city in the northeast US saved $18 million over five years by standardizing with McAfee.
- A major consumer manufacturer reduced the number of security vendors used from three to one. The company also reduced the number of security management consoles and servers by 75% and identified more than $1 million in savings over three years related to helpdesk, incident management, and patching costs.
- A large healthcare organization cut security spend in half by going with McAfee. It reduced the complexity of vendor management processes, including hardware, software licensing, and audit and compliance costs by $3 million.
- A US state government standardized its security framework with McAfee and determined that it will save between $5 million and $8 million over three years.

## Consolidation Is a Winning Proposition

In a *Federal Times* article on budget cuts, VanRoekel remarked, "I think fiscal pressure produces an outcome that is one where you will see a wave of innovation and a wave of efficiency gains that would not have been formed in time of budget increases." Security Connected does exactly that—it provides an innovative approach to security that produces major efficiency gains.

The Security Connected platform delivers:

- Optimum security at a reasonable cost.
- An integrated approach to threat mitigation that lets you interconnect products, services, and partnerships.
- Cost-effective COTS solutions that will perform in your environment—whether large or small—much better than GOTS.
- An industry-leading vendor with a comprehensive set of top-rated security tools.
- The simplicity of a single platform of solutions that work together and complement one another.
- McAfee GTI, which adds all-important threat intelligence to the entire framework.
- Additional choices of products integrated with the Security Connected platform through our Security Innovation Alliance, yielding interoperability and openness, as well as operational efficiencies.
- Proven cost savings.

Taking advantage of an integrated framework such as Security Connected and using COTS rather than GOTS technologies produces major efficiency gains. It is possible to get comprehensive cybersecurity that provides real-time threat visibility and protection at a reasonable cost. The right integrated COTS approach to security can meet all of a government agency's requirements—optimizing its security posture, reducing its spend, simplifying the operation, and meeting government cybersecurity requirements. We call that a good value proposition.

## More Information

For more information on Security Connected visit **http://www.mcafee.com/us/enterprise/security-connected/index.aspx**. For more information on Public Sector visit **http://www.mcafee.com/us/industry/public-sector/index.aspx**.

## About McAfee

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. **www.intelsecurity.com**.

1. **http://fedconnects.com/index.php/2013/01/part-one-federal-it-budgets-and-infrastructures-face-challenges-and-a-new-era/**
2. **http://cio.gov/wp-content/uploads/2012/09/FY2013-IT1.pdf**
3. **http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800_53_r4_draft_fpd.pdf**
4. **http://dailycaller.com/2012/07/24/beleaguered-homeland-security-agency-wastes-57-million-on-failed-computer-contract/**
5. **http://www.va.gov/oig/pubs/VAOIG-12-01903-04.pdf**

**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee, and the McAfee logo are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2013 McAfee, Inc. 60183wp_sec-conn-value_0413B_fnl_ETMG