Your Guide to Key Advancements in Government Cybersecurity

Table of Contents

Executive Summary

There's a lot of talk in government about modernizing aging systems and adopting digital services to give citizens the same type of experience they're used to getting from private companies.

But none of these initiatives can stand on its own without a solid cybersecurity strategy. Underpinning each effort is a major push to improve how the government secures its data and systems — and those approaches are steadily evolving. They have to if agencies stand any chance of defending against sophisticated cyberattacks, a daily barrage of phishing attempts and the unintentional consequences of poor cyber hygiene among rank-and-file employees.

That's why governments at all levels are increasingly taking a proactive, departmentwide approach to cybersecurity. They're starting to invest in emerging technologies such as artificial intelligence (AI) to supplement their modest staff sizes. They're also forging partnerships across state lines, marrying security with DevOps and finding creative ways to attract and train cyber talent.

In this guide, we highlight those key advancements in addition to specific examples from federal, state and local agencies that put these approaches into practice. Rather than rehash the basics of cyber in this guide, we dive into deeper topics such as DevSecOps and machine learning in cybersecurity to provide practical examples and tips for how you can adopt similar approaches at your organization.

Before we begin, let's look at a few government programs that should be on your radar and key stats that help quantify the enormity of the security challenges that agencies face.

Meet the Experts

To better understand how agencies are advancing in key areas of cybersecurity, we included insights from government chief information officers, federal executives and other experts throughout the guide.

Ryan Aniol
Deputy Chief Information Security Officer, State of Minnesota

Cambray Crozier
Communications Director for CIO, State of Minnesota

Rajiv Das
Chief Security Officer and Deputy Director, State of Michigan

John Felker
Director, National Cybersecurity and Communications Integration Center (NCCIC), Department of Homeland Security

Paul Haugan
Director of Innovation and Technology, Auburn, Washington

Beth Killoran
CIO, Health and Human Services Department

Michael Kratsios
Deputy Assistant to the President and Deputy U.S. Chief Technology Officer

Shannon Lietz
Founder, DevSecOps Foundation

Tim Roemer
Department of Homeland Security Deputy Director and Governor's Public Safety Adviser, State of Arizona

Michael Sherwood
CIO, City of Las Vegas

Jim Smith
CIO, State of Maine

Elayne Starkey
Former CSO, Delaware

Janet Stevens
CIO, Agriculture Department's Food Safety and Inspection Service

Aaron Wieczorek
Digital Services Expert, United States Digital Service, Veterans Affairs Department

Government Cybersecurity Federal Initiatives in Action

Federal

Modernizing Trusted Internet Connections to Enable Secure Cloud Adoption

The federal government may have found a workaround to the Trusted Internet Connections (TIC) program, an 11-year-old initiative to optimize and standardize the security of individual external network connections that federal agencies use.

The Small Business Administration is one of the agencies leading that charge. On the heels of a 90-day pilot in early 2018, Deputy CIO Guy Cavallo said the security features SBA tested are comparable, if not better than, what TIC provides.

"We had incredible visibility into everything," he said of the pilot. "The TIC's just looking at traffic. This umbrella is looking at many, many other features, such as improper or incorrect passwords on your servers."

Another issue with TIC is that it doesn't mesh well with cloud, and it has failed to keep pace with the massive growth of government networks and data. Cavallo said SBA saw a performance boost during the pilot. Stay tuned for next steps on these efforts.

AIS Helps Public, Private Sectors Share Cyberthreats

A Homeland Security Department program is helping federal agencies and the private sector team up against cyberthreats. The Automated Indicator Sharing (AIS) capability lets participants exchange information on cyberthreat indicators at machine speed, regardless of whether they are public or private entities, said John Felker, Director of DHS' National Cybersecurity and Communications Integration Center.

AIS is a free, voluntary program that makes participants aware of threat indicators such as malicious IP addresses or the email accounts behind a phishing attempt. AIS has more than 260 member organizations — 190 of which are non-federal entities. Since March 2016, DHS has shared more than 3 million unique cyberthreat indicators. Data sharing is voluntary, however, so AIS faces the challenge of having members contribute equal information. Felker said partners should communicate with one another for the best cybersecurity posture.

73%

of federal agencies lack visibility into what is happening on their networks, and especially lack the ability to detect data exfiltration.

Source: Federal Cybersecurity Risk Determination Report and Action Plan

38%

of federal cyber incidents did not have an identified attack vector, suggesting agencies' ability to determine threat actors' motivations and methods behind cyberattacks has not improved.

Source: Federal Cybersecurity Risk Determination Report and Action Plan

Government Cybersecurity State and Local Initiatives in Action

State

MS-ISAC Hosts Program to Help State, Local Election Officials

The Multi-State Information Sharing & Analysis Center (MS-ISAC) launched a pilot program in 2017 aimed at supporting state and local election officials with cybersecurity. The initiative began as a four-month operation in seven states and has since expanded to include nearly all 50 states and more than 450 local election offices. The program seeks to identify products and tools for boosting communications and guarding against cybersecurity dangers facing the election community. MS-ISAC's work came after DHS declared in January 2017 that election infrastructure is a critical infrastructure subsector.

State, City Governments Embrace NIST Framework

When the National Institute of Standards and Technology (NIST) partnered with other federal agencies and the private sector to develop the first iteration of the NIST Cybersecurity Framework (CSF), the focus was on protecting our nation's most critical assets. The primary audience was entities that own and operate critical infrastructure vital to public safety and national security, such as utilities, telecommunications, transportation and healthcare. But a growing number of state and local governments are aligning with the framework to address gaps in their security efforts. Virginia, Florida, California's Contra Costa County, Houston and Evanston in Illinois are a few of the governments that use CSF.

Local

Arizona Cybersecurity Team Includes Local Governments

Local governments got a seat at the table when Gov. Doug Ducey signed an executive order in March 2018 that created the Arizona Cybersecurity Team (ACT). ACT unites academia, the private sector, and federal, state and local officials to tackle several issues, including enhancing public/private information sharing and developing measures to boost the cyber workforce. The program mandates that two representatives come from local governments, with one of the two representing a rural community. "We can take what one city is doing and then we can help bring that out to the rest of the cities and the rural areas as well," said Tim Roemer, the Arizona Department of Homeland Security's Deputy Director and the Governor's Public Safety Adviser.

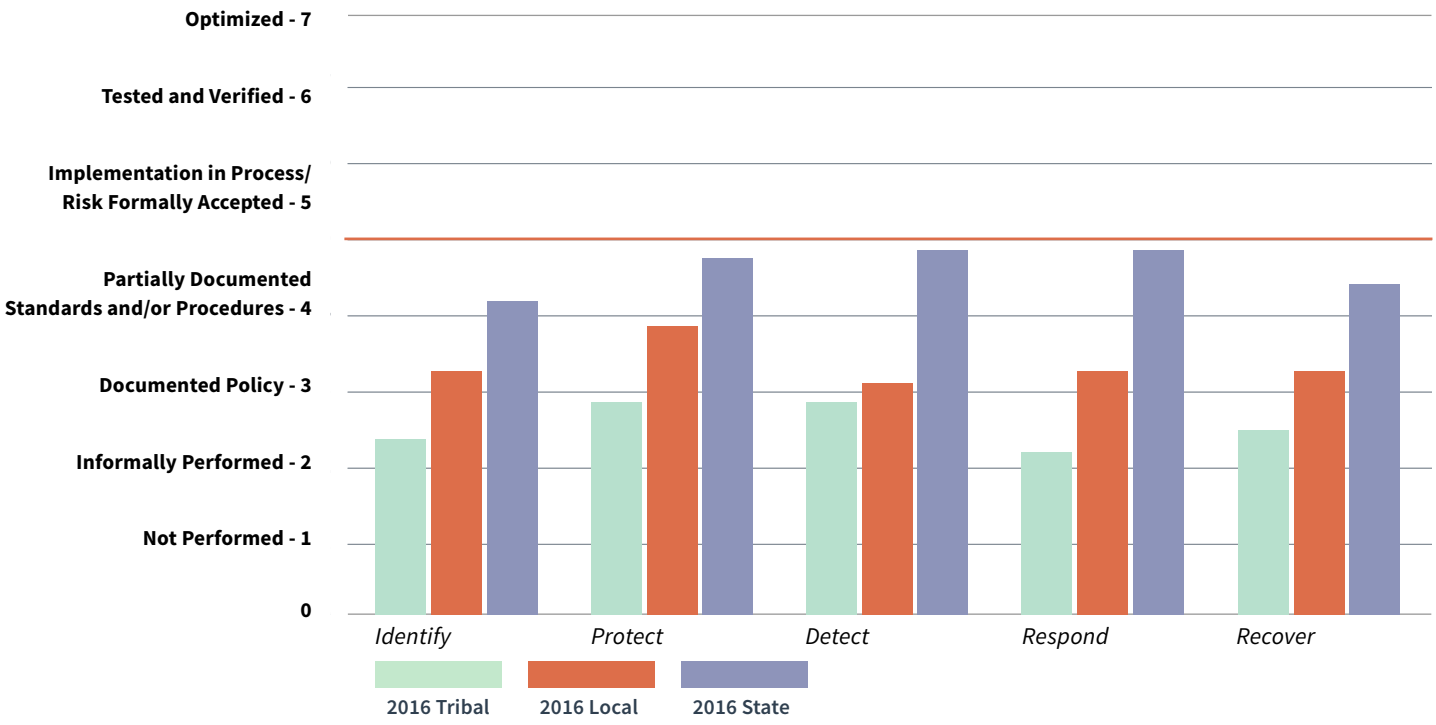
Michigan Embraces CISO-as-a-Service

Michigan is hardening its cybersecurity defenses by conducting a pilot program that brings a chief information security officer's (CISO) benefits to local governments as a service. CISO-as-a-service helps smaller organizations such as county governments by assessing a network's cybersecurity capabilities without a full-time employee's costs. "We have 13 counties out of 84 counties in pilot right now," Michigan CSO and Deputy Director Rajiv Das said during a June 2018 Fortinet/Route Fifty webinar. "We want to help them operationalize those programs, such as incident response [and] operations procedures."

"We want to bring in CISO-as-a-service programs to help with the elections this year," added Das, who is also the Michigan Department of Technology, Management and Budget's Deputy Director. "Election results are a primary concern for us."

The Nationwide Cyber Security Review (NCSR) is a self-assessment that measures state, local, tribal and territorial governments' gaps and capabilities. NCSR was developed using the NIST Cybersecurity Framework Core, with minor alterations.

Using results from the 2016 NCSR, local, state and tribal peer profile groups were created. The graph below represents the averages within each peer profile across the NIST Cybersecurity Framework functions — Identify, Protect, Detect, Respond and Recover — and provides an approximation as to the overall maturity. The horizontal red line (Implementation in Process) represents the recommended minimum maturity level. For more information visit cisecurity.org.



7 - Optimized

Your organization has formally documented policies, standards and procedures. Implementation is tested, verified and reviewed regularly to ensure continued effectiveness.

6 - Tested and Verified

Your organization has formally documented policies, standards and procedures. Implementation is tested and verified.

5 - Implementation in Process

Your organization has formally documented policies, standards and procedures, and is in the process of implementation.

5 - Risk Formally Accepted

Your organization has chosen not to implement based on risk assessment.

4 - Partially Documented Standards and/or Procedures

Your organization has a formal policy in place and started the process of developing documented standards and/or procedures to support the policy.

3 - Documented Policy

Your organization has a formal policy in place.

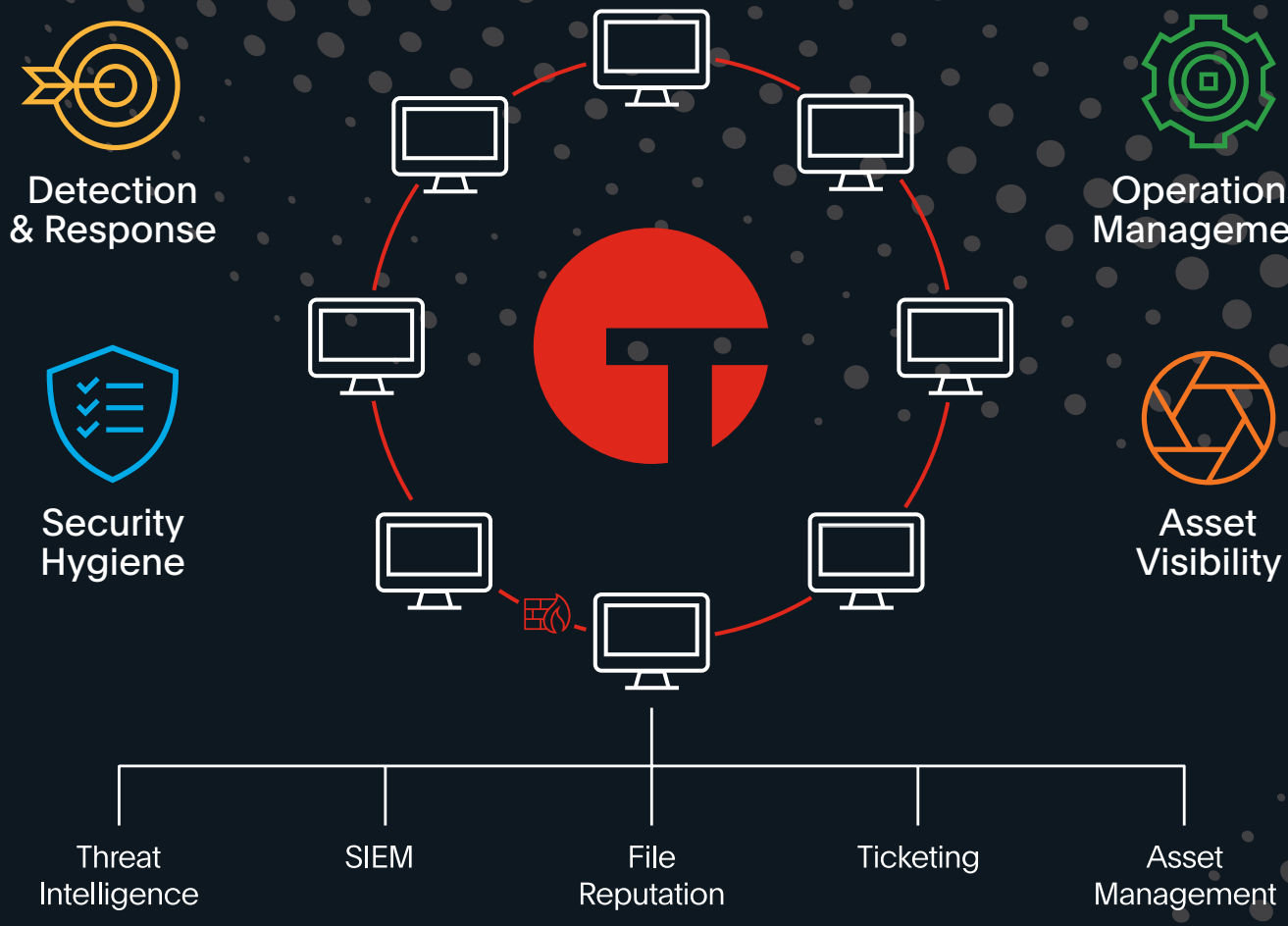
2 - Informally Performed

Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.

1 - Not Performed

Activities, processes and technologies are not in place to achieve the referenced objective.

Tanium provides limitless visibility and control across security and operations



To learn more, visit:
tanium.com/industries/government/

TANIUM™

Cybersecurity and CDM DEFEND

An Interview with Ralph Kahn, Vice President of Federal, Tanium

Government agencies see that the best offense is a strong defense amid escalating cybersecurity threats.

The Continuous Diagnostics and Mitigation (CDM) program demonstrates this by helping federal agencies fortify their networks and systems' cybersecurity. This risk-based approach uses agency-installed sensors to perform automated, ongoing searches for known cyber flaws and evidence of real-time and historical attacks. Sensor results alert network managers about their most critical cyber risks, prioritizing them to help allocate resources based on severity.

The Department of Homeland Security (DHS) and the General Services Administration (GSA) launched CDM in 2013, with Phase 1 focusing on what was on an agency's network and Phase 2 centering on who was on those networks. CDM's Phase 3 is known as DEFEND and focuses on what is happening on an agency's network and how it is protected. It also fixes and upgrades gaps from earlier phases as well as incorporating new and emerging technologies.

To better understand how agencies can successfully leverage DEFEND, GovLoop spoke with Ralph Kahn, Vice President of Federal at Tanium. Tanium is an endpoint security and systems management company and an approved DEFEND vendor.

"DEFEND is happening five years after Phase 1," Kahn said. "The solutions, the requirements, the state of the art technologies, and the attackers have all changed dramatically." DHS acknowledges this and has refocused the program to encourage agencies to continually upgrade and procure new cybersecurity technologies across the board rather than via sequential phases. DEFEND will now field capabilities previously slated for Phase 4 – protecting valuable data.

Kahn said that many adversaries commit more sophisticated cyberattacks today than when CDM began. "Attackers are moving faster, and there are new classes of cyber defense technologies, best practices and metrics that agencies must adopt to counter today's threat environment."

Phase 1 required the management and control of devices, software, security and configuration settings and software vulnerabilities. Phase 2 added controlling and managing account access and trust for people granted access, credentials and authentication and security-related behavioral training.

DEFEND moves beyond asset management to more extensive and dynamic security control monitoring. Security incidents can be mitigated and contained to prevent threats from spreading through the infrastructure. Its capabilities include incident response, event management, myriad forensics tools and mitigating security threats to prevent spreading.

Kahn said DEFEND gives agencies greater input on what tools are installed. Using the Request for Service (RFS) process, agencies can cite specific requirements rather than taking what integrators prescribed in Phases 1 and 2.

"We know that bad things are going to happen, so how do we implement a system that enables us to detect them, minimize their impact and recover from them quickly?" he asked. "That's where most agencies should aim in the DEFEND era."

Kahn said that agencies are changing their defensive postures for an evolving cybersecurity landscape.

"It's about continuous monitoring and continuous visibility to enable finding bad guys rapidly," he said. "We all know adversaries will breach our perimeters. The goal is to build resilience into our defenses, find them faster, remediate intrusions quicker and resume normal operations with minimal disruption."

Tanium provides agencies the ability to scan their end points in real time, enabling cyber defenders to more quickly and easily spot anomalies and start remediating them.

"Today many attackers operate at faster speeds than defenders can defend," Kahn said. "Tanium levels the playing field, allowing cyber defenders to defend at the same speed as the attackers."

"When CDM first came out, 72-hour compliance was state of the art," he said. "Today continuous compliance is the gold standard. Agency leadership should demand compliance every hour of every day to reduce their organization's attack surface."

CDM Phases 1 and 2 also revealed that the acute labor shortage of skilled cyber security professionals is growing. Agencies leveraging DEFEND should investigate automating routine cyber tasks at which machines excel. More automated cyber work leaves agency workforces freed for other things.

Many agencies use Tanium as a force multiplier, utilizing its built-in automation and orchestration for hunting, mitigation, compliance and forensic analysis. A platform with built-in capabilities orchestrated in work flows designed for promoting best practices is a huge advantage for cyber defenders over today's complex stove-piped environments.

Agencies implementing DEFEND can pursue updated metrics, automate and orchestrate their core security processes and increase operational resilience. Successfully performing these measures should dramatically improve agencies' security postures at significantly reduced costs.

Cybersecurity Through Automation, Artificial Intelligence and Machine Learning

Emerging technologies such as automation, AI and machine learning have the potential to reshape entire fields — and government cybersecurity is no exception.

These three capabilities are often intertwined, with automation enabling agencies to perform actions with limited or no human intervention. Machine learning assists computers by using data to exponentially improve their results on a task, and AI allows machines to imitate functions humans classify as cognitive.

The federal government has taken notice, and the Trump administration has prioritized funding for foundational AI research, plus autonomous systems, computing infrastructure and machine learning. Trump's fiscal 2019 budget request made him the first president in history to list AI, autonomous and unmanned systems as administration research and development priorities.

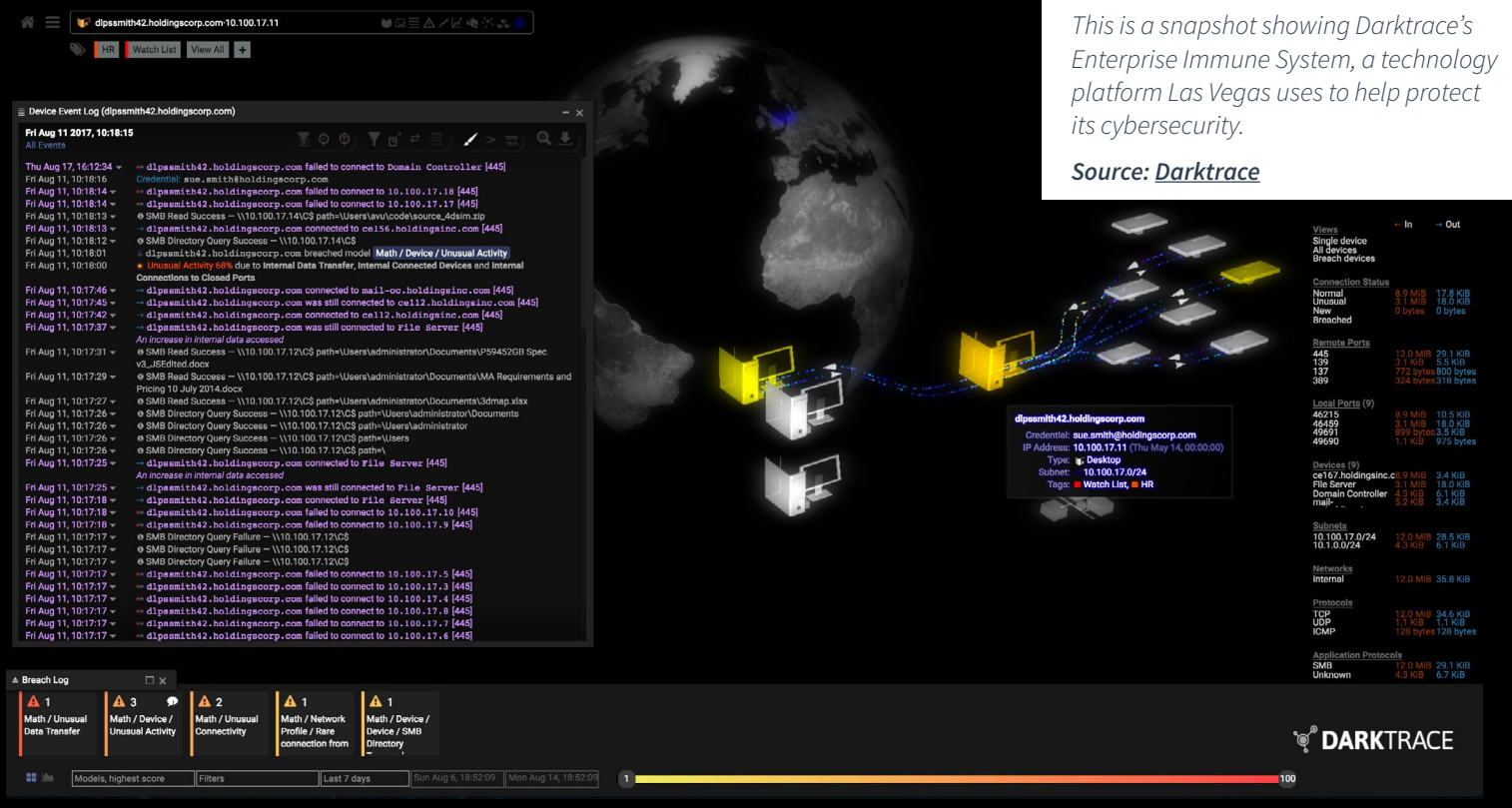
"Artificial intelligence holds tremendous potential as a tool to empower the American worker, drive growth in American industry and improve the lives of the American people," Michael Kratsios, Deputy Assistant to the President and Deputy U.S. Chief Technology Officer, said May 10 at the White House's Artificial Intelligence for American Industry Summit. "Our free market approach to scientific discovery harnesses the combined strengths of government, industry and academia, and uniquely positions us to leverage this technology for the betterment of our great nation."

Automation, AI and machine learning are increasingly important to the federal government's cybersecurity infrastructure, and state and local governments are following suit. All three capabilities accelerate the speed at which cyberthreats are addressed, while reducing cost and overall human involvement.

An October 2017 ServiceNow survey found that 39 percent of federal decision-makers identified intelligent automation as very beneficial to resolving security threats.

There are concerns that automating processes could have a negative impact and complicate an organization's cybersecurity, however, because the technology also gives hackers a new attack tool.

Government applications for automation, AI and machine learning keep evolving, but some federal, state and local agencies are already reaping huge cybersecurity benefits from using these technologies.



This is a snapshot showing Darktrace's Enterprise Immune System, a technology platform Las Vegas uses to help protect its cybersecurity.

Source: Darktrace

Las Vegas Uses AI, Machine Learning to Boost Cybersecurity

Las Vegas's government is using advanced machine learning technology to ward off threats to the city's private, sensitive data.

The technology platform, known as the Enterprise Immune System, uses AI algorithms and unsupervised machine learning to help safeguard Las Vegas's cybersecurity, which is no small feat because of the city's size.

Las Vegas has more than 640,000 residents, an online network of 3,000 users and an annual influx of more than 42 million tourists. CIO Michael Sherwood said shielding such a large amount of data is difficult given these statistics.

"The threat landscape here is always evolving," he said. "You only have so much [of what] we'll call 'brain capital' in your organization. Mathematically, I don't think you can hire your way out of cybersecurity. You need supplements. You have to trust in technology."

Darktrace, the company behind the Enterprise Immune System, calls it a "self-learning cyber defense technology that begins to understand a 'pattern of life' for a network as soon as it is installed."

The system plots an "understanding of normality" for an environment's individual users, devices and networks, helping it recognize unusual activity and potential dangers afterward.

Las Vegas uses the tool to automatically take measured action against potential threats without human involvement, such as halting a download from a banned filesharing program.

The city can also see a 3D representation of its cyber environment, letting government officials visualize external and internal dangers in real time.

"These technology tools are helping me allocate more resources more appropriately," Sherwood said. "I can take the labor savings and move that to other areas and make the organization more efficient. It's critical to the operation."

AI and machine learning programs such as Darktrace's allow cybersecurity teams to do more with less by reducing human involvement.

Las Vegas is not the only government using this technology. Others include Scotland; Livingston County, Michigan; Auburn, Washington; and Australia's Lockyer Valley Regional Council.

"Ensuring the security and functionality of a network that serves 80,000 citizens and protecting sensitive financial data on the city's multimillion[-dollar] budget, is a task too great for a single security officer," said Paul Haugan, Auburn's Director of Innovation and Technology. "After deploying the Enterprise Immune System, it's like we have a 24/7 security team."

"The AI alerts us to threats we would never have known about," Haugan added. "For us, deploying Darktrace wasn't an option; it was a necessity in staying ahead of today's advanced and unpredictable threats."

Cybersecurity is an ever-shifting landscape, but AI and machine learning can help governments of all shapes and sizes.

Success Factors

1 **Consider how automation, AI and machine learning could meet your agency's specific needs** and then explore the technology in action. Experiment with tools in-house to see what changes they will bring and how they affect mission objectives.

2 **Use automation, AI and machine learning as a force multiplier** to strengthen your workforce's capabilities on implementation. Let these tools handle operations they can perform safely and redistribute organizational labor elsewhere.

3 **Switch from a reactive to a proactive cybersecurity posture using automation, AI and machine learning.** Improve these tools by gradually reducing the amount of human oversight required to operate them and tightening their threat-detection capabilities.

Disrupt Cyber Attacks with PowerBroker® Privileged Access Management

ATTACKER

1. PERIMETER EXPLOITATION

Exploits asset vulnerabilities via drive-by downloads, phishing, direct hacking, etc.

2. PRIVILEGE HIJACKING & ESCALATION

Hijacks privileges via exploits and phishing, or leverages stolen/cracked passwords

3. LATERAL MOVEMENT & EXFILTRATION

Leverages privileges, passwords and exploits to compromise other network resources.

BEYONDTRUST

Identifies and remediates vulnerabilities

Limits access to sensitive systems and data

Enforces least privilege to prevent client-side attacks

Eliminates shared accounts and password sharing

Reduces default user privileges to contain potential account hijackers

Monitors all privileged activities for security and accountability

Shrinks asset, privilege and password attack surfaces inside the perimeter

Correlates and analyzes user and asset behavior to identify in-progress threats

Automatically sends alerts and reduces or prevents privileged access

Ready to disrupt the cyber attack chain?
Learn more at www.beyondtrust.com

BeyondTrust FEDERAL

Defend DoD IT Networks from Known (and Unknown) Threats

Address the four lines of effort mandated in the DoD Cybersecurity Discipline Implementation Plan (CDIP) by employing a unified IT risk management platform that combats internal and external threats while managing privileged access for all users. Learn more: Addressing the Department of Defense Cybersecurity Discipline Implementation Plan

Move Confidently to the Cloud – You're Protected

Protect the IT infrastructure in your datacenter or the cloud with zero-gap coverage for diverse and hybrid environments. Discover and assess any IT resource in your organization with agentless and agent-based scanning that protects your high value assets, whether they are connected to your network or not. Learn about our cloud solutions.

A Layered Approach to Cybersecurity Evens the Modernization Playing Field

An Interview with Morey Haber, Chief Technology Officer, BeyondTrust

In today's world of complex IT environments and highly motivated adversaries, government organizations must be more vigilant and proactive than ever before. Government IT professionals are challenged to support mission achievement with a balance of security and end user productivity.

Mandates such as the Cybersecurity Strategy and Implementation Plan (CSIP) and the Defense Department's (DoD) Cybersecurity Discipline Implementation Plan strive to provide structure and accountability to ensure optimal security.

These and others — including the National Institute of Standards and Technology (NIST) cybersecurity and the Federal Information Security Management Act of 2002 (FISMA) frameworks — however, add to the challenges federal agencies face through annual reviews and cumbersome reporting requirements.

In a recent interview with GovLoop, Morey Haber, Chief Technology Officer at BeyondTrust, discussed how a layered approach to IT modernization makes the process easier for agencies by adding security barriers while supporting legacy systems and modern technologies. BeyondTrust partners with government organizations to provide visibility and awareness solutions that effectively maintain security and support compliance requirements.

Any successful modernization strategy starts with understanding what's in your IT environment. "You have to decide what you're going to tackle first," Haber said.

Agencies that comprehend their IT environments can determine the best tradeoffs for modernization. Systems that are fully air gapped should not be a high priority since they lack the same risks as those with internet connections.

Haber said organizations should also remember their primary mission and what requirements drive it. Modernizing mission-critical systems requires more urgency than those that merely support agency goals.

Modernizing legacy systems introduces concerns including cost, technologies' lifespans and vulnerabilities. Haber added that a key issue is whether an organization is using a custom-built or commercial off-the-shelf (COTS) system.

Haber said custom-built systems usually last 15 years or longer, while COTS typically have shorter lifespans. Either system must meet an agency's cybersecurity life expectancy before its expiration date or parts become obsolete.

Helping employees understand they should not customize or personalize government-issued technology at work is also crucial. These technologies must meet established security standards for government business.

Besides enforcing those standards across the workforce, agencies should also consider the benefits of layered cybersecurity, separating portions of their IT infrastructure with security layers. Layering helps government agencies leap from legacy systems to modernized technology by isolating applications, devices and systems from other non-mission-critical environments, ensuring stronger, disciplined-based cybersecurity.

The strategy adds specific safeguards to different IT layers on a case-by-case basis, protecting each as needed and ensuring the health of the greater whole. Cybersecurity layers include networks, hardware, infrastructure perimeters, devices, and Bluetooth and Wi-Fi endpoints.

"Security is like an onion," Haber said. "Every single layer and every single resource must be considered an onion layer. Each may require different strategies."

Haber said government IT staff modernizing their agency's technology should recognize what cybersecurity layers impact their mission, acting accordingly to ensure each layer's security. He recommended that agencies use a SWOT analysis to identify the Strengths, Weaknesses, Opportunities and Threats related to their business units or specific projects.

Haber noted that not all government agencies should implement the same cybersecurity layers, adding some could ignore them entirely because of their mission parameters.

Through a unified suite of solutions, BeyondTrust integrates privileged access management with vulnerability management to provide a centralized view of user, account and asset security. Incorporation of threat and vulnerability intelligence with behavioral analytics adds context to risk assessments and provides a complete view of user and asset risk — with the ability to understand how they affect one another.

"Using these two layers — privileged access and vulnerability management — are how we help protect government assets," Haber said, "regardless of whether the application or system is custom-built or based on a commercial product."

Haber added IT modernization is crucial for government agencies, but so is understanding the cybersecurity requirements necessary for technology asset protection.

"When you consider the layered approach, regardless of COTS or custom, you must consider which ones you're going to modernize first, and which will be cost effective and provide effective layers of security, based on risk," he said. "They all tie together. After all, two identical resources, one plugged into the internet and one air gapped on a raised floor, have two completely different risk profiles and two different layered security models. They must be prioritized and modernized differently."

Developing the Cyber Workforce Through Innovative Hiring and Training

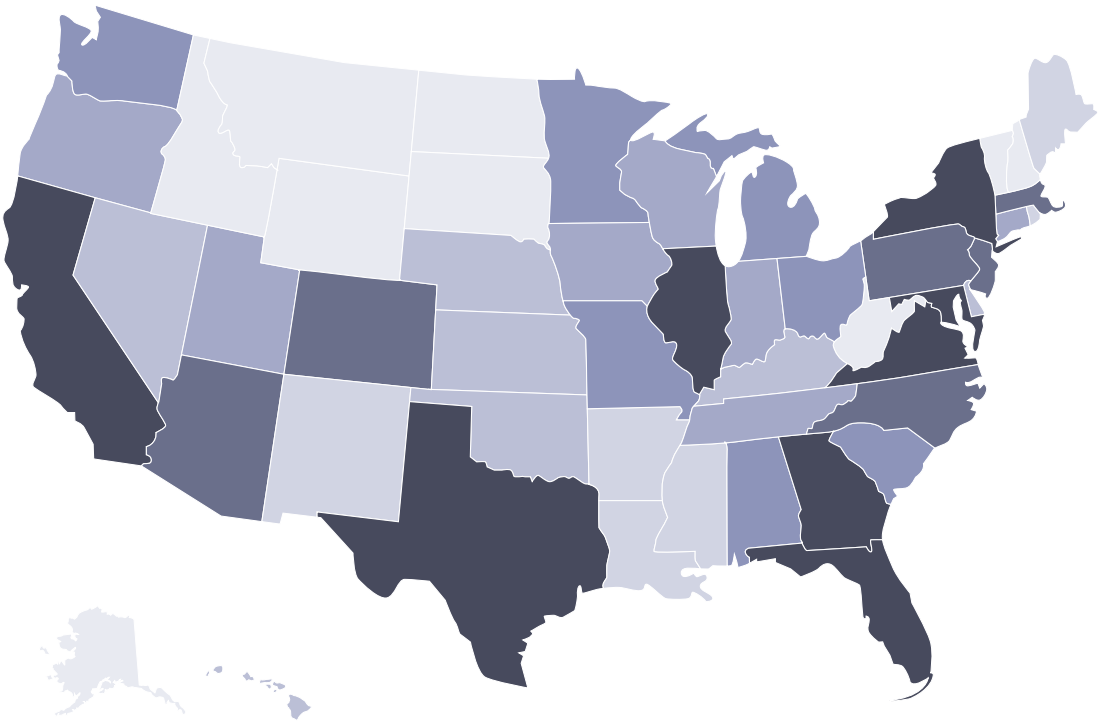
Globally, projections suggest there will be a cybersecurity workforce shortage of 1.8 million by 2022, according to a May 2018 joint report to the President from secretaries at the Commerce and Homeland Security departments.

"Positions needing to be filled range from entry-level jobs that can be performed by high school graduates who have received additional training through coursework, apprenticeships, or on-the-job experience, to the most knowledge-dependent, requiring advanced degrees coupled with lengthy on-the-job experience," the report found.

But despite the need for a wide range of talent, there's concern about the abundance of mid-level openings, most of which require a bachelor's or master's degree and at least three years of experience, according to that same report. This suggests that "creating more entry-level jobs would offer opportunities for acquiring and developing talent."

At the federal level, agencies are just starting to gain some clarity around the size and critical needs among the cybersecurity workforce, per a 2015 law and accompanying Office of Personnel Management guidance.

But when it comes to hiring, there is no standardized, governmentwide assessment for validating employees' skills, which can be challenging if hiring managers aren't adept at identifying a candidate's technical competencies. Other roadblocks include competition from other public-sector agencies and private companies, hiring freezes, and modest compensation packages. Despite these challenges, some agencies are making progress to improve hiring and employee training.



Between April 2017 and March 2018 there were 301, 873 online job postings for cybersecurity-related jobs, according to Cyberseek.

Source: Cyberseek.org

Maine, Delaware, HHS Tackle Cyber Workforce Challenges

Connecting with the right job candidates can be one of the most challenging aspects of recruitment and hiring, especially when attracting highly in-demand cybersecurity professionals.

Maine CIO Jim Smith isn't looking to just woo talented, mid-career and senior professionals to work for the state. He is relying heavily on better branding and a structured and professionalized internship program. It has led the state's Office of Information Technology (OIT) to hire 78 percent of its interns to fill full-time positions since the program launched in 2013. Interns are assigned mentors and given hands-on, impactful work.

Grooming talent is a key part of Maine's IT workforce efforts. "[Twenty-five] percent of OIT employees will be eligible to retire in the next two to three years; that equals almost 1,700 years of State of Maine I.T. experience," according to the department's 2017 annual report.

Smith is also partnering with the state's largest employers to create a cybersecurity apprenticeship program. Although it's still in the discussion phase, Smith believes the program holds great promise for the state's public- and private-sector organizations. "Maine companies are spending money right now trying to train their own, so why not create a unified approach to that?" Smith said. "And the apprenticeship is really an earn-while-you-learn type of thing. So, you have a formal training program, but you also employ the person, and they work for you part-time."

Nationwide, there's a big push for government, industry and academia to align in other ways, too. The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework is one example. "[It] establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed," according to NIST, which leads the effort.

At the Department of Health and Human Services, CIO Beth Killoran and her team are using the NICE framework to create position descriptions, competency-based performance plans and individual development plans that employees can opt to use. The focus is on creating a library of standardized materials around nearly 30 cyber-related roles that Killoran's team has identified as most common across the organization.

These reusable templates will not only save hiring managers time and ideally improve the quality of candidates, but they will also help employees better map their career paths and identify what competencies, certifications or credentials are most common for specific roles.

But what about governments that are experiencing a slow or no-growth period? Take Delaware, for example. The state is using its resources to train talent and equip them to meet its most pressing cyber needs. The state's Department of Technology and Information offers an annual boot camp to prepare employees to take the Certified Information Systems Security Professional exam — an independent information security certification.

More than 100 people have gone through the boot camp in the past five years. State employees get priority, with remaining seats going first to local and county government employees, then to university students, and then to private-sector partners, said Elayne Starkey, shortly before announcing her retirement as the state's CSO in July 2018.

The state also offers a shadowing program in which employees from other departments can come to the central IT department and get a feel for the type of work being done and see if anything sparks their interest, Starkey said. Employees who need additional training for cyber roles can take free courses using DTI's website outside normal work hours.

Success Factors

1 **Professionalizing internship programs improves the quality of candidates, making it an effective recruitment tool.** As much as possible, try to align the intern selection process and project assignments with the method used for full-time employees.

2 **Look for opportunities to partner with federal agencies** such as DHS that may offer funding and expertise to help you develop your workforce through training and other means.

3 **Familiarize yourself with NICE to gain a national view of cybersecurity activities underway.** NICE often opens the door to collaboration by connecting organizations that are working on similar efforts.

How Federal Cybersecurity Standards Reach State, Local Governments

An Interview with Shawn Wells, Chief Security Strategist, U.S. Public Sector, Red Hat

Government agencies have long battled with how to operate efficiently while innovating effectively for the future. Technology advancements have made iterating through experimentation relatively inexpensive, helping learning and innovation occur faster.

Cybersecurity is often viewed as a hindrance to experimentation and innovation. The federal government has recently invested significantly in modernizing cybersecurity best practices in frameworks applicable to all its agencies in key areas, including procurement, configuration management and continuous information technology monitoring.

State and local governments can now accelerate their innovation and learning by aligning their cybersecurity approaches more closely with their federal counterparts. Such frameworks provide federal, state and local agencies with a common roadmap to more robust cybersecurity nationwide.

"Everybody recognizes that cyber events are happening," Shawn Wells, Red Hat's Chief Security Strategist, U.S. Public Sector, told GovLoop during a recent interview. Red Hat is a leader in secure, open-source software solutions. "Regardless, not every agency can stand up a cybersecurity operation and staff it."

Agencies must subsequently determine what tools, techniques and practices can help fill that gap and decide how insights can be shared across government. One of the biggest barriers is often costs. "Three immediate opportunities for reuse include Common Criteria, which helps shift cybersecurity into technology procurements, the National Institute for Standards and Technology's (NIST) National Checklist Program (NCP), which provides secure configuration guidance and government tools such as the Homeland Security Department's Automated Indicator Sharing program (AIS)," Wells said.

The Federal Aviation Administration (FAA), for example, was once burdened with verifying security system components after receiving them from system integrators. FAA Information Assurance teams would often find the solution lacking after issuing contracts during final acceptance testing, with money already spent and little time for addressing cybersecurity concerns.

When the FAA released contracts to build a centralized security dashboard, it included clauses restricting system integrators to Common Criteria Certified components. Common Criteria is an internationally recognized process for evaluating security features of commercial technologies. Once the technologies pass an audit by a NIST-validated laboratory, they are listed in the federal "Product Compliant List." Agencies then have assurance that those technologies meet government security requirements.

State and local organizations can also incorporate Common Criteria into software procurements, which saves time by providing a high degree of trust in a product's cybersecurity. Wells added that Common Criteria policies are developed through open source initiatives lead by the National Security Agency (NSA). Agencies can share their experiences with one another, refining cybersecurity standards for the broadest, strongest protections.

"The Common Criteria process validates technology, such as ensuring secure multi-tenancy of virtualization and container platforms, but also considers how the vendor develops that technology," Wells said. "Auditors are sent to vendor facilities to ensure both secure software development practices and the physical security of where the software is developed. In 2016, Red Hat became the first provider of a Common Criteria Certified Linux container framework. State and local agencies can now bring innovations to production faster by building on this trusted foundation."

Agencies can also use the NCP, which curates secure configuration guides for hardening commercial technologies to government standards. The NCP is a "publicly available resource that contains information on a variety of security configuration checklists for specific IT products or categories of IT products," according to NIST.

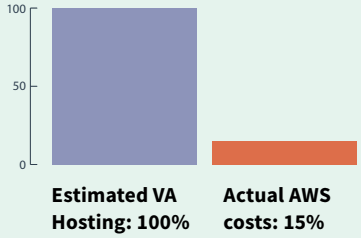
NCP checklists help protect government agencies by listing instructions and procedures for configuring IT products to specific operational environments. Many include tailored guidance for state and local governments, such as specialized baselines for criminal justice systems. They also identify unauthorized changes to a product and whether it's properly configured.

"Common Criteria validates commercial products' security features, and the NCP complements this process by ensuring agencies have configuration guides that ensure technologies can be deployed securely," Wells said. "Agencies know instantly if software vendors meet their security control standards, saving them valuable time historically spent attempting to harden procured technologies."

All government agencies must perform efficiently without overspending or sacrificing cybersecurity. Red Hat helps with secure, stable open source software capable of being deployed in data-sensitive environments while driving mission successes.

Cybersecurity must be baked into everything an agency does. Best practices and standards boost consistency across federal, state and local agencies to ensure that data is protected and that organizations can still innovate and modernize their systems.

Cloud cost savings of 85% vs. internal VA hosting

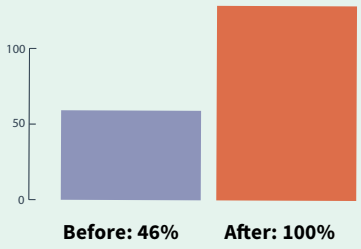


Number of Vets.gov accounts

424,467

that have been secured to the highest level of federal certification (LOA3) against fraud, abuse and cyberthreats

Pages optimized for viewing on mobile devices

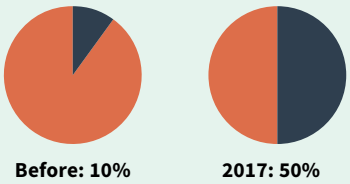


Accessibility and 508 compliance targets

100%

daily automated testing of all Vets.gov features to enforce their accessibility to users of assistive technology

Percent of the approximately 600,000 annual healthcare applications completed online



Days in VA release cycle

This is a snapshot of various improvements that have been achieved through the use of DevSecOps, including daily software releases that used to take as much as three months.
Source: Vets.gov

Breaking Down Barriers and Improving Collaboration Using DevSecOps

Managing a seamless and secure IT enterprise is no small task in today's complex environment.

For starters, your agency relies on a host of systems and applications to meet daily demands from internal and external customers.

Ensuring that those systems are updated with the latest code, operating smoothly and running securely requires a joint effort across multiple teams. But those teams' varying missions can clash at times.

Developers work to push code that corrects glitches, providing user enhancements and fixing software vulnerabilities. The IT operations team keeps these systems running and functional for the hundreds or thousands of people who depend on them. And equally important is the security team that must ensure the same systems are secure, up-to-date and compliant with federal standards.

To bridge the divide between development, operations and security teams and ensure that systems stay updated, running and secure all at the same time, agencies are investing in a new approach known as DevSecOps. At its core, DevSecOps is "a cultural and engineering practice that breaks down barriers and opens collaboration between development, security, and operations organizations using automation," according to the General Services Administration's definition. The focus is on rapid, frequent delivery of secure infrastructure and software to production, which a growing number of agencies are prioritizing.

The purpose and intent of DevSecOps is to build on the mindset that everyone is responsible for security with the goal of safely distributing security decisions at speed and scale, according to Shannon Lietz, founder of the DevSecOps Foundation, a community focused on incorporating security within Agile and DevOps practices.

VA, USDA's Food Safety and Inspection Service Share Their DevSecOps Journeys

DevSecOps is still in its infancy across government, but at the Veterans Affairs Department, digital service experts have been using this approach to manage and improve major cloud-based applications such as Vets.gov and Caseflow, an internal-facing application that helps lawyers develop cases for veterans' benefits appeals.

"DevSecOps to us is just an iteration off of DevOps, and it's kind of this additional culture of security…permeating everything that you do," said Aaron Wieczorek, a Digital Services Expert at VA. The goal is to integrate these best practices across VA and even influence policies that are more compliance-driven and less rigorous than the continuous integration of security and deployment of new features that DevSecOps offers.

Before DevSecOps, releasing software updates would take upward of three months. "[Today], every one of our releases is in the release cycle about a day, and the reason we're able to do that is because we've proven that this is a… secure way of doing things," Wieczorek said. "DevSecOps helped us achieve this."

He credits these advancements to the strong relationship his team has built with the stakeholders who approve code releases. Because the digital service team has proven the efficacy of DevSecOps, others are more trusting of it and willing to embrace it. Agile is at the heart of these efforts, so changes are small, iterative and immediately correctable if needed.

DevSecOps empowers VA to address vulnerabilities as soon as humanly possible and keeps users' data secure, Wieczorek said. For example, when the computer chip vulnerabilities Spectre and Meltdown were discovered — putting most of the world's computers at risk — VA's digital service team was in better shape than many others. "Because we were practicing DevSecOps, within two days Amazon Web Services released an update to their underlying machine images that we use for our servers, and they automatically got updated," Wieczorek said.

At the Agriculture Department's Food Safety and Inspection Service (FSIS), CIO Janet Stevens and her team took a hard look at factors that affect the agency's mission and how they could integrate ongoing efforts such as IT modernization and the creation of Centers of Excellence at the department.

"[There's] a lot of activity there, plus we're just looking at how can we deliver as quickly as possible, as securely as possible, and stay in line with what our business needs are," Stevens said.

"We felt we needed to reorganize, but of course, how do you do that? You don't want to just try to wing it," she added. Through much research, feedback and internal conversations, FSIS decided DevSecOps was the best way forward, and they are gradually adopting this new approach.

FSIS defines DevSecOps in terms of orchestration, or everything working in unison, Stevens said. Among the questions the team is considering is how FSIS' designs, processes, structure, tools, resources and workforce align through orchestration.

"As we do less and less ops here…we need to get all those service providers — telecom, everybody — into this process," she said. The real work is underway now as FSIS moves beyond conceptualizing DevSecOps to embedding it into the agency's DNA. This will require integrating teams, new roles for some employees, renaming divisions and more.

Because DevSecOps is more about culture and change management than it is about new security tools, Stevens is keeping the focus on people by talking about DevSecOps in terms of what the changes mean for employees, the customers they serve and overall agency operations.

As the agency better aligns to adopt DevSecOps, Stevens encourages employees to keep this in mind: Mission first, people always.

Success Factors

1 **Make people the priority.** You can talk about different structures, concepts and frameworks for DevSecOps all day, but until you focus on the human element you won't be successful. Internal and external customers need to understand how DevSecOps affects them.

2 **DevSecOps is not only a tech term, it is a transformation in the way agencies develop, operate and secure data, applications and infrastructure.** Before diving into DevSecOps, consider what silos may prevent teams from collaborating and what organizational changes may be necessary.

3 **Look to other organizations for inspiration.** GSA, for example, released a DevSecOps guide that describes at a high level the expectations, scope of responsibilities, maturity model and metrics associated with any DevSecOps platform at the agency.

CenturyLink®

CenturyLink Network Security

Securing Government IT Today for a Better Tomorrow

Cyberthreats are persistent and stealthy. CenturyLink tracks nearly 200,000 threats per day that impact over 100 million unique targets.[1] We help agencies and organizations proactively thwart threats before they become security breaches.

Benefits of the CenturyLink Security Portfolio:

- Managed Security Services, E3A, ECS, MTIPS, DDOS, NBS(ANS), CDM
- Limit exposure to cyberattacks with multi-layered security services
- Comply with government cybersecurity and connectivity policies
- Identify cyberthreats with threat intelligence, monitoring, detection and mitigation
- Analyze cyberattacks with analytics and threat management services

CenturyLink solutions are available on multiple, approved government contract vehicles including:

- Enterprise Infrastructure Solutions (EIS)
- General Services Administration (GSA) IT Schedule 70
- Networx Enterprise and Universal
- Alliant 2
- WITS 3
- Connections II, plus more

As a network provider, we are positioned to protect customer data before it gets to the customer premise.

Resource 1: CenturyLink 2018 Threat Report, CenturyLink Threat Labs.

Call **1.886.9FEDNET** or visit **centurylink.com/federal** for contract information.

Enhancing Government Cybersecurity With Managed Services

An Interview with Dave Young, Vice President for Strategic Government, CenturyLink

There's no shortage of policies, regulations and standards outlining how agencies should protect the government's most critical systems and data.

In fact, over the past several years the Government Accountability Office (GAO) has made about 2,500 recommendations for federal agencies to enhance their information security programs and controls, according to a 2017 GAO report.

"The challenge seems to be execution," David Young, Senior Vice President for Strategic Government at CenturyLink, said in a recent interview with GovLoop. "With that lens, you look at funding, staffing and training. There is a lot of work that needs to get done, so finding ways to speed that up is essential."

As a major player in the critical infrastructure space, CenturyLink works closely with government agencies to lower their cybersecurity risks, improve compliance and protect their assets using flexible and cost-effective IT security solutions. But part of the challenge for companies and their government customers is trying to keep pace with constantly evolving cyberthreats while wading through regulatory hurdles. These impediments include burdensome acquisition and operational compliance requirements that slow the adoption of critical cyber capabilities, Young said.

Young highlighted two Homeland Security Department programs that are enabling agencies to target malicious cyberthreats. Under the Einstein 3 Accelerated (E3A) program, CenturyLink is one of few approved internet service providers that supports near real-time inspection of federal network traffic and then blocks any known or suspected cyberthreats.

Through DHS's Enhanced Cybersecurity Service (ECS) program, CenturyLink uses threat indicators provided by the government to augment critical infrastructure companies' existing capabilities. Specifically, this managed service offering allows owners and operators of critical infrastructure to block access to specific malicious domain names and stop emails with specific malicious criteria from entering a network.

Such programs are vital for agencies and critical infrastructure operators considering that most email antivirus programs catch, on average, only 45 percent of cyber criminal activity, leaving organizations open to risks like phishing, bots and other social media engineering techniques.

"Our security portfolio provides layers of enhanced cybersecurity protections to protect customer data from computers to the cloud," Young said.

CenturyLink also partners with agencies through its Managed Trusted Internet Protocol Service (MTIPS), which enables agencies to physically and securely connect to the public internet while complying with federal security requirements.

But agencies should not be satisfied with simply checking a box to meet security requirements. They must constantly examine changing cyberthreats and work with their internal and external partners to respond accordingly.

In terms of capacity and the demand that cybersecurity puts on the workforce, having access to managed services like those offered by CenturyLink provides agencies with cyber capabilities that are immediately operational and cost-effective, especially for smaller agencies, Young said.

"Cyberthreats adapt very quickly, and keeping pace is hard enough," Young said. "That's why more communication is necessary."

Partnerships, such as participating in the President's National Security Telecommunications Advisory Committee (NSTAC), are one example of how the public sector is working closely with the private sector, including CenturyLink, to share important insights that can improve the availability and reliability of telecommunication services.

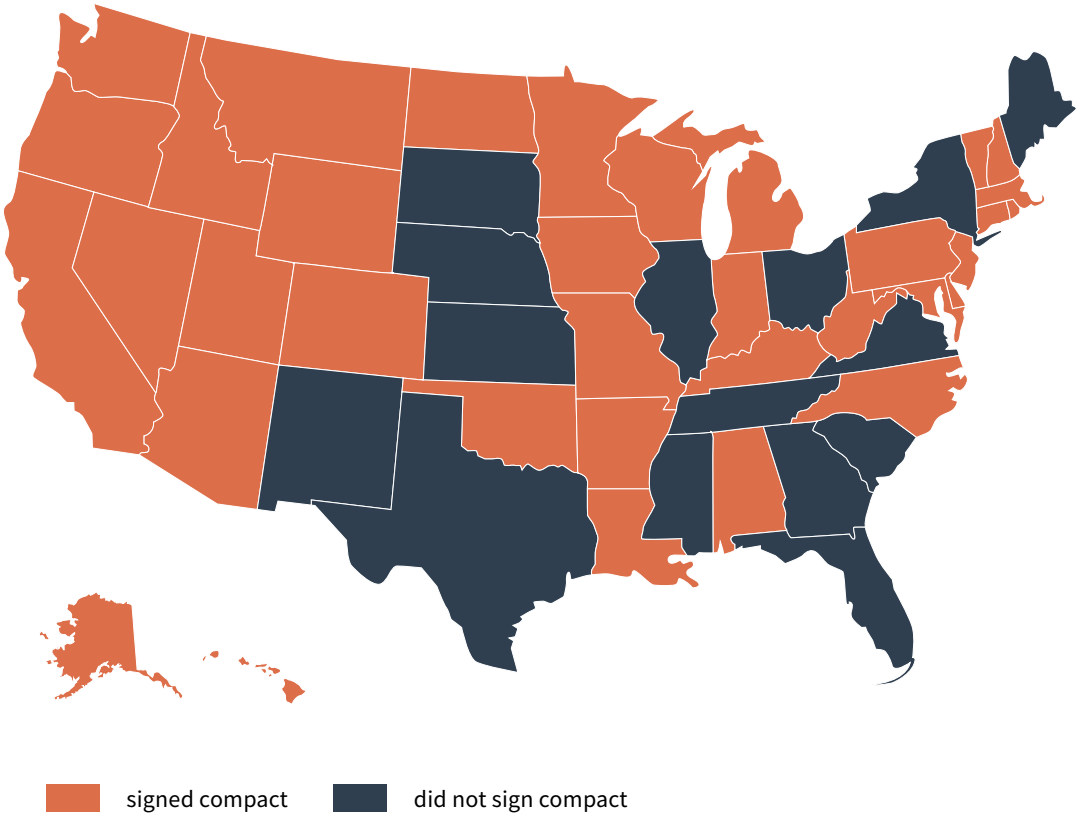
CenturyLink also has its own threat lab, which was designed to provide customers with consumable information that gives organizations increased situational awareness and helps them align their cyber capabilities with active threats around the world.

In addition to improved information sharing, there are promising solutions that agencies should have on their radar as cybersecurity continues to evolve. But as with any new capability, it takes time for these technologies to mature.

"For example, network function virtualization is a great way to deliver capabilities in the network, where they are consumed," Young said. "Because of the inherent virtualization and the decoupling of capability from hardware, there is a quicker turnaround time for delivering the capabilities that our customers want and demand."

The key for agencies is finding the right balance that enables them to meet rigorous federal standards while still having the flexibility to quickly adapt to cyberthreats.

"Anything that impedes the loop from capability to deployment needs to be examined very carefully," Young said. Once agencies identify and remove these barriers, they can focus their time and resources on adopting capabilities that meet their most pressing cyber needs.



This map highlights the 35 states where governors signed a compact in 2017 aimed at improving cybersecurity across the U.S.

Source: National Governors Association (NGA)

Strengthening Security Through State and Local Partnerships

A cyberthreat against one is a cyberthreat against all, especially for state and local governments. They are increasingly uniting against their common enemies to boost their mutual cybersecurity postures. And the foes are many: hackers, ransomware, viruses and more.

A ransomware attack struck the Atlanta city government's computer services in March 2018, disrupting programs that residents use to pay their bills or request new water services online. Wired reported in April 2018 that Atlanta spent more than $2.6 million addressing the debilitating incident.

Local governments are no safer than their statewide counterparts, a December 2017 ransomware attack on Mecklenburg County, North Carolina shows. The disruption interrupted county services for roughly a month, with residents unable to pay property taxes, register deeds and more.

State and local governments are increasingly entering into cybersecurity partnerships that transcend physical boundaries. These alliances foster better information sharing, improved cooperation on cybersecurity challenges and increased dialogue about best practices.

The Center for Internet Security (CIS), a nonprofit organization aimed at helping "safeguard private and public organizations against cyberthreats" worldwide, is helping lead that charge. CIS' MS-ISAC offers one example of how states can overcome cybersecurity challenges by working together.

"The mission of the MS-ISAC is to improve the overall cybersecurity posture of state, local, territory and tribal governments," according to the group's website. "Collaboration and information sharing among members, the U.S. Department of Homeland Security (DHS) and private sector partners are the keys to success."

A September 2016 Deloitte/NASCIO survey found that 96 percent of state enterprise-level CIOs and state business officials said they are collaborating with MS-ISAC. Ninety-two percent said the same of local government entities and DHS fusion centers.

America's cyber health improves when state and local governments team up, with the various parts strengthening defense of the whole.

Governors Unite on Compact to Improve State Cybersecurity

Cybersecurity threats prompted 38 governors to sign a compact in 2017 aimed at improving their states' cyber defenses.

A Compact to Improve State Cybersecurity pledges to improve states' cybersecurity governance, prepare and defend them from cyberattacks, and grow the U.S. cybersecurity workforce.

"Cyberthreats pose serious risks to the core interests of all states and territories," it reads. "Recent cyber intrusions have stolen volumes of confidential data, exposed critical services to disruption and resulted in significant economic impacts to states."

"States are attractive targets because they collect and store massive amounts of personal and financial data," the compact adds. "In short, cybersecurity is a whole-of-state affair that requires high-level executive engagement."

Cambray Crozier, Communications Director for Minnesota's CIO, said Gov. Mark Dayton's decision to join the compact last year has helped strengthen interstate and national cybersecurity.

"One great thing about this compact is it is a commitment of governments across the nation," she said. "It helps us work together across local governments, state governments and the federal government."

"This gives us the opportunity to share information with other governors and learn lessons from one another," Crozier added. "This really delivers value not just for Minnesota but all states."

Crozier said Minnesota faces more than 3 million cyberattacks daily, potentially endangering the state's 35,000 government employees and 5.5 million residents.

The compact addresses such challenges by tasking the states involved with "creating and exercising cybersecurity disruption response plans that emphasize a whole-of-state approach."

Ryan Aniol, Minnesota's Deputy CISO, said the pact has helped the state communicate more effectively with partners about cybersecurity challenges.

"If another state is in a cyberattack, being able to diverge that to your partners is critical," he said. "It's really understanding what the threats are today, how they impact us and where are they going."

"Being able to share that with other states helps improve the cybersecurity posture of the country," Aniol continued. "It's being ahead of the curve."

The compact also commits signers to "growing the nation's cybersecurity workforce," a pledge Crozier said Minnesota is enthusiastically keeping.

"Minnesota, like many states, has both a challenge and an opportunity related to the IT and cybersecurity workforces in our state," she said. "[We're] looking for ways we can grow the talented total workers in our population."

"That's not something we do alone," Crozier added. "We do it side-by-side with private companies, our universities and even focusing on STEM (science, technology, engineering and mathematics) in our education system."

Minnesota contributes to America's cybersecurity workforce by recruiting graduates of the National Science Foundation's CyberCorps Scholarship for Service program, which "provides scholarships to students for cybersecurity-related degree programs at select two- and four-year colleges and universities in return for service in Federal, State, local or tribal governments upon graduation," according to the initiative's website.

Aniol said the program has helped Minnesota by helping prepare the state's next generation of cybersecurity defenders.

"It helps us bring in the door a really talented workforce," he said. "It's a really great win-win for everybody involved."

Success Factors

1 **Share cybersecurity successes, failures and threats** with other governments at the federal, state and local levels when possible. A clear, free-flowing information-sharing network keeps partners invested in one another's cybersecurity needs.

2 **Secure the support of government leaders** who can represent your efforts to partners and increase investments in your cybersecurity efforts.

3 **Bring academia and the private sector into the equation** to connect your organization with cybersecurity ideas and talent.

Government-Grade Cloud: The Right Mix of Security, Standards

An Interview with Jose Padin, Public Sector Chief Technology Officer, Citrix

Government agencies adopting the cloud face the challenge of maintaining strong cybersecurity while meeting strict federal standards for doing so.

Data ranks among an agency's most precious assets, so protecting it from cyberthreats is vital. Federal guidelines subsequently urge agencies to make data security a priority of successful cloud adoption. Government-grade clouds help thread this needle by offering the cloud's many benefits at the federal government's formal cybersecurity benchmark.

In a recent interview with GovLoop, Jose Padin, Public Sector Chief Technology Officer at Citrix, outlined the benefits of a government-grade cloud and how Citrix is supporting agencies. Citrix is a secure workspace and networking company whose Citrix Cloud Government maintains robust cybersecurity on top federal compliance and regulatory standards.

Among the chief benefits of government-grade clouds is that they help agencies manage their growing mission compute needs while remaining nimble and well-shielded from cyberthreats. "We have many government workloads that generate a ton of storage," Padin said. "That data is very important and needs to be secured at a very high level. Hosting data in the cloud gives agencies the ability to grow as quickly as their needs evolve — and those needs change dynamically."

Agencies using Citrix Cloud Government can use any government-grade infrastructure, quickly access mission-critical applications from any device and have a solution that meets federal security requirements.

Ultimately, agencies are freed up to focus on their mission, Padin said. "We manage the core infrastructure to get a secure digital workspace up, running and functional to allow the government to shift and allocate resources for more important mission-focused areas as opposed to standard infrastructure maintenance."

A true government-grade cloud should meet requirements set by the Federal Risk and Authorization Management Program (FedRAMP), which sets governmentwide protocols for security assessment, authorization and continuous monitoring of cloud-based services and infrastrucsture.

Padin said Citrix Cloud Government runs on FedRAMP-authorized infrastructure and has much of the same functionality that users can get from commercial-grade cloud solutions. Some of the FedRAMP requirements that cloud vendors must meet include developing a security awareness and training policy and drafting a strategy for eliminating cybersecurity flaws.

"You get high-grade security, elasticity and compliance that meets the government's needs through FedRAMP accreditation in these clouds," Padin said of government-grade clouds. "You get the best of both worlds."

Citrix Cloud Government and other government-grade clouds are capable of defending web applications from dangerous cyberthreats like denial-of-service attacks. Such platforms can also quickly recover from disasters and create a secure bring-your-own-device (BYOD) program by managing data rather than the underlying tool.

Padin noted that government-grade clouds also help agencies reduce spending and IT infrastructure management. "It gets them out of the day-to-day business of managing hardware, keeping hardware up-to-date and worrying about large-scale upgrades that over the lifetime can cost agencies and taxpayers," he said.

These FedRAMP-approved cloud infrastructures support virtualized workloads that are high performance, reliable and secure. Data remains isolated from remote connections, safeguarded from hackers and unmanaged devices.

Government-grade clouds enhance agencies' flexibility by securely providing mission-critical applications abstracted from endpoint devices. Employees then experience uninterrupted, high-level, secure access while using such platforms as they switch devices, locations and networks.

Agencies have sometimes struggled with cloud adoption because legacy systems are hosted on-premise and are often costly and can be difficult to migrate to the cloud. Padin said that Citrix Cloud Government gives agencies a platform for securely leveraging their current on-prem deployments while migrating to the best government-grade cloud infrastructure for their needs.

"They have the choice and flexibility to use any type of cloud and on-premise solutions that meet their agency's specific needs," he said.

Padin added that government-grade clouds help organizations save money without sacrificing cybersecurity. In addition to security, one of the biggest benefits of moving infrastructure to the cloud is reducing operations and management costs. They can also make use of faster speeds dynamically as needed.

"Moving a traditional desktop to a secure digital workspace in the cloud allows the end user to continue to have a seamless experience," Padin added. "It allows the user to reap the benefits of increased security and flexibility, and it enables them to spend more time focused on their mission."

Conclusion

There's no single approach to cybersecurity that will resolve the range of challenges agencies face, but advancements in key areas such as AI and DevSecOps are helping to fill gaps in their security efforts.

The combination of modest cyber workforce sizes, limited budgets and more sophisticated attacks is forcing agencies to invest resources in areas that allow them to reap the most benefits. For example, cities such as Las Vegas are using AI to augment their in-house staff. With DevSecOps, agencies are releasing securer code faster, which leads to better internal procedures and improved services for users.

On the workforce front, agencies at all levels are making strides to improve how they hire and train the workers who will implement these new technologies and adopt new processes.

As agencies mature their security programs, expect to see an increased reliance on secure, digital and repeatable processes that free up security professionals to tackle more high-level tasks. You can also expect to see an increase in partnerships across state, county and city lines.

About GovLoop

GovLoop's mission is to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 270,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop

Thank You

Thank you to BeyondTrust, CenturyLink, Citrix, Red Hat, and Tanium for their support of this valuable resource for public-sector professionals.

Authors

Nicole Blake Johnson, Managing Editor
Mark Hensch, Staff Writer

Designer

Megan Manfredi, Junior Designer

govloop

1152 15th St. NW Suite 800

Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501
www.govloop.com

@GovLoop