carahsoft The Trusted Government IT Solutions Provider®

Cybersecurity Buyer's Guide **for Government**

Discover cybersecurity solutions that empower agencies to stay compliant, secure, and resilient against evolving threats.

FEATURING: ***Solution Areas*** • ***Success Stories*** • ***Policies & Executive Orders*** • ***Contract Vehicles*** • ***Upcoming Events***

carahsoft The Trusted Government IT Solutions Provider®

Securing Government Systems with Trusted Cybersecurity Solutions

Explore Carahsoft's extensive portfolio of cybersecurity products and services designed to protect government infrastructures, networks, and assets. Our solutions empower agencies to mitigate risks and ensure compliance with proven technologies from leading vendors.

Discover which cybersecurity vendors align best with your organization's goals, offering solutions in Cloud Security, Supply Chain Risk Management, Identity & Access Management, and more.

Scan below to access case studies, contract vehicles, upcoming cybersecurity events, helpful resources, and more.

©2026 Carahsoft Technology Corp. All Rights Reserved.

Welcome to the Cybersecurity Buyer's Guide!

The cybersecurity market continues to thrive as a top priority for CIOs and senior leadership across all sectors. From protecting commercial enterprises against reputational damage and financial loss to protecting national security and ensuring the safety of our healthcare systems, the importance of cybersecurity has never been more evident. As cyber threats grow in complexity and persistence, the cybersecurity market continues to evolve and advance through constant innovation. Despite the ongoing cyber skills gap and talent shortage, organizations are making strides by investing in smarter technologies, strategic partnerships, and workforce development.

The cyber landscape is highly fragmented with thousands of products and services designed to address a wide range of challenges to keep an organization's data, systems and networks secure. While prevention and protection remain foundational, the focus has shifted towards prioritizing cyber resilience to ensure quick recovery and response with minimal operational disruptions.

Carahsoft has built one of the most comprehensive portfolios of cybersecurity products and services, including endpoint security, network security, cloud security, data protection, identity management, incident response, workforce training and development and supply chain security. Our expert team works with our partners to deliver tailored solutions to help our customers achieve their desired outcomes.

Brian O'Donnell
Vice President of Cybersecurity Solutions
Carahsoft

Table of Contents:

Cybersecurity Solution Areas

As Government IT modernization advances and interconnectivity initiatives expand, the need for cybersecurity solutions is more crucial than ever. Cyberattacks are on the rise across the Public Sector, which poses a significant risk to critical infrastructures, applications, networks and cloud environments.

The dedicated Cybersecurity Team at Carahsoft specializes in providing IT security solutions to Federal, State and Local Government, as well as Education and Healthcare organizations. We aim to safeguard the entire cyber ecosystem with proven technology. Our certified Government Product Specialists help our customers build comprehensive cyber solution stacks to meet evolving Government security requirements.

Carahsoft has established strategic, long-term relationships with the industry's leading cybersecurity manufacturers to offer Government entities proven, cost-effective protection for infrastructures, networks, cloud environments and assets. Our comprehensive Cybersecurity Solutions Portfolio covers the essential areas to protect your organization, including:

Network and Infrastructure:
Safeguard foundational systems

Security Operations and Incident Response:
Monitor, respond to and neutralize threats

Endpoint Security:
secure access points across all devices

Identity and Access Management:
Manage user IDs and permissions

Web and Messaging Security:
Guarantee secure online communication

Risk and Compliance:
Ensure government security compliance

Mobile Security:
Safeguard device and apps

- **Data Security:**
  Protect information data at every stage
- **IoT and Industrial Security:**
  Protect interconnected devices
- **Cyber Skills Training:**
  Enhance team's IT security expertise
- **DevSecOps:**
  Integrate security into application development
- **Quantum Security:**
  Future-proof data security and integrity from quantum decryption
- **Artificial Intelligence:**
  Accelerate risk detection, generate incident reports and automate threat response in real time

Network & Infrastructure

Network and Infrastructure solutions provide public sector organizations with preventative software and services for underlying network infrastructures to block unauthorized actions of data. Secure foundational networks and infrastructures from hackers and malware with our cutting-edge technology solutions. Select a technology vendor to learn more about their products and services.

Akamai	AppGate	ARMIS	Attivo Networks	Cloudflare	Conceal
Extrahop	f5	Fidelis Security	Forescout	Fortinet	Forward Networks
Gigamon	HYAS	iboss	illumio	infoblox	Intrusion
LiveAction A BlueCat Company	neustar	Nlyte Software	paloalto Networks	Secureworks	Skybox Security
SolarWinds Public Sector	Sophos	splunk>	Trend Micro	TrinityCyber	tufin
Veracode					

Security Operations & Incident Response

Equip your security teams with the technology to effectively minimize and prevent attack incidents, ensuring readiness for future threats. Select a provider to learn more about their security products and services.

Endpoint Security

Endpoint Security Solutions provides Public Sector organizations with advanced software design to secure devices like desktops, laptops, mobile phones and tablets from cyberattacks. Strengthen your defense strategy by safeguarding each entry point with advanced technology. Choose a provider to learn more about their security products and services.

Identity & Access Management

Identity and Access Management Solutions empower IT teams to enhance access security by ensuring that only authorized personnel with privileged access gain entry to organizational resources. Reinforce your department's security framework and streamline access with innovative IAM solutions. Choose a provider to learn more about their products and services.

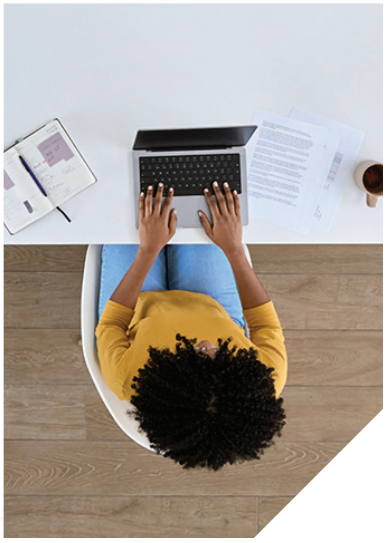
Web & Messaging Security

Web and Messaging Security Solutions offer Public Sector organizations advanced IT solutions to protect digital communications and online interactions. Protect web applications, email security and messaging platforms from threat actors. Select a provider to learn more about their products and services.

Risk & Compliance

Risk and Compliance Solutions enable organizations to manage and address security risks while ensuring Government compliance. Improve your department's security posture and regulatory compliance efforts. Choose a provider to learn more about their products and services.

anchore | AvePoint | BLACKDUCK | BLACKWIRE | caveonix | CIMCOR
cloudcover | CLOUDFIT SOFTWARE | COHESITY | CoreView | CYTELLIX | CYTURUS
druva | FLASHPOINT | flexera | ivanti | Kion | NextgenID
ninjaOne | Onspring | opentext | privaini | Qualys | RACKTOP
RAPID7 | RegScale | runZero | SafeLogic | secpod | SecurityScorecard
sonatype | splunk> | stackArmor | SYNERGIST TECHNOLOGY | TANIUM | tenable
THREATLOCKER | Trustwave Government Solutions | TYCHON | VERITAS | VulnCheck | WIZ
XM Cyber

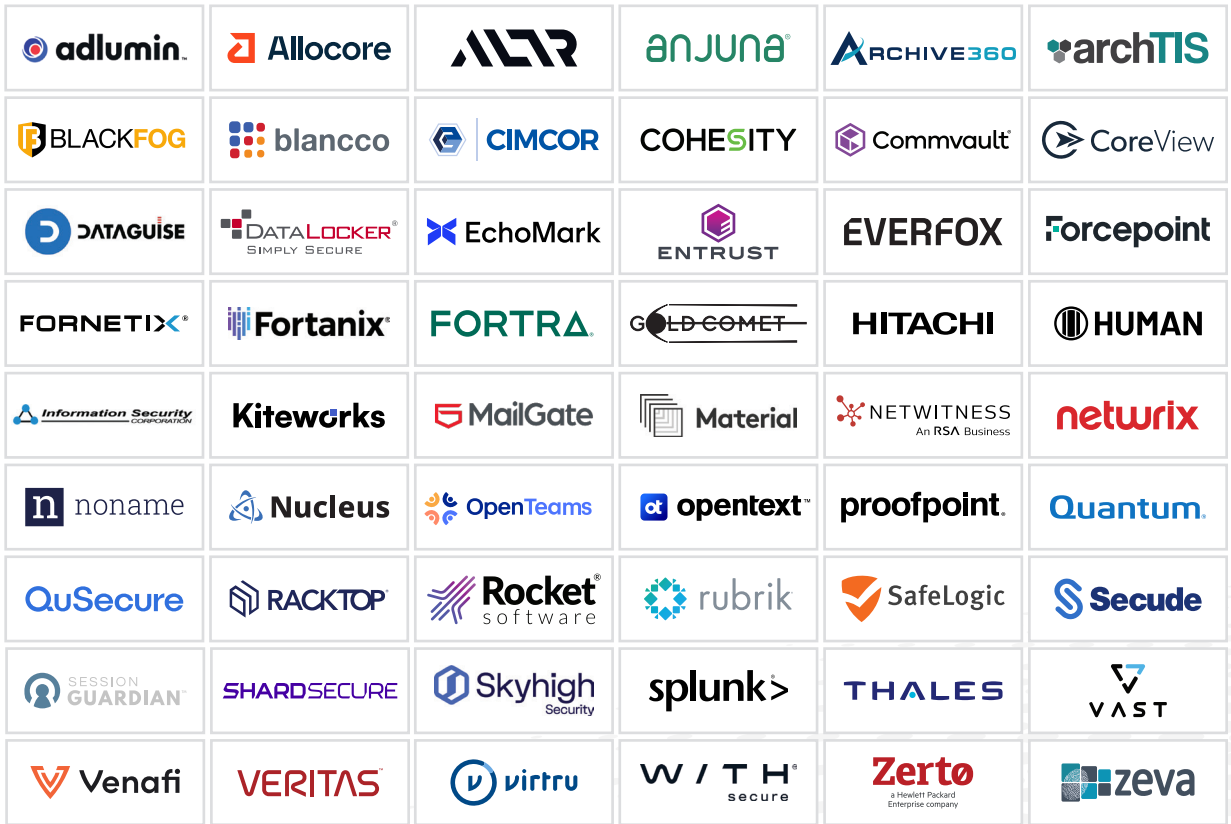


Mobile Security

Mobile Security Solutions ensures that the Public Sector has the technology resources to secure mobile devices against cybersecurity vulnerabilities. Safeguard sensitive apps and data on company phones and tablets from unauthorized access. Select a provider to learn more about their products and services.

Data Security

Data Security Solutions equips the Public Sector with innovative solutions to secure sensitive information and data. Ensure critical data remains protected from unauthorized access or breaches. Select a technology vendor below to learn more about our leading Data Security products and services.



IoT & Industrial Security

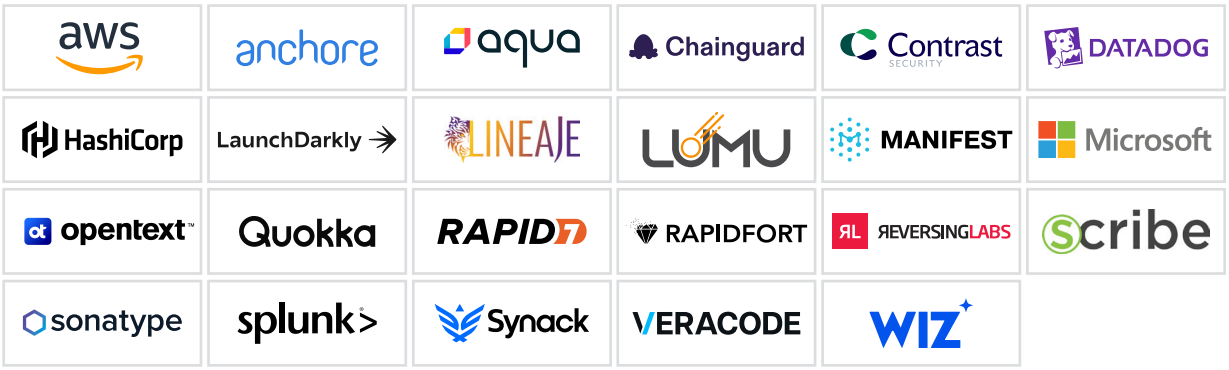
IoT and Industrial Security Solutions provide comprehensive protection for industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. Ensure your security team has the resources to safeguard your connected devices, data and systems from unauthorized access and cyber threats. By implementing industrial-grade security protocols from the start, you can mitigate risks, ensuring the smooth operation of your industrial processes. Explore below to discover leading IoT and Industrial Security products and services.

Cyber Workforce Development

Cyber Skills Training Solutions empowers security teams with advanced training solutions to enhance their skills and knowledge. Equip your team with the latest techniques, strategies and best practices to stay ahead of evolving threats for the most effective defense from cyber threats. Choose a provider to learn more about their products and services.

DevSecOps

The DevSecOps segment equips development teams with tools and best practices that prioritize security throughout the software development lifecycle. Embed security at every stage to deliver secure applications. Choose a provider to learn more about their products and services.



Quantum Encryption Security

Quantum Computing Security Solutions are preparing Public Sector organizations for the threats related to quantum computers. Future-proof your critical infrastructures from potential decryption with quantum-safe cryptographic solutions and services. Choose a provider to learn more about their products and services.

Artificial Intelligence

Empower your Security Teams to accelerate threat detection, expedite incident response times and generate comprehensive incident reports instantly with AI-powered solutions. Proactively secure data and systems from cyber attacks to quickly adapt and evolve against ever-changing threats. Select a provider to learn more about their products and services.

Cyber Threat Intelligence

Enable security operations teams to detect cyber threats quickly and accurately across enterprise and mission environments. Improve visibility into adversary activity, reduce risk exposure, and protect sensitive data and systems from cyber threats. Explore providers to learn more about their threat detection solutions.

PenTesting

Support cybersecurity programs by evaluating the effectiveness of security controls through penetration testing solutions. Identify exploitable weaknesses, improve risk awareness, and help protect critical systems and sensitive data from cyber threats. Explore providers to learn more about their penetration testing offerings.

Symantec™
by Broadcom

Security That's Simple, Effective and Everywhere

Depend on Symantec as the resilient, reliable and scalable foundation for your cybersecurity needs.

Explore Our Cybersecurity Solutions

carahsoft

State and Local Government Cybersecurity and IT Solutions

Traditional government IT resources face digital challenges. And success today depends on applications. F5 can help.

Explore State and Local Government Cybersecurity Solutions

- Mitigate App Vulnerabilities
- Optimize Container Management
- Inspect Encrypted Traffic for Threats
- Discover and Secure APIs
- Zero Trust Through Identity Awareness
- Mitigate Bots and Abuse

Learn more about F5's state and local government solutions here:
https://www.f5.com/solutions/us-federal-government/state-and-local-government

Success Stories

Many agencies have found success strengthening their cybersecurity posture to support their mission. Explore how other government customers have achieved their goals with the help of Carahsoft's cybersecurity vendors.

U.S. School District Prevented Insider Threats

In 2022, a large public school district in Texas with over 75,000 students was given a grade of "A" by the Texas Education Agency. A leader in educational excellence, the district provides unparalleled learning experiences designed to prepare and inspire each student to live an honorable, fulfilling life. To that end, the district's Technology Operations department is focused on creating and sustaining a best-in-class infrastructure to securely accommodate the current and next generations of digital content and tools for all stakeholders. When the department's new cybersecurity lead recognized a weakness in the district's security approach, Akamai Guardicore Segmentation helped fill the gap.

The Challenge:

The Texas school district had traditionally relied on firewalls and geofencing to keep its IT environment safe from external threats. However, it lacked a way to prevent internal threats — specifically, insiders with malicious intent. "If they could access one system, it would have been easy for them to access every other system," explained the Manager of Systems Engineering for the district.

Lacking visibility into legitimate communications between internal systems, the school district was unable to stop illegitimate, malicious east-west traffic. Recognizing the threat this posed, the Technology Operations department — comprising network engineering, systems engineering, and cybersecurity — understood the need for a comprehensive solution to mitigate risk. "We would be remiss if we didn't put in place a solution to ensure the full security of the information associated with our students and staff," the manager continued.

The Solution:

After evaluating its options, the school district selected Akamai Guardicore Segmentation. "It was one of the better solutions on the market," the manager said.

The Technology Operations department audited its environment to identify the applications and systems to be protected by Akamai Guardicore Segmentation. "We started with our tier-one applications, but the mandate was to protect all of them with the solution," the manager continued.

Guided by Akamai, the district easily and quickly ringfenced priority applications — including Active Directory and SQL Server — with precise segmentation policies to eliminate unwanted data flows between systems. The auditing and deployment process fostered cross-functional collaboration. "It was a group effort to determine how we would label devices, build out ringfences, and more. In that way, Akamai Guardicore Segmentation gave us common ground for working together closely."

Once a ringfence was in place, the school district was alerted to potential issues. "No traffic could get through unless we allowed it," explained the school district's Manager of Systems Engineering. As a result, the district felt assured the Akamai solution was immediately protecting those applications.

"Once we had a sense of traffic to and from an application, we would move to blocking mode if necessary. Akamai Guardicore Segmentation provides a straightforward pathway to phase in protection across our environment," the manager said.

"Akamai Guardicore Segmentation provides a priceless view into our environment and helps ensure our critical systems are protected from unauthorized east-west traffic. "

Manager of Systems Engineering, Texas School District

Though some applications are not candidates for ringfencing, the school district still benefited from newfound visibility into communications between those applications and others, such as Active Directory. All groups within the Technology Operations department can see data flows from and to any application that is ringfenced, essentially gaining visibility into what is happening with all systems in the environment. "Akamai Guardicore Segmentation provides an up-to-date view of how things are running and a simple way to identify unwanted traffic. Moreover, we can easily configure the solution to allow or block traffic as necessary," said the manager.

That visibility enables the network engineering, systems engineering, and cybersecurity teams to work together as needed to address issues as they arise. "When we are alerted to suspicious traffic, the Akamai solution provides the context we need to come up with a resolution that prevents what is unwanted while ensuring our environment operates as needed," the manager explained.

"We love using Akamai Guardicore Segmentation. It's easy to configure and manage and is an invaluable solution for any school district looking to protect itself from inside threats."

Manager of Systems Engineering, Texas School District

Key Takeaways:

According to the school district's Manager of Systems Engineering, Akamai Guardicore Segmentation is continually helping to thwart cyberattacks: "Malicious IP addresses hit our systems on a regular basis. The Akamai solution provides a view into unusual activity — such as unusual port activity on a web server — empowering us to block access and potential attacks."

Plus, by working seamlessly with other security tools, Akamai Guardicore Segmentation further elevates the district's security stance. For instance, the school district uses a privileged access management (PAM) solution to provide outside vendors with needed access to specific systems. Rather than allowing Remote Desktop Protocol (RDP) access to those servers, the district requires its engineering department to use the PAM solution to remotely manage servers. And Akamai Guardicore Segmentation helps prevent that RDP access.

As the school district's Manager of Systems Engineering explained, this combined security measure prevents people from remote desktopping into servers, as was possible in the past: "By using the Akamai solution to block RDP access, we can ensure no one remotely connects to our server environment."

To date, the school district has implemented Akamai Guardicore Segmentation on 375 of its 500 existing servers, and it plans to protect every application possible with the microsegmentation solution. "We are constantly rolling out new applications — sometimes as often as one per week — and from the get-go, we secure them with the Akamai solution. This gives us more confidence as we deploy new apps since Akamai Guardicore Segmentation enables us to visualize how our apps are working and communicating," concluded the district's Manager of Systems Engineering.


Akamai
Cyber Threats Evolve.
So Should Your Defense.

Gigamon®

Riverside County Adopts Zero Trust Model, Delivering Secure Services to Millions

Riverside County, the fourth-largest county in California by population, faced mounting cybersecurity challenges in protecting its vast network infrastructure and sensitive data. By partnering with Gigamon, the County significantly enhanced its network visibility and threat detection capabilities, resulting in a more secure and resilient IT environment.

The Challenge:

Riverside County, one of the largest counties in the United States, was grappling with the growing complexity of its IT infrastructure as it expanded its digital services and adopted hybrid cloud environments. With more than 40 departments relying on centralized IT support, the County faced mounting pressure to ensure high availability, visibility, and security across a sprawling network landscape. Traditional tools were no longer sufficient to manage the increasing volume of data and the sophistication of cyber threats.

The County's IT team struggled with limited visibility into east-west traffic, making it difficult to detect anomalies, respond to incidents, and maintain compliance with regulatory requirements. At the same time, operational inefficiencies and blind spots hindered their ability to proactively manage performance and protect critical services. These challenges underscored the need for a modernized, unified approach to network monitoring and threat detection that could scale with the County's evolving needs.

The Solution:

To address mounting cybersecurity and performance challenges across a sprawling IT infrastructure, Riverside County partnered with Gigamon to gain unified network visibility and enhance threat detection. Faced with limited insight into east-west traffic, tool inefficiencies, and growing security risks, the county implemented the Gigamon Deep Observability Pipeline to provide real-time, centralized visibility across its entire network environment—including data centers and remote sites.

With Gigamon, Riverside County successfully streamlined network monitoring, optimized existing security tools, and significantly reduced response times to potential threats. The deployment enabled seamless integration with third-party solutions like Splunk and Cisco, providing contextual, actionable data for faster and more accurate threat analysis. As a result, the county not only improved its security posture but also achieved greater operational efficiency and cost savings—empowering its IT team to protect sensitive public sector data while maintaining agility and compliance across all departments.

Key Takeaways:

Enhanced Network Visibility:
Riverside County leveraged Gigamon to gain deeper insight into their network traffic, enabling faster threat detection and response without overloading security tools.

Stronger Security Posture:
Riverside County leveraged Gigamon to enhance visibility into east-west traffic, a foundational step toward implementing a Zero Trust architecture by ensuring continuous monitoring and validation of network activity.

Enhanced Operational Efficiency:
By optimizing tool usage and reducing network blind spots, the county improved incident response times and reduced the load on their security infrastructure.

Cost Savings through Tool Consolidation:
Gigamon enabled the county to consolidate and streamline security tools, resulting in reduced operational costs and better resource allocation.

Scalability and Future Readiness:
The solution supported scalability to accommodate growing infrastructure and evolving cybersecurity needs, ensuring long-term adaptability without compromising security or performance.

infoblox.

San Francisco Sharpens Visibility into Network Operations to Strengthen its Security Posture with Infoblox

From the mid-19th century Gold Rush to the Summer of Love and the emergence of the tech industry in the digital age, San Francisco has long been regarded as a hub of business and technology innovation. However, this elevated global profile also makes the City and its IT infrastructure prime targets for hackers and malicious attacks.

The Challenge:

As with many municipalities in recent years, ransomware has been a core focus of the city's cybersecurity efforts. The San Francisco team has also had to cope with relentless phishing and web spoofing attacks. On a weekly basis, they see dozens upon dozens of phishing attacks, some of which could be ransomware exploits, but more often are blunt attempts to get recipients to initiate the processing of fraudulent transactions. In a similar vein, attackers have repeatedly set up fraudulent websites closely mimicking the look and feel of genuine City of San Francisco web properties. The extensive online presence of the city's web properties, including multiple pages within the core SF.GOV domain and related sites, creates a significant attack surface, especially in terms of exposure to lookalike domain exploits.

"We've seen multiple instances where attackers set up lookalike websites to pretend that they are a city organization, either for collecting personal information or for paying traffic fines and similar," said Nathan Sinclair, cyber defense operations manager for the City and County of San Francisco. "Some are amateurish and easy to spot, but many look remarkably real. We did have some security tools in place that could detect and block these types of activities, but not at the DNS layer. It was a blind spot that Infoblox Threat DefenseTM enabled us to resolve and strengthen our security posture."

The Solution:

San Francisco has been using Infoblox NIOS for many years to manage its core DNS, DHCP and IPAM (DDI) operations. However, despite being a long-time customer, Sinclair and his security team were not very familiar with Infoblox's security offerings. This was largely due to conventional IT best practices where networking teams are responsible for managing DDI infrastructure while security teams are responsible for managing security information and event management (SIEM) systems.

"With the segregation of duties we had in place, my only real exposure to Infoblox was that we'd get nominal amounts of networking data from the NIOS instance to ingest into our SIEM/SOAR stack to check for suspect traffic," related Sinclair. "But then in consulting with one of our client organization departments, they'd recently adopted Infoblox Threat Defense and gave us a demo. Immediately, we recognized that here was a solution that provides complete visibility into network vulnerabilities. It would be a powerful tool for blocking exploits, stopping incursions before they could do damage, and strengthening our defenses overall."

Threat Defense operates at the DNS level to identify and uncover threats that other solutions cannot and stop attacks earlier in the threat lifecycle. Through pervasive automation, machine learning and ecosystem integrations, Threat Defense also drives efficiencies in SecOps to uplift the effectiveness of the existing security stack built on SIEM/SOAR capabilities. "We immediately realized that from a functional standpoint, Threat Defense would boost our security capabilities," said Sinclair. "If the network team wants to forward rules to us for addressing emerging threats, we now have a tool that lets us carry out our own security processes. It's our tool, we own it."

Key Takeaways:

Visibility

DNS operations were a blind spot for Sinclair and team. This lack of visibility was a major security weakness as malicious hackers in recent years have focused more of their attacks at the DNS layer. Infoblox Threat Defense automatically collects all logging data from the city's DDI infrastructure. It then instantly renders that data into easily understood graphs, charts and hierarchies to paint a comprehensive picture of exactly what's flowing in and out of the network's DNS systems.

Enforcement of Blocking Rules

Previously, enforcing new blocking rules required coordination with multiple stakeholders. Now, continuous threat intelligence feeds directly into the security stack, allowing the team to immediately enforce new blocking rules and stopping attacks in their tracks.

Protections for Remote Workers:

The Covid pandemic made supporting remote workers a huge challenge for the SF team. Infoblox Threat Defense was implemented in short order and ensures adaptable security for remote workers and endpoints, providing peace of mind regardless of location.

DNS CAN BLOCK 92% OF MALWARE ATTACKS

Understand how to defend against DNS exploitation. Request a Security Workshop:

infoblox.com/**Carahsoft-Workshop**

infoblox®

opentext™

Security reimagined

Don’t navigate your AI journey alone

opentext™

OpenText Fortify Increases Competitive Advantage by Shifting Security Left Into the DevSecOps Application Lifecycle

To streamline application development and avoid redundant efforts, a centralized DevSecOps platform that is enhanced with OpenText Fortify was established to deliver secure, scalable, and automated application development. This solution accelerates delivery, embeds security into every stage of the lifecycle, and minimizes cyber risk.

The Challenge:

To prevent each agency building their own stack and reinventing the wheel, centrally create and maintain a DevSecOps platform, rather than just DevOps processes. This "software factory" would provide baked in security, automated tools, services, and standards that enable departments to develop, secure, deploy, and operate applications in a secure, flexible, and interoperable fashion. Applications can be launched in days rather than months with tremendous cost and time savings.

The Solution:

The use of hardened container technology ensures that multiple DevSecOps pipeline structures are available with various options to avoid vendor lock-in and enable true scalability. Iron Bank is this agency's Centralized Container Repository of authorized and hardened containers that supports the end-to-end lifecycle needed for modern software development.

To deliver on the promise of DevSecOps, and embed cybersecurity into application development and deployment, a range of options is the most critical component of Iron Bank's success. OpenText is a great additional option for Iron Bank. OpenText Fortify enables integrated security scanning right into the development cycle so that any issues are found early and fixed as part of the development testing cycles. With security automatically injected into the infrastructure, teams achieve faster accreditation of new applications and cyberattack levels are reduced.

This solution allows development teams to deliver new software releases multiple times a day which is necessary to maintain a competitive edge. It is fast, secure, and scalable, and the application output is automatically authorized because of the foundation put in place with our DevSecOps processes.

Key Takeaways:

- Time and cost savings through accelerated application delivery
- Integrated application security scanning delivers higher quality applications
- Continuous code monitoring and scanning reduces attack surface
- Prevent lateral movement by leveraging zero trust

RSA

Protecting Sensitive Police Department Data with Phishing-Resistant Hardware Passkey

A 360-question data security audit conducted by a government security agency on a week's notice would be a daunting prospect for any law enforcement entity. But one police department in the southeastern U.S. passed with flying colors, thanks to identity management capabilities from RSA.

The Challenge:

Could there be a greater challenge for a local police department than learning that auditors are on the way to check for compliance with Criminal Justice Information Service (CJIS) security policies? How about learning that they'll be there within the week?

It's a development that would have left many scrambling to prepare—but for one midsized police department in the southeastern U.S., it proved to be a relatively light lift, thanks to its deployment of FIDO2 phishing-resistant passwordless authentication from RSA.

The Solution:

RSA had worked with the police department over time to evolve their technology for securing data related to sensitive criminal justice information , starting with basic multi-factor authentication (MFA) and ultimately evolving to include phishing-resistant hardware authenticators based on the FIPS 140-3 Level 3 standard.

As a result, a state audit that was expected to take at least a week to complete—if not several weeks—was over within an astonishing five hours. This also meant the police department's IT team didn't need to worry about the prospect of having to dedicate extra personnel to the audit effort for a long period of time—which could have left the department light on resources for the duration. That would also prove to be important shortly after the state team left, when the FBI followed with its own audit to check compliance with federal policies governing protection of criminal justice information.

Because the department deploys advanced identity management technology—such as the RSA iShield Key 2 series authenticators—it can maintain its exemplary status and ensure that it continues protecting sensitive data from data breaches, phishing, and other emerging attacks. At the same time, the department can operate more efficiently and cost-effectively in the future because its authenticator firmware is field-upgradable by users, making it future-proof against new threats.

Next for the police department is the continuation of its successful cloud journey with RSA, as it moves to convert from its current hybrid deployment to having identity and access management operations 100% in the cloud.

Key Takeaways:

Challenge:
Passing local and federal audits intended to demonstrate police department competence and capabilities for protecting sensitive data.

Solution:
Advanced passwordless multi-factor authentication (MFA), including phishing-resistant hardware-based authentication managed in the cloud.

Impact:
Law enforcement that continues to do an increasingly exemplary job of securing some of the most sensitive data in local government.

RSA

No more phishing.
No more passwords.
Just true, enterprise-ready passwordless authentication.

RSA provides the broadest range of passwordless authentication methods on the market with the greatest security depth to secure federal, state, and local agencies. Meet regulations, prevent credential theft, and accelerate Zero Trust maturity with the market's only true E2E passwordless solution:

- Deploy E2E passwordless for all users and use cases, including desktop login, SaaS/Web, mobile, Windows servers, legacy, and air-gapped environments—without forced upgrades or complex workarounds
- Manage mobile passkeys, QR codes, code matching, biometrics, OTP, and firmware-upgradable hardware authenticators from a single platform
- Meet Executive Order 14028, OMB M-22-09, OMB M24-14, CJIS, and other requirements
- Phishing-resistant, brute-force resistant, bypass-resistant, outage-resistant
- FIDO2 certified across mobile passkeys and FIPS 140-3 certified security keys; supports PIV and HOTP

Contact us to learn more about how RSA keeps every login secure, resilient, and compliant for government agencies.

SailPoint

Mission critical modern identity security

Zero trust supported by AI-driven solutions

- Reduce security threats with increased visibility
- Protect public safety with an ICAM aligned strategy
- Enact least privilege access with a zero trust architecture

sailpoint.com

SailPoint in the Public Sector: Efficiencies Gained From an ICAM Enterprise Solution

The alignment of existing infrastructure with a new enterprise Identity, Credential, and Access Management (ICAM) solution from SailPoint enables a military department to automate workflows and make access decisions driven by AI and machine learning. The successful SailPoint onboarding allowed an Integrated Logistics Systems Supply (ILS- S) Program Management Office (PMO) team to quickly and efficiently produce system artifacts, provide system demonstrations, and establish a solid foundation for the project, enabling a smooth transition to development.

The Challenge:

- Maintain existing user capabilities while simultaneously prepopulating new user data constructs to align with the enterprise solution.
- Create a synchronization system within ILS-S so that changes to existing data would be accurately reflected in the tool during testing and roll-out to production.
- Limit the impact for users on the Go-Live date with disruption to less than 1% of the over 18,000 active users in ILS-S.

The Solution:

Public sector infrastructure must secure against emerging cybersecurity threats by protecting access to sensitive data, applications, and systems. This requires a cybersecurity approach that includes modern identity security, also known as strong identity governance.

Strong identity governance manages the lifecycle of digital identities for users, applications, and data – allowing agencies to provide automated access to the right identities at the right time with the right permissions, while mitigating potential security and compliance risks.

SailPoint identity security and an ICAM aligned strategy is the foundation for digital modernization and helps organizations increase visibility, better manage digital identities, reduce security threats, and follow best practices for access and policy modeling.

Key Takeaways:

By employing an agile methodology and ensuring thorough testing at every stage, ILS-S was able to successfully integrate SailPoint's ICAM solutions without compromising users' capabilities.

This served as a great example of how careful planning, flexibility, and rigorous quality assurance can enable smooth migrations to advanced identity management systems. SailPoint's ICAM solution helps assist ILS-S to maintain audit readiness and limit NFRs by ensuring user access is validated through the proper chain-of-command and permissions. In the public sector, SailPoint provides options for SaaS or on-prem environments.

splunk>
a CISCO company

University of San Francisco Promotes Efficiency, Increases Transparency With Splunk Cloud SIEM

Founded in 1855, the University of San Francisco (USF) is a Jesuit university located in the heart of San Francisco.

Like other universities, USF faces many challenges—from making payroll on time to maintaining accreditation and ensuring IT and security systems are in place to educate 10,000 students and support 2,500 faculty and staff. After evaluating several options, USF invested in Splunk Cloud as its new security information and event management (SIEM) solution. Since deploying Splunk Cloud, USF has seen benefits including:

- Improved security posture and ensured payment card industry (PCI) compliance
- Reduced phishing investigations from days to minutes
- Promoted transparency among university executives and staff

---

The Challenge:

- Needed to maintain high standards and keep the university's excellent reputation intact
- Wanted to enhance security posture and reduce vulnerabilities within systems
- Needed a baseline to establish health of information security
- Tasked with protecting PII data and ensuring PCI compliance
- Lacked security operations visibility among university staff and executives
- Recruitment and retention of talented InfoSec professional staff

"Splunk's turnkey cloud offering and hybrid option makes it magnitudes better than any of the others."

Nick Recchia, ISC Director and Information Security Officer

Within USF's Information Technology Department, the Information Security and Compliance (ISC) group is tasked with the enormous challenge of providing security strategy, assessment and risk consultation as well as compliance monitoring and auditing across the university. Previously, ISC staff were concerned about the university's security posture and its ability to protect against and prevent phishing attempts and security breaches. USF recognizes the need to protect valuable personally identifiable information (PII), such as Social Security numbers and credit card data.

Nick Recchia, ISC director and information security officer, explains that as the university underwent a technology transformation, the group sought a SIEM solution that would enable the department to be more proactive in preventing security breaches. Additionally, USF required a solution that could ensure PCI requirements were met, and that would promote security operations transparency among university executives and staff.

"We evaluated a handful of SIEM solutions and created a matrix to compare them against one another. There were several similar features and opportunities among them, but there were also big differences," Recchia explains. "Splunk's turnkey cloud offering and hybrid option makes it magnitudes better than any of the others."

The Solution:

- Implemented SIEM solution to create a more secure online environment and further safeguard university reputation
- Transformed data into valuable insights to enhance security posture
- Established baseline to monitor and improve health of information security
- Ensured PCI compliance by creating and sending automated alerts for faculty and staff to reset their passwords
- Protected PII data
- Provided a time-saving solution that promotes transparency across the university and among executives
- Provided a platform to increase engagement and meaning behind the work performed by InfoSec professional staff

Previously, USF had found difficulties in ensuring that all faculty and staff completed the mandatory information security training required by university officials. Recchia explains, "We have over 2,500 hard-working people throughout this university who are required to take basic training. And it's difficult for them to remember to take time out to complete this important task. So, how do you ensure they complete it and make it a simple process? We did it by creating a meaningful alerting system."

The ISC department uses the Splunk platform, integrated with ServiceNow, to send automated alerts to everyone required to take the course, to notify supervisors of their employees' status, and to enable staff to visualize the information gathered from the alerting system. As a result, the university has also significantly increased knowledge and transparency among executives, particularly through the widespread distribution of monthly reports that track university employees' progress in completing the training. Overall, the department has been able to produce measurable and substantial results, improving security awareness while gaining notice and visibility throughout the university.

"The way that we see the problem is that universities need to establish a baseline for IT security health," Recchia says. "And if they're ready to take that step toward it and make meaningful progress, coupled with executive leadership support and talented staff, such as USF Splunk expert Tim Ip to manage the product, then Splunk can be the most favorable tool you can get."

Key Takeaways:

Recchia explains that in the past the ISC department's systems and responses to security threats lacked transparency, both within the department and across the university. Since implementing Splunk Cloud as part of its technology transformation, the department is not only promoting efficiency but also providing full transparency into its processes.

Prior to adopting Splunk Cloud, the manual process of investigating a phishing email would span from hours to days. Now, the Splunk platform enables the department to generate a list of all who need to be contacted, enabling investigations to take place within minutes. This new process has given all parties involved access to the steps taken within the investigation.

"The top benefit of using Splunk Cloud is that it provides a system that promotes transparency and engagement," Recchia says. "The platform has really opened the eyes of our peers and colleagues to the positive impact of a SIEM solution."

Additionally, with the use of Splunk Cloud to automate processes, the department has assured that USF remains PCI-compliant. For example, alerts have been helpful both in informing employees to change their passwords at a set pattern, and in providing reminders to update their antivirus software.

"The value Splunk adds is tremendous," concludes Recchia."And it's fun. When you can do something that's fun and you strive to make your career fun, and we can map out professional development and then demonstrate value to the organization, overall, it is an amazing and rewarding investment."

splunk>
a CISCO company

Power the SOC of the Future

Strengthen digital resilience by modernizing your SOC with unified threat detection, investigation and response.

- Gain visibility and detection at scale to reduce organizational risk.
- Unify detection, investigation, and automated response for speed and efficiency.
- Solve any use case with a vast user community, apps, and partner ecosystem.

tenable | carahsoft

Your exposure ends here.

Cyber risk solutions for federal, state and local governments

Tenable® is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for approximately 44,000 customers around the globe. See how Tenable can help your team expose and close the priority cyber weaknesses that put your agency at risk.

Visit Tenable.com for more information.

tenable

Government Financial Institution Strengthens Cybersecurity with Tenable, Uncovering 30% More Critical Vulnerabilities

A leading government financial institution strengthened its cybersecurity posture by implementing Tenable Vulnerability Management, identifying nearly 30% more critical vulnerabilities than its previous solution. The platform enhances coverage, improves accuracy, and enables seamless integration.

The Challenge:

Inconsistent results, incomplete coverage and general frustration with its incumbent vulnerability management solution had this government financial institution ready for a change. The cybersecurity team expressed consistent complaints related to incorrect or missing scan results, confusing remediation steps and the inability to easily integrate with the organization's ServiceNow workflow. Leadership needed a solution that provides better coverage, more accurate results and better remediation guidance as a way to rebuild trust among the InfoSec teams and internal customers.

The Solution:

During the pilot phase Tenable Vulnerability Management found almost 30% more "critical" and "high" vulnerabilities than the agency's incumbent solution. As a result, the organization selected Tenable for consistent discovery and coverage of common CVEs across growing attack surface, better data quality and compliance reporting, and ServiceNow integration.

The Government of the District of Columbia Consolidates Security on the Zscaler Zero Trust Exchange

The Government of the District of Columbia oversees and manages all critical services for residents of the District of Columbia. Zscaler replaces legacy VPN appliances to streamline security architecture, bolsters real-time risk awareness, and protects 15,000 users.

The Challenge:

- An outdated security infrastructure could not support remote working and contributed to operational inefficiencies.
- Traditional VPN appliances extended the corporate network to end user devices, putting sensitive data at risk of compromise.
- Legacy security point products limited visibility around threats, making risk assessment and mitigation more challenging.

The Solution:

- Provided secure, direct connectivity to the internet and SaaS applications, enabling work-from-anywhere flexibility
- Replaced legacy VPNs with microsegmented zero trust access to enforce consistent security policies for private resources
- Leveraged AI-powered data and insights to bolster risk awareness and mitigate potential threats in real time, at scale

Key Takeaways:

Zero trust architecture enhances security posture:
Processes 3B transactions and blocks 200k+ threats monthly

Improves the remote user experience for 15,000 users:
Seamlessly integrates with existing identity solutions

Enables a more comprehensive focus on risk management:
Driven by better insights into risk factors and security posture

zscaler™

Secure. Simplify. Transform.

Protect your agency with the most accredited security cloud in the world. FedRAMP Moderate and High, DoD IL5 and StateRAMP authorized.

- Protect data from cyberthreats
- Reduce IT cost and complexity
- Improve user experience
- Meet mandates with confidence

FedRAMP

StateRAMP

Learn more at
zscaler.com/federal

© 2023 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

Carbon Black.
by Broadcom

Detect and Respond to Advanced Attacks

Protect your organization from the latest cyber threats with the industry's pioneer for EDR and Application Control solutions.

carahsoft

Get Started Today!


CROWDSTRIKE
2025 Global Threat Report
Stay ahead of the evolving threat landscape
The CrowdStrike Global Threat Report 2025 provides cutting-edge insights into the evolving cyber threat landscape.
Learn how adversaries are adapting and what you can do to stay ahead.
crowdstrike.com/en-us/solutions/federal-government/

proofpoint.

The leader in human-centric security

THREAT PROTECTION

Stop threats targeting your people

DATA SECURITY & GOVERNANCE

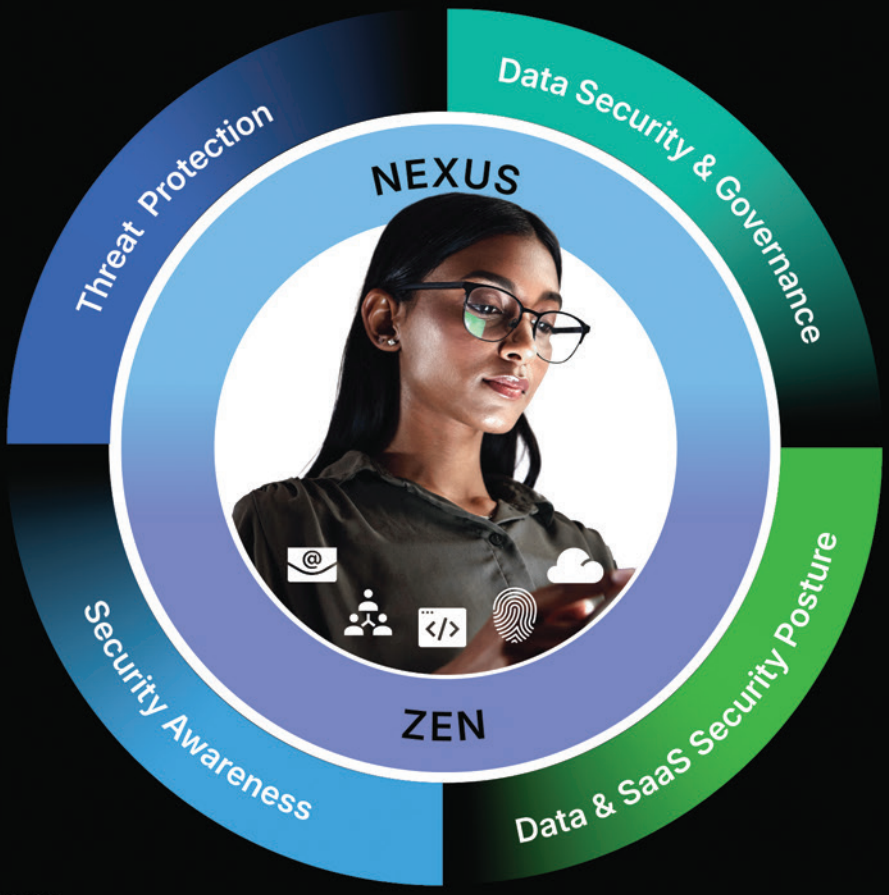
Data loss and govern communications

SECURITY AWARENESS

Provide employees with continuous guidance

DATA & SAAS SECURITY POSTURE

Remediate data & SaaS exposures



proofpoint.com

Policies and Executive Orders

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

Congress enacted CIRCIA in March 2022 in response to the SolarWinds cyberattack in 2020. The Act requires critical infrastructure cyberattacks be reported to CISA within 72 hours and ransomware payment within 24 hours. The public comment period for the Notice of Proposed Rulemaking (NPRM) related to CIRCIA closed on July 3, 2024. CISA will publish the final rule 18 months following the publication of the NPRM.

CISA outlines the core contents of the proposed regulations as follows: defining "covered entity" and applicable criteria, define "covered cyber incident" that must be reported to CISA, reporting requirements and exceptions, report submission deadlines, manner, form and content of CIRCIA reports, third-party reporting procedures, data and records preservation requirements, enforcement mechanisms, and information protections and restrictions on use.

Executive Order 14306

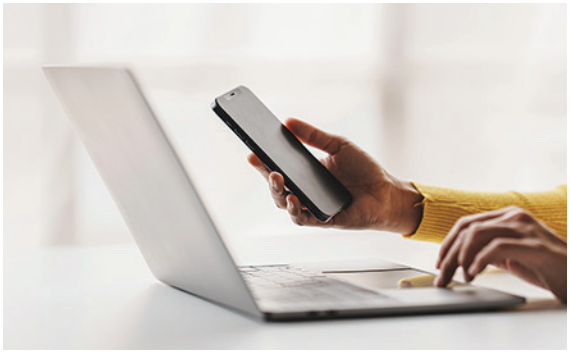
On June 6, 2025, President Trump released Executive Order 14306: Sustaining Select Efforts to Strengthen the Nation's Cybersecurity, which amends parts of EO 14144 and 13694. The order directs the Federal government to adopt the latest encryption protocols, prioritize AI, and advance post-quantum cryptography. Additionally, the order encourages the use of AI to transform cyber defenses through rapid identification of threats and increasing the scale of threat detection. Addressing quantum computing threats, the order requires agencies to use advanced encryption protocols by 2030, additionally agencies must maintain regular updates on post-quantum cryptography products that are available.

Executive Order 14144

Executive Order 14028, published on May 12, 2021, provided essential foundational steps to strengthening cybersecurity within the United States and emphasized the importance of Zero Trust Architecture (ZTA). Building upon EO 14028, The Biden Administration issued Executive Order 14144 Strengthening and Promoting Innovation in the Nation's Cybersecurity on January 16th, 2025, to address the rapid evolution of cyber threats, notably those from foreign nations. The order is focused on defending digital infrastructure, securing the services and capabilities most vital to the digital domain, and building the capabilities necessary to address key threats.

GSA Acquisition Workforce MV-23-02

On January 11th, 2023 the General Service Administration released Memorandum for the GSA Acquisition Workforce MV-23-02. This memo states that the agency will begin collecting self-attestations from software producers by June 12, 2023. Since the publication of the MV-23-02, the Cybersecurity & Infrastructure Security Agency released a draft form, which is open for public comment through June 26, 2023. The deadline, per M-23-16, will be three months and six months after the form is finalized for critical and non-critical software suppliers, respectively. This means, no software can be acquired until it has been approved by GSA's Chief Technology Officer (CTO) including software renewals and major version changes. CISA officially published the final common SSDF Self-Attestation form on March 11, 2024. If a vendor is unable to attest, the acquisition will need to be resolicited or go awarded to the next best offer.



Executive Order 14239

The Trump Administration released an Executive Order 14239: Achieving Efficiency through State and Local Preparedness on March 19, 2025. The order shifts the focus to state and local governments to prepare for cyberattacks and extreme weather conditions, additionally launching a National Resilience Strategy. It calls for states to review their current infrastructure and preparedness policies, modernizing them to streamline federal policies and operations. The establishment of the National Risk Register by November 19, 2025, is stated within the order to identify and analyze natural and malicious risks to national infrastructure.

Executive Order 14028

Executive Order 14028: Improving the Nation's Cybersecurity, released in May 2021, is the most influential piece of federal Zero Trust policy yet. The executive order directed agencies to implement Zero Trust Architecture and strengthen the software supply chain. It required service providers to report cyber incidents and threat information that could impact the government, instructed the NIST to publish standards for testing of vendor software source code, and created cybersecurity event log requirements for Federal departments and agencies.

EVERFOX

Priority Critical Cybersecurity

- Cross Domain Solutions
- Threat protection
- Insider Risk

About Everfox

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity for more than two decades. Leading the way in delivering innovative, high-assurance solutions. But we're just getting started.

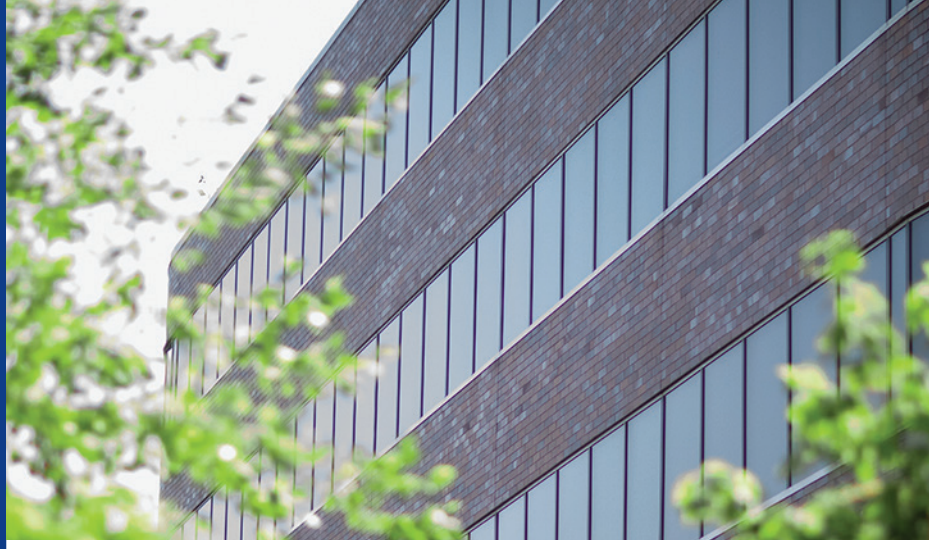
Learn more:
www.everfox.com

© Everfox 2025

okta

Every breach starts somewhere. Don’t let it start with Identity.

Learn more at okta.com/solutions/secure-identity



Contract Vehicles

Carahsoft offers a number of contract options for purchasing Cybersecurity solutions. Our contracts offer purchasing options for civilian, defense, education, state, and local government customers. Customers can purchase solutions off of these major contract vehicles:

GSA Multiple Award Schedule (MAS)

Carahsoft & our Reseller Partners hold GSA Multiple Award Schedule's (MAS) that allow customers to procure a wide variety of FedRAMP solutions. Carahsoft holds Contract #47QSWA18D008F and allows customers to purchase everything from AI infrastructure to advanced analytics solutions.

ITES-SW2

The purpose of the ITES-SW 2 acquisition is to support Army, Department of Defense (DoD) and all Federal Agency enterprise Information Technology (IT) infrastructure and info-structure goals by leveraging Commercially availableOff-The-Shelf (COTS) software products and maintenance in 14 product categories in addition to related incidental services and hardware.

NASA SEWP V

The NASA SEWP V GWAC (Government-Wide Acquisition Contract) provides the latest in Information Technology (IT) products and product-based services for all Federal Agencies. SEWP provides the best value and cost savings through innovative procurement tools and processes; premier customer service and outreach; and advocation of competition and cooperation within the industry.

NASPO ValuePoint Cooperative Purchasing Organization

The NASPO ValuePoint Cooperative Purchasing Organization (formerly WSCA-NASPO) provides the highest standard of excellence in public cooperative contracting. By leveraging the leadership and expertise of all states with the purchasing power of their public entities, NASPO ValuePoint delivers best value, reliable, competitively sourced contracts.

Since 1993 NASPO ValuePoint has been the cooperative purchasing arm of NASPO (the National Association of State Procurement Officials) encouraging, fostering and guiding the nation's most significant public contract cooperative. NASPO ValuePoint is a unified, nationally focused cooperative aggregating the demand of all 50 states, the District of Columbia and the organized US territories, their political subdivisions and other eligible entities spurring best value, innovation and competition in the marketplace.

OMNIA, Partners – Cobb County

Carahsoft holds a OMNIA Partners, Cobb County, GA Technology Products, Solutions and Related Services contract (#23-6692-01) that provides full access to a portfolio of value-driven contracts, spend visibility analytics, and subject matter experts.

OMNIA, Partners – Education Software Solutions and Services

Carahsoft Technology Corp., The Trusted Government IT Solutions Provider®, today announced that it has been awarded a Region 4 Education Service Center (ESC) contract (#R191902) for Educational Software Solutions and Services available now through OMNIA Partners. This contract makes these solutions available to state and local government agencies, education institutions, non-profits, municipalities, and additional public sector organizations through Carahsoft and authorized reseller partners.

Educational Software Solutions and Services are available through this contract and Carahsoft's reseller partners to public sector organizations in all 50 U.S. states and the District of Columbia, and the contract is established for a five-year period of performance through April 30, 2025. All solutions on this contract are offered at special discounts off their manufacturer list price, and additional price reductions can be provided on a deal-by-deal basis. Solutions from more than 200 providers are available through the contract, encompassing:

- Software Licenses
- Product Support
- Maintenance Services
- End User Computing
- Cloud Subscription Services
- Training
- Professional Services

Explore the benefits of how you can count on Carahsoft and our Reseller Partners

- 24x7 availability: Call us at 888-662-2724
- Dedicated support specializing in serving enterprise ready solutions
- Ecosystem of value-added reseller partners
- Contract Expertise: We understand your procurement needs and the outcomes you're seeking
- Quick turnaround quote: Get the IT solutions you need with the fast, accurate service you deserve
- Substantial cost savings on Zero Trust products and service portfolio from certified technology brand partners
- Advanced technology solutions including development tools, agile planning, build & test, application deployment, continuous integration (CI/CD), cloud providers and more

Upcoming Cybersecurity Events

In 2026, cybersecurity is defined by rapid change, evolving threats, and new technologies reshaping how organizations protect their environments. As government and industry continue to adapt, staying informed and connected is more important than ever, with a growing emphasis on Zero Trust architectures, endpoint detection and response, network segmentation, and phishing-resistant multi-factor authentication. Carahsoft, in collaboration with our extensive ecosystem of cybersecurity partners, is hosting and supporting a series of events designed to help federal, state, and local governments, as well as education and healthcare organizations, understand what's next. Check out these top events to learn more about what to expect in cybersecurity throughout this year.

Billington State and Local Cybersecurity Summit

March 9-11, 2026 | Washington, D.C.

The 2026 State and Local Summit will bring together top federal, state, and local government officials along with industry experts to share best practices and address their most pressing cyber risks. This event enables state and local leaders to learn from one another, enhance current cyber operations and bolster future defenses. In addition to a world-class program, networking and exhibitor opportunities will also be provided. Attendees can expect in-depth discussions and practical insights on the evolving cyber threat landscape, policy priorities, and real-world solutions impacting state and local governments. Highlights include:

- Strategic insights on cybersecurity priorities for state and local government
- Best practices in cyber resilience, risk management, and incident responseAdvancing cyber diplomacy
- Real-world case studies from government and industry leadersEngineering AI into cybersecurity platforms
- Conversations on emerging technologies and their impact on security and compliance

RSA Public Sector Day

March 23, 2026 | San Francisco, California

The Public Sector Digital Summit 2026 delivers a comprehensive look at the technologies, strategies, and innovations transforming government. Designed to bring together public sector leaders and industry experts, the summit offers a dynamic mix of keynote presentations, panel discussions, and interactive sessions focused on modernizing government services.

Now entering its next edition, PSD 2026 will feature an engaging lineup of government and industry speakers, collaborative learning opportunities, and dedicated networking experiences that encourage meaningful connections and knowledge sharing. Attendees can expect in-depth conversations around digital transformation, secure service delivery, and the future of public sector technology.

For a preview of what to expect at this year's summit, topics highlighted in previous sessions included:

- Zero Trust and cybersecurity modernization
- Cloud and data-driven government
- Digital identity and secure access
- Emerging technologies shaping public services

GovCIO CyberScape Summit

April 16, 2026 | Arlington, Virginia

TThe CyberScape Summit offers an expansive program of expert speakers, thought-provoking sessions, and interactive learning opportunities designed to address the most pressing digital security and IT modernization challenges facing government today. Now in its latest

iteration, the summit brings together senior government officials, cybersecurity practitioners, and industry innovators to explore emerging threats, strategic solutions, and forward-looking technology trends.

CyberScape 2026 will feature a robust agenda that includes keynote presentations, panel discussions, and collaborative breakout sessions, alongside networking opportunities that foster meaningful engagement across public and private sectors. Attendees will gain valuable insights into the latest strategies for protecting critical infrastructure, advancing secure digital services, and strengthening organizational cyber posture.

TechNet Cyber 2026

June 2-4, 2026 | Baltimore, Maryland

TechNet Cyber brings together government, military, industry, and academic leaders to explore technologies, policies, and strategies shaping the future of cybersecurity. Hosted by AFCEA, this premier conference provides an immersive environment for attendees to engage in meaningful dialogue around securing networks, advancing cyber operations, and protecting critical missions.

Each year, TechNet Cyber delivers an exceptional lineup of senior government and military speakers, informative sessions, and a dynamic exhibit hall showcasing innovative cyber solutions and technologies. The event also offers valuable networking opportunities designed to foster collaboration across the public and private sectors.

carahsoft

Count on Carahsoft®

The Trusted Government IT Solutions Provider®

Carahsoft proudly teams with our manufacturer and reseller partners to offer hundreds of IT solutions that are available on Carahsoft's GSA MAS, ITES-SW2, NASA SEWP V, NASPO ValuePoint, NCPA, OMNIA Partners, and numerous state and local contracts.

Learn more

carahsoft.com • sales@carahsoft.com • 703-871-8500

©2026 Carahsoft Technology Corp. All Rights Reserved.

FORESCOUT

Keep Government Operations Secure, Available & Compliant

Zero trust relies on real-time visibility of the attack surface. The Forescout Platform continuously identifies, protects and ensures the compliance of all managed and unmanaged cyber assets – IT, IoT, IoMT and OT – with least privileged access.

CONTROL LATERAL MOVEMENT
through the network with traffic flow analysis and advanced segmentation management

PRIORITIZE RISKS
and contain the weakest links before attackers do

MITIGATE THREATS
by staying ahead, own compliance, and avoiding the aftermath

Leave No Asset Unseen, *Especially The Unmanaged Ones*

The Forescout Platform provides seamless context sharing and granular workflow orchestration via ecosystem partners, helping you more effectively manage cyber risk and mitigate threats inside a Zero Trust framework.

Comply and Connect

Operate on agency-issued devices and guest devices to provide a clear view of every endpoint that touches a system. Devices that meet internal standards can connect. Those that don't are flagged and remediated.

www.forescout.com/zerotrustforgov

RAPID7

TAKE COMMAND OF YOUR ATTACK SURFACE

From Endpoint to Cloud with Rapid7

Enterprise Vulnerability Management (On-prem, SaaS, or Self Hosted)

Threat Intel - APTs, Vulnerability, Exploit Availability, Dark Web

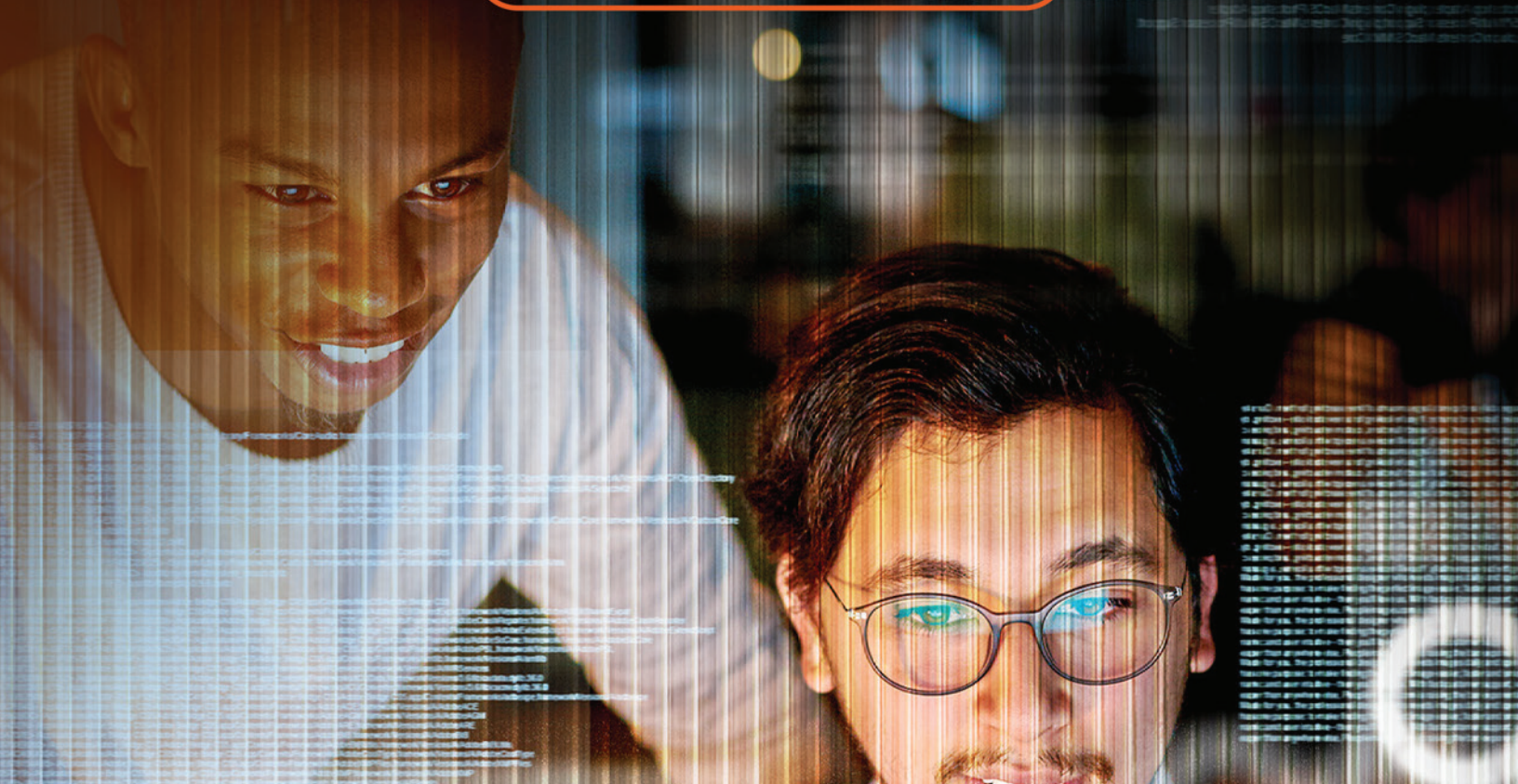
Continuous Threat Exposure Management and Asset Intelligence

Container Scanning and IaC Security

Unified Cloud-Native Application Protection (CNAPP)

Metasploit - #1 Penetration Testing Tool in the World

LEARN MORE AT RAPID7.COM



Like to know more about our **Cybersecurity** offerings?

Scan the QR

or contact us:
(571) 591-6111
Cybersecurity@Carahsoft.com
carahsoft.com/solve/cybersecurity

carahsoft.

Carahsoft Technology Corp. partners with thousands of vendors, resellers, system integrators and MSPs to proactively market, sell and deploy a comprehensive range of IT solutions for public sector customers across the U.S. and Canada.

Scan to view our solutions, latest events, trending topics and more.

carahsoft.com 11493 Sunset Hills Road, Suite 100 | Reston, Virginia 20190

© 2026 CARAHSOFT TECHNOLOGY CORP. | ALL RIGHTS RESERVED