Symantec Federal Solution Brief

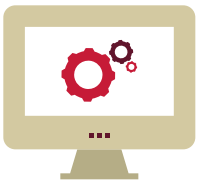
10 Reasons Why ThunderCat Should Be Your Go-To Cyber Security Partner

Federal agencies are under pressure to streamline and modernize their infrastructures to reduce costs, improve security, and accommodate modern capabilities. But they confront a critical challenge in doing this while simultaneously leveraging their existing information technology investments and staffing efficiently.

ThunderCat Technology helps agencies accomplish this. We work with industry-leading partners like Symantec to design and install architectures that unify cloud and on-premises security that employs advanced threat intelligence to realize our customers' risk management goals.

10 Reasons Why ThunderCat Should Be Your Go-To Cyber Security Partner

Here are 10 reasons why federal agencies choose ThunderCat to assist them with their cyber security modernization efforts:



1. Our broad array of technology and service offerings

Backed by our network of innovative technology partners, ThunderCat offers federal customers a wide array of strategies and solutions to address their data storage, networking, security, and applications needs. ThunderCat represents, distributes, integrates, and provides high value solutions from IT vendors that are industry leaders in data center infrastructure, mobility, enterprise applications, cyber security, and big data and data analytics.

When it comes to cyber security, ThunderCat helps agencies deploy innovative solutions that unify cloud and on-premises security to protect against threats and safeguard information across all control points and attack vector: at the endpoint, throughout the network, across email, and embedded within web applications.

Our differentiation rests on our mix of leading vendor partners, an innovative approach to integrating technologies to address specific needs and goals, and our ability to repurpose and optimize existing IT resources.

2. Our deep understanding of the federal marketplace

ThunderCat understands that federal agencies operate within unique threat and compliance environments. Agencies face threat landscapes that are as complex and unrelenting as any: In fiscal 2017, agencies reported more than 35,000 major cyber security incidents — almost three times the number as a decade before. This hostile environment has given rise to myriad mandates, guidance, and programs that aim to improve the government's cyber security posture. These include the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM), Einstein, and Trusted Internet Connections (TIC) programs; the Defense Department's Joint Regional Security Stacks (JRSS), Risk Management Framework (RMF), and Security Technical Implementation Guide (STIG) programs; the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity guidance; and the White House's Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, among many others.

ThunderCat helps our federal customers understand and navigate these many programs and mandates. But we also know that compliance does not equal security — and we help our agency customers achieve the compliance they are required to meet without sacrificing on the security they need to protect the organization and its most sensitive data resources.

10 Reasons Why ThunderCat Should Be Your Go-To Cyber Security Partner

3. Expertise in cloud security

Working with partners like Symantec, ThunderCat delivers enterprise security solutions, including Cloud Workload Protection, Cloud Access Security Broker (CASB), and Cloud Data Loss Prevention (Cloud DLP).

Cloud Workload Protection provides agency CISOs an accurate accounting of everything happening in their public cloud deployments, proven security controls, and security that is integrated into cloud operations. Symantec's Cloud Workload Protection and CWP for Storage solutions provide elastic security for AWS, Microsoft Azure, and Google Cloud Platform workloads via cloud-native integration, enabling agencies to enjoy public cloud benefits without worrying about the security and integrity of their data. With Cloud Workload Protection, agencies can extend their IT governance, risk, and compliance (GRC) and RMF security control regimes into the public cloud. It does this by providing discovery and visibility of public cloud workloads, robust security across public clouds, and elastic, cloud-native protection that scales automatically with dynamic cloud infrastructure and enables DevOps to build security directly into application deployment workflows.

CASB helps agencies to securely adopt cloud apps and meet regulatory compliance requirements by providing visibility, data security, and threat protection for sanctioned and unsanctioned apps in the cloud. CASB solutions, such as Symantec's CloudSOC, protect data in the cloud by identifying sensitive data, monitoring data at risk, encrypting sensitive content, and enforcing policy controls to prevent data breach. It also enables agencies to discover and control the use of shadow IT; investigate and respond to incidents; and detect and remediate threats in cloud apps.

Cloud DLP helps agencies take advantage of the cloud without losing visibility and giving up control of sensitive data by providing robust discovery, monitoring, and protection capabilities for cloud-based storage and email. Solutions such as Symantec DLP for Cloud Storage and Symantec DLP Cloud Prevent for Microsoft Office 365 allow agencies to confidently migrate email to the cloud by seamlessly integrating with Office 365 to provide deep visibility into sensitive information that is being stored, how it's being used, and with whom it is being shared.

ThunderCat also helps agencies unify cloud and on-premises security to protect against threats and safeguard information across every control point and attack vector: endpoints, networks, email, and cloud applications. ThunderCat arms agencies with the largest civilian threat intelligence network, robust point-to-point integrations, and a broad technology ecosystem that improves visibility, enhances controls, accelerates responses, and reduces ownership costs.

10 Reasons Why ThunderCat Should Be Your Go-To Cyber Security Partner

4. A dedicated security team

As cyber threats compound in number, sophistication, speed, and malicious behavior, government agencies have properly assigned information security as a top priority. ThunderCat has made security expertise a major focus of its business strategy and technology portfolio. Our dedicated security team provides advisory services to help customers design, assemble, and deploy highly secure information architectures. ThunderCat assembles solutions that can comb through internal and external threat and intelligence data, apply behavioral analytics to quickly spot network anomalies, and deliver end-to-end user and application visibility to provide real-time situational awareness.

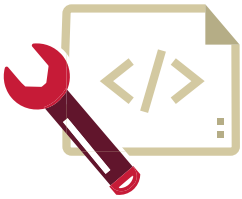
5. Detailed market research

Many agencies find their staffing and budget resources stretched, limiting their ability to thoroughly research current technologies and capabilities that could address critical challenges. ThunderCat understands innovative and emerging cyber security technologies, such as web isolation and cyber analytics. Web isolation, for example — also sometimes called browser isolation — has been identified multiple times by market research firm Gartner as one of the leading emerging technologies in the cyber security arena because it completely protects against web-borne malware, ransomware, and phishing attacks from uncategorized and risky websites.

Being attuned to the latest IT marketplace innovations, ThunderCat offers critical insights that can inform agencies early on as they plan and shape their cyber security and modernization programs, whether it is a computer network defense (CND) program or a new insider threat initiative.

6. Recognition in the market place

ThunderCat Technology has earned numerous industry awards and recognitions that attest to its value in the market. These include being named among the INC 500, Washington Technology Fast 50, Washington Technology Top 100, Solution Provider 500, CRN Tech Elite 250, SmartCEO Future 50, CRN Fast Growth 100, Washington Business Journal 50 Fastest Growing Companies, and VAR 500.

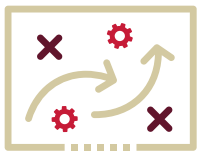


7. Expertise in open source security tools and orchestration

Open source tools and platforms have evolved significantly in recent years and are strong options for agencies to consider when looking for efficient and cost-effective ways to enhance their existing security stacks and protect their networks. ThunderCat helps agencies understand and expertly navigate the rapidly expanding ecosystem of open source security tools and platforms that include such names as Bro, Suricata, Volatility, Cuckoo, and others.

In addition, our vast knowledge of today's security orchestration and automation solutions helps agencies arrive at smarter decisions when addressing the growing challenge of alert fatigue encountered by agency security teams.

10 Reasons Why ThunderCat Should Be Your Go-To Cyber Security Partner

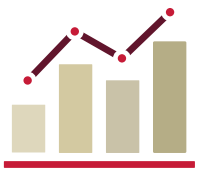


8. Experience helping agencies move from reactive to proactive cyber postures

When it comes to cyber defense, many agencies struggle at getting beyond the unrelenting detect-and-respond cycle to adopt more proactive and effective approaches to the problem. ThunderCat leverages partners like Symantec to deliver a continuous threat mitigation architecture at the network boundary, employing solutions such as Symantec ProxySG, Symantec Content Analysis System (CAS), and Symantec Web Isolation. The ProxySG consolidates a broad feature-set that protects federal enterprises from a wide array of threats, whether on the network, the web, or in the cloud, by sitting between users and their interactions with the Internet and inspecting content to identify malicious payloads, mitigate risks, and prevent data loss. CAS provides multi-layered security for effective defense against known and unknown threats by using a unique, multi-detection approach to quickly analyze suspicious files and URLs, interact with running malware to reveal its complete behavior, and expose zero-day threats and unknown malware.

Web Isolation prevents web-borne threats from reaching user's devices and solves the challenge of providing secured access to uncategorized and potentially risky websites by creating a secure execution environment between users and the web.

Deploying these solutions in an integrated architecture protects against more than 85 percent of the most common attack vectors and enables agencies to neutralize threats like spear phishing, watering-hole attacks, and known bad ghost networks before malicious payloads are downloaded.



9. Experience incorporating analytics and non-traditional threat feeds

Federal agencies may not realize that their SIEM and network data feeds are providing them only a partial view of their risk profile, undermining any resulting security posture they may adopt. ThunderCat provides nontraditional threat feeds, such as dark web, social media, public records, and financial risk data, to deliver a more complete picture of the threat landscape. ThunderCat then architects solutions that — when integrated with traditional SIEM and physical security logs — correlate, analyze, and deliver deeper, more actionable insights to inform more effective security postures.

10. A focus on innovation

Technology is constantly evolving and ThunderCat is attuned to the latest developments in cyber security solutions. We have an extensive track record of helping agencies incorporate transformational capabilities — including threat intelligence, web isolation, network visibility, cyber analytics, and a variety of information assurance tools — to enhance security postures for improved risk mitigation.

Symantec

Integrated Cyber Defense Platform (ICDx)

The fundamentals of cyber security have evolved greatly in recent years. The number and variety of threat vectors has increased as has the complexity and sophistication of today's cyber threats. In an era of cloud and mobile computing, this means that individual products must now work together seamlessly, and federal security teams need solutions that future-proof their operations so they can defend sensitive information against rapidly-evolving security threats.

Symantec understands that today's solutions must offer integrated protection across endpoints, the web, and messaging applications. Symantec's Integrated Cyber Defense Platform (ICDx) unifies cloud and on-premises security to protect users, information, messaging, and the web. Powered by unparalleled threat intelligence, ICDx is comprised of the industry's most comprehensive cloud security solutions to govern access, protect information, defend against advanced threats, and protect workloads as they move to the cloud.

Federal enterprises can no longer afford to relinquish their security to any one or two technologies or approaches. With ICDx, agencies now can deploy multiple components at every control point — desktop machines, the perimeter network, the cloud, and the mail server — that interact seamlessly, sharing information about potential signs of trouble.

THUNDERCAT TECHNOLOGY

A Service-Disabled Veteran Owned Small Business

ThunderCat Technology

(703) 674-0216
(571) 323-0918 *fax*

1925 Isaac Newton Square,
Suite 180, Reston, VA 20190

www.ThunderCatTech.com

Contract Information

GSA Schedule: GS-35F-0530U
SEWP Prime: NNGO7DA45B
NAICS: 423430, 541519
CAGE Code: 50WM7
DUNS: 809887164