THUNDERCAT TECHNOLOGY

A Service-Disabled Veteran Owned Small Business

CISCO Partner
Gold Certified

Cisco & ThunderCat Technology

Industry-leading Collaboration and Cybersecurity Solutions for Today's Evolving Federal Workplace

More federal employees are working outside of the office than ever. And this increasingly hybrid workplace is under greater duress due to cyber threats that continue growing in number and sophistication.

To adapt and succeed in these challenging times, federal agencies need innovative solutions to improve workplace collaboration and cybersecurity. Cisco has been a steady market leader in delivering to federal agencies the right mix of collaboration and cybersecurity solutions to suit their specific mission and infrastructure needs. ThunderCat Technology—one of the few Service-Disabled Veteran-Owned Small Businesses that is a Cisco Gold Partner—has been a trusted value-added reseller across the federal civilian, defense, and intelligence marketplace with a proven track record of excellent customer service.

Together, Cisco and ThunderCat can help your agency find the right solutions for your employees' unique needs when it comes to cybersecurity and collaboration tools.

Cisco Collaboration Solutions

Today's hybrid work environments demand that federal employees be able to collaborate with their colleagues, clients, and partners wherever they are. Two of Cisco's top collaboration tools are Cisco Webex Meetings and Cisco Webex Calling. Both solutions are FedRAMP-authorized and include robust cybersecurity protections.

Cisco Webex Meetings

Cisco Webex Meetings offer secure, integrated audio, video, and content sharing from any device, anywhere. Intelligent features—such as noise removal, Webex Assistant with real-time translations, and People Insights—automate meeting tasks to help you work smarter.

Features and benefits include: simple joining and scheduling, video-first experiences from any device, AI-powered tools to automate common meeting tasks, and integration with leading productivity tools, including Microsoft Teams, Slack, Workplace by Facebook, Salesforce, and many others.

Webex Meetings provides the highest level of protection for meeting data with support for AES 256-Bit GCM Encryption. In addition, industry-leading data loss prevention and compliance capabilities also protect meeting artifacts including recordings, Webex Assistant transcriptions, action items, and highlights.

Cisco Webex Calling

Many federal employees work from home or other remote locations but need a phone service with all the features of a modern business phone system. Cisco Webex Calling is an enterprise-grade cloud-based phone solution that provides secure and reliable enterprise-grade communications, easy setup and maintenance, centralized management, and end-to-end encryption for robust security. Webex Calling also works with any Session Initiation Protocol (SIP) service provider.

Features and benefits include: PBX business features; integrated user experience for calling, meetings, and messaging; desk phone, PC, and mobile device integration; voicemail messaging; intelligent call routing and auto attendants; secure geo-redundant network; integrated management and analytics; and global presence and support.

Cisco Cybersecurity Solutions

To effectively deal with today's fast-evolving cybersecurity threats, federal agencies must maintain continuous visibility into their networks and install layered, interlocking solutions that deliver robust security protection. Cisco's wide array of cybersecurity solutions can address virtually any security requirement for federal agencies. These solutions include the following:

- Cisco switches are always learning, adapting, and protecting. By employing automation, security, artificial intelligence, and machine reasoning, Cisco switches build the foundation for digital transformation at the data center, the core, or the edge.
- Cisco Catalyst Access Points offer intelligence, resiliency, integrated security, and the benefits of the new, high-efficiency Wi-Fi 6 standard. These Access Points are ready for growing user expectations, IoT devices, and next generation cloud-driven applications.
- Cisco Wireless LAN Controllers are resilient, secure, and intelligent solutions that will take your network beyond Wi-Fi 6.
- Cisco VPN Client, called Cisco AnyConnect Secure Mobility Client, empowers remote workers with frictionless, highly secure access to the enterprise network from any device, at any time, in any location while protecting the organization.
- Cisco Secure Firewalls offer you the deepest set of integrations between core networking functions and network security, delivering the most secure architecture ever.

To effectively deal with today's fast-evolving cybersecurity threats, federal agencies must maintain continuous visibility into their networks and install layered, interlocking solutions that deliver robust security protection.

- Cisco Identity Services Engine (ISE) enables a dynamic and automated approach to policy enforcement that simplifies the delivery of highly secure network access control. ISE empowers software-defined access and automates network segmentation within IT and OT environments.
- Cisco Secure Network Analytics (StealthWatch) outsmarts emerging threats with industry-leading machine learning and behavioral modeling that lets you know who is on the network and what they are doing. This solution also applies smarter network segmentation to protect critical data.

ThunderCat Technology has partnered with Cisco Systems to help the Defense Department transition to its next-generation cybersecurity regime, called Comply-to-Connect (C2C). C2C integrates and orchestrates multiple solutions that, taken together, discover, identify, characterize, and report on all devices connecting to the network. The C2C framework, which is currently being deployed on both classified SIPR and unclassified NIPR networks, is comprised of five phases—and Cisco solutions support all of them:

Phase 1: *Verify the identity of users and devices before network access is granted.*

To achieve this: Cisco switches, Cisco access points, and Cisco Secure Firewalls can be configured to send information to Cisco ISE to identify end users.

Phase 2: *Control access to resources, based on policy and authorization.*

To achieve this: Cisco ISE can be integrated with the Assured Compliance Assessment Solution (ACAS), McAfee ePolicy Orchestrator (ePO), and other existing DoD tools to automate Network Admission Control (NAC) and posture assessments.

Phase 3: *Obtain visibility into who is connected to the network while providing continuous monitoring.*

To achieve this: Cisco ISE automates policy enforcement while Cisco StealthWatch helps administrators keep unauthorized users and devices from accessing restricted areas of your network while also extending visibility and control to your data center and the cloud.

Phase 4: *Prevent and control malicious activities, such as propagation of malware, network infiltration, data exfiltration, and denial of service.*

To achieve this: Cisco ISE and Cisco StealthWatch make sure devices connect only when and where they are authorized—for example, by authenticating endpoints and determining if they comply with the agency's security posture.

Phase 5: *Automate breach response and remediate vulnerabilities.*

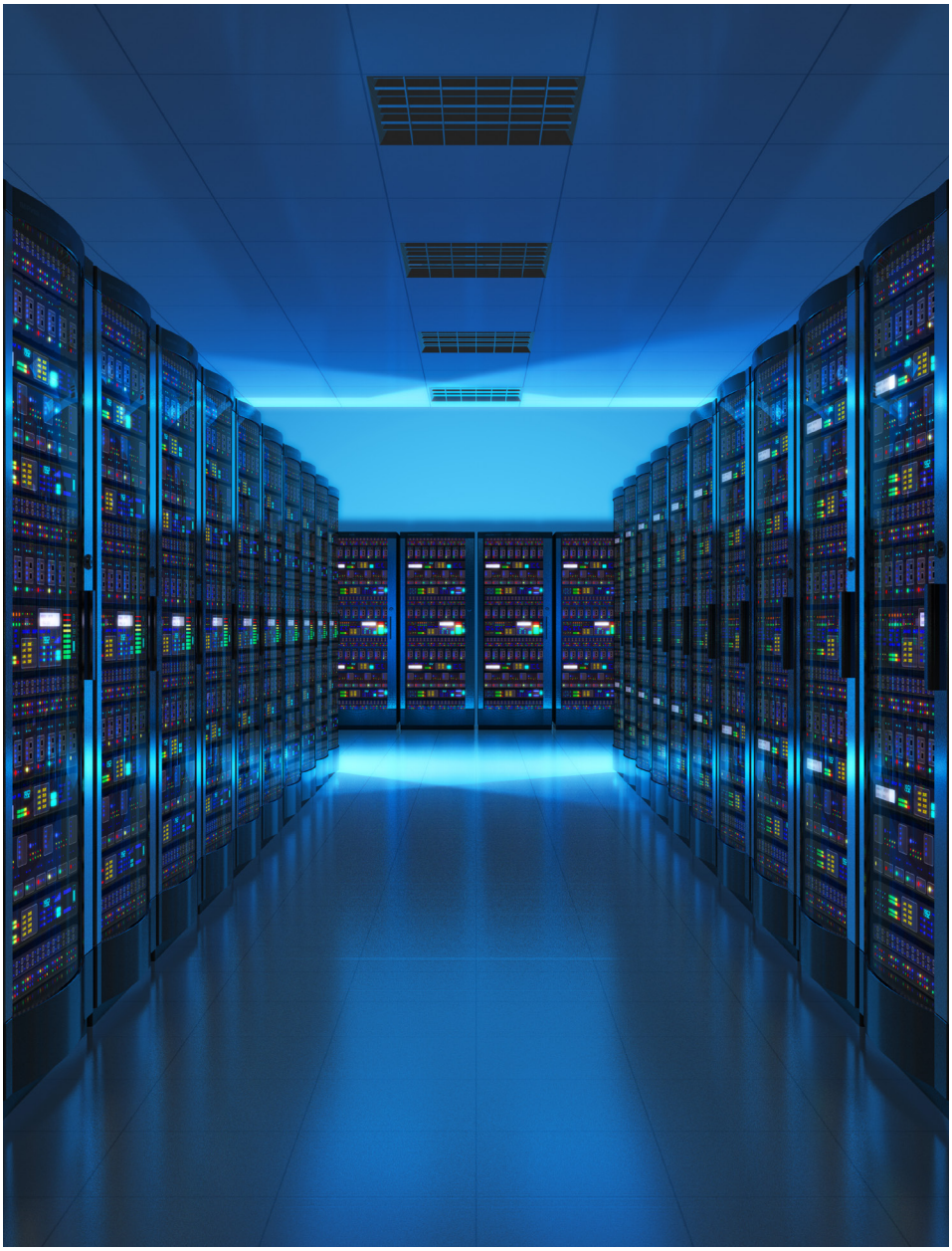
To achieve this: Cisco ISE automates a wide spectrum of response and remediation tasks, including network admission control and port security, device profiling, and the application of security patches when a device connects to the network.

About Cisco

Cisco has been a highly trusted solution provider to the federal government for many years. Its vast portfolio of solutions can address most federal use cases and environments in the areas of cybersecurity, wireless communications, workplace collaboration, and enterprise networks. Cisco solutions are known for delivering industry-leading innovation, high degrees of integration, smart responsiveness, and peerless technical support.

About ThunderCat Technology

ThunderCat Technology is one of the few Service-Disabled, Veteran-Owned Small Business in the federal marketplace that is a Cisco Gold Partner. ThunderCat is a premier and trusted provider of information technology to government organizations, educational institutions, and commercial enterprises. We approach each engagement with integrity and a commitment to help our customers fulfill their mission. ThunderCat specializes in security, networking, data center, cloud, and collaboration solutions with Cisco's vast portfolio of technologies. Led by a team of solutions architects who hold various CCIEs, we are able to architect, consult, train, manage and deploy multiple Cisco solutions in any environment.



For more information about how ThunderCat Technology can help your agency address its workplace collaboration and cybersecurity needs, please go to www.thundercattech.com/partners/cisco/.

ThunderCat | Contracts: GSA Schedule 70: GS-35F-0537U | SEWP V (SDVOSB): NNG15SD26B | SEWP V (Small Business): NNG15SC92BAn ISO 9001: 2015 Registered Company | NAICS: 423430, 541519 | DUNS: 809887164 | CAGE Code: 50WM7
Address: 1925 Isaac Newton Square E., Suite 180 Reston, VA 20190 | Phone: (703) 674-0216 | Fax: (571) 323-0918
Email: info@thundercattech.com

ThunderCat is the premier and trusted provider of Information Technology to the U.S. Federal Government, State and Local Governments, and Fortune 500 companies. As a Service-Disabled Veteran-Owned Small Business, and value-added reseller, ThunderCat approaches each engagement with integrity and commitment to help our customers fulfill their mission.