Modernizing Government Cybersecurity

Contents

Service Your Citizens, Your Mission

As a government agency, you face the ongoing challenge of modernizing IT to meet evolving demands from citizens and employees while complying with cybersecurity frameworks and regulations. Your transformation aims to enhance service delivery and efficiency but requires careful consideration of security governance.

Your modernization efforts may include secure online payment systems, cloud collaboration, IoT for smart cities, and mobile apps.

This Solution Brief was designed to guide you through government IT modernization, emphasizing both innovation and security. We explore initiatives to transform your operations, improve citizen experiences, and strengthen cyber defenses. Learn to streamline processes, implement security governance frameworks, and support compliance requirements.

The Future of Governance: Secure, Efficient, and Citizen-Centric

The imperative for digital transformation in your government agency has never been more pressing. As you face increasing citizen demands, expanding mission scope, and budget constraints, technology offers the key to revolutionizing your operations and service delivery.

By embracing digital transformation, government agencies can:

- **Improve citizen services:** Offer personalized experiences through online portals, enhancing satisfaction
- **Enable data-driven decision-making:** Use analytics and AI for evidence-based policies
- **Enhance efficiency and reduce costs:** Streamline workflows and automate processes
- **Increase transparency and accountability:** Implement open data initiatives
- **Promote equity and inclusion:** Ensure digital services are accessible to all

However, modernization also presents challenges:

- **Cybersecurity threats:** Protect against phishing and data breaches with robust security measures
- **Collaboration and interoperability:** Foster cross-agency collaboration for better service delivery
- **Change management and culture shift:** Navigate organizational resistance to foster innovation

By leveraging comprehensive security solutions and strategic digital transformation, agencies can balance innovation with protection, meeting 21st-century governance challenges while safeguarding critical assets and citizen data.

Benefits of Digital Transformation in Government

Improve citizen services

Increase transparency and accountability

Enable data-driven decision-making

Promote equality and inclusion

Enhance efficiency and reduce costs

Reduce cybersecurity threats

Improve collaboration and interoperability

FedRAMP NIST CSF EUCC NIS2 ISO 270001 MITRE

Navigating the Compliance Maze: From Local to Global

As you modernize your government services, adhering to key compliance standards and regulatory requirements is crucial. This helps improve data protection, maintain public trust, facilitate interoperability, and reduces legal and security risks while promoting transparency and accountability.

Frameworks like FedRAMP, NIST CSF, EUCC, and NIS2 provide important guidelines, helping your systems meet security, privacy, and operational requirements. These frameworks can help build citizen trust, protect sensitive data, streamline security assessments, and support cloud-first strategies.

If your agency operates across international borders, you may need to address cross-regional compliance challenges by understanding and adhering to the local laws in each jurisdiction where you conduct activities. Cybersecurity requirements can vary significantly between countries, and practices acceptable in one region may not be permissible in another. You'll need to consider regulations on data transfers and protection, such as the new U.S. Bulk Sensitive Data Regulatory Program. Prioritizing cross-border cybersecurity compliance mitigates risks, fosters cooperation, and supports secure, efficient service delivery internationally.

Explore Security Frameworks and Certifications

Building Blocks for Modernization

Your government IT modernization requires a strategic approach to many different elements. It involves not just updating technology but also rethinking processes and security paradigms. The foundation of your transformation rests on several key pillars:

- **Zero Trust Architecture:** Forms your cybersecurity cornerstone, requiring continuous verification for all users and devices
- **AI-Driven Processes:** Enhances your efficiency and decision-making, from automating tasks to providing data-driven insights
- **Cloud Adoption:** Enables scalability, cost-effectiveness, and improved service delivery
- **Cyber Resilience:** Helps you withstand and recover from attacks, minimizing disruption
- **Incident Response:** Ensures you take quick and effective action when security breaches occur

By embracing these technologies and approaches, you can better serve citizens, protect data, and adapt to evolving digital landscapes and cyber threats.

A Simplified Approach to Security and Compliance

Modernizing government IT shouldn’t be overwhelming. As you face increasing cyber threats and regulatory demands, strategic initiatives can streamline processes while maintaining security and compliance. Key focus areas include:

- Adoption of integrated security platforms
- Automation of compliance tasks
- Leveraging cloud-based solutions with built-in security
- Using AI/ML to enhance threat detection
- Standardizing processes and training for security

Optimizing operations with digital solutions gives your employees time back to focus on more important matters. Focusing on these areas can help simplify transformation, enhance security, and work towards efficiently meeting requirements.

Key Security Challenges in Government IT

Cloud and Application Security

- Data breaches in cloud environments
- Malware in cloud-based systems
- Misconfigured cloud services

Network Security

- Unauthorized access threats
- Denial of service attacks
- Data interception risks

Data Center Security

- Physical and insider threats
- Virtual machine escape attacks
- Unauthorized movement within data centers

User and Device Security

- Phishing and malware threats
- Lost devices and weak credentials
- Insider threats by users

Threat Detection and Response

- APTs and zero-day exploits
- Ransomware and stealthy malware
- Lateral network movement

See the Cisco Security portfolio and how Cisco Can Help

Cloud and Application Security

Your agency can leverage Cisco's Cloud and Application Security solutions for protection while navigating the complexities of digital transformation. These solutions provide you security across cloud environments, applications, and data, supporting integrity and compliance with regulations. By utilizing advanced threat intelligence, AI-driven analytics, and automated defenses, you can adopt cloud technologies while maintaining a strong security posture. Cisco's integrated approach enables you to implement seamless protection from the network edge to the application layer, helping to safeguard your sensitive information and critical infrastructure against evolving cyber threats.

Learn more about Cloud and Application Security Solutions

Cisco Secure Cloud Analytics

Cisco Secure Cloud Analytics is a Software-as-a-Service (SaaS) solution that provides comprehensive analytics of network and cloud traffic, enabling organizations to detect and respond to threats in real-time. It offers high-fidelity threat detection by analyzing network flows and telemetry and integrates with Cisco XDR for extended detection and response capabilities. Secure Cloud Analytics is designed to be easy to deploy and manage, providing visibility across hybrid environments without the need for additional hardware or software agents.

Cisco Secure Email Threat Defense

Cisco Secure Email Threat Defense provides comprehensive protection against email threats that can compromise an organization's brand and operations. It uses advanced threat detection capabilities to uncover known, emerging, and targeted threats, and rapidly searches for and remediates threats in real time. Additionally, it augments native Microsoft 365 security by providing complete visibility to inbound, outbound, and internal messages, leveraging superior threat intelligence from Cisco Talos.

Cisco Secure Workload

Cisco Secure Workload is a hybrid-cloud workload protection platform designed to secure compute instances in both on-premises data centers and public clouds. It uses machine learning, behavior analysis, and algorithmic approaches to offer a holistic workload protection strategy, including micro-segmentation and proactive identification of security incidents. Additionally, it provides zero-trust micro-segmentation across any workload, environment, or location, reducing the attack surface by preventing lateral movement and continuously monitoring compliance.

Cisco Secure DDoS Protection

Cisco Secure DDoS Protection is a solution designed to defend organizations against sophisticated DDoS attacks using advanced behavioral-based and machine learning algorithms. It provides protection against both network-layer (L3/4) and application-layer (L7) attacks, including encrypted SSL-based DDoS attacks, without adding latency.

Cisco Secure Web Application Firewall

Cisco Secure Web Application Firewall (WAF) is a fully managed, cloud-based service that provides comprehensive protection against web application attacks, leveraging Radware's Cloud WAF Service. It ensures the security and availability of websites, mobile applications, and APIs by defending against both common and advanced threats, including DDoS attacks.

Network Security

Network security is essential for your government agency as you navigate an expanding threat landscape. You must protect increasingly complex networks connecting on-premises, cloud, and mobile environments. Cisco helps by providing the visibility, control, and advanced threat protection needed to secure these dynamic networks. Our solutions support your business continuity and compliance efforts. Cisco's built-for-cloud approach enables security everywhere, empowering secure work from anywhere.

Learn more about Network Security

Cisco Next Generation Firewall

Cisco's Next-Generation Firewall (NGFW) provides advanced security features beyond traditional firewalls, including application awareness, integrated intrusion prevention, and threat intelligence to block modern threats like advanced malware and application-layer attacks. It offers unified management and advanced threat protection before, during, and after attacks, ensuring better security and faster speed.

Cisco Secure Firewall ASA

The Cisco Adaptive Security Appliance (ASA) is a family of security devices that protect corporate networks and data centers of all sizes. It provides highly secure access to data and network resources anytime, anywhere, using any device, and has been a proven firewall and network security platform for over 15 years with more than 1 million security appliances deployed worldwide. The ASA 5500-X Series with FirePOWER Services offers advanced threat defense options, including intrusion prevention, malware defense, and application visibility, making it a comprehensive security solution.

Cisco Identity Services Engine (ISE)

The Cisco Identity Services Engine (ISE) is a comprehensive Network Access Control (NAC) solution that serves as the foundation for a zero trust security model. It enables secure access for users and devices across networks and clouds, providing visibility and control over who and what is on your network. Cisco ISE allows organizations to enforce policies, manage endpoints, and deliver trusted access, ensuring compliance and enhancing infrastructure security.

Cisco Secure Network Analytics (SNA)

Cisco Secure Network Analytics (SNA) provides enterprise-wide network visibility to detect and respond to threats in real-time. It continuously analyzes network activities to establish a baseline of normal behavior, using advanced analytics and machine learning to identify anomalies and threats such as ransomware, DDoS attacks, and insider threats. SNA integrates seamlessly with existing security controls, offering comprehensive threat monitoring across encrypted network traffic without the need for additional probes or sensors.

Cisco Secure Network Analytics Data Store

The Cisco Secure Network Analytics Data Store provides a centralized repository for network telemetry, collected by Flow Collectors. This setup, with clustered data nodes holding network flow data and backups, enables faster query retrieval and improved fault tolerance. By consolidating data in one place, it enhances performance and efficiency for graph and chart generation using Cisco Secure Network Analytics. Additionally, its architecture allows for flexible scaling of flow collection and storage, tailored to customer needs and budgets.

Cisco Telemetry Broker

Cisco Telemetry Broker simplifies the management of network telemetry by brokering hybrid cloud data, filtering unneeded data, and transforming data into a usable format. It provides increased visibility to hybrid cloud environments and allows seamless coexistence of customers and tools by freeing telemetry from proprietary protocols.

Cisco Umbrella for Government

Cisco Umbrella for Government is a cloud-native security service designed to meet the specific needs of U.S. Federal, State, and Local government agencies. It provides a comprehensive suite of security features, including DNS-layer security, Secure Web Gateway, and Cloud Access Security Broker (CASB), all while complying with FedRAMP Moderate, StateRAMP, and TX-RAMP standards. Additionally, it integrates with CISA's Protective DNS and supports enhanced device security and PIV/CAC card support, ensuring robust protection for government infrastructure.

Meraki MX

The Meraki MX is an enterprise security and SD-WAN appliance designed for distributed deployments that require remote administration. It provides a cloud-managed solution that integrates security, networking, and physical security into a single dashboard, making it ideal for network administrators who demand both ease of use and robust security features. The MX series includes features such as application-based firewalling, content filtering, and advanced malware protection, all powered by Cisco Talos, ensuring a secure and high-quality network experience.

Cisco Security Cloud Control

Security Cloud Control enhances operations with a cloud-native design and AI-driven features, consolidating security functions and automating tasks to improve visibility, scalability, and efficiency. It provides unified management for Hybrid Mesh Firewall, enforcing zero trust across data centers and IoT environments. The solution also enables Universal ZTNA for seamless zero trust enforcement across cloud and on-premises setups, simplifying hybrid workforce experiences with consistent policies. Security Cloud Control establishes an adaptive defense system that evolves with the network, optimizing security and operational efficiency.

Cisco Defense Orchestrator (CDO)

Cisco Defense Orchestrator (CDO) simplifies and centralizes the management of security policies across Cisco security devices and services. It offers a unified interface for configuring, monitoring, and maintaining firewall rules, VPN settings, and other security policies. By streamlining operations, CDO enhances visibility, reduces complexity, and ensures consistent security enforcement across on-premises, cloud, and hybrid environments. Its intuitive design supports efficient policy updates and compliance checks, enabling organizations to effectively manage their security posture.

Cisco Secure IPS

Integrates threat protection and full-stack visibility, providing context-aware security that delivers in-depth information about users, devices, and applications on your network. It includes Security Intelligence with analysis of IP, DNS, and URL data, and identification of Indicators of Compromise (IoCs), allowing for automation and delivering security at a lower total cost of ownership.

Cisco Secure Firewall Management Center (FMC)

Serves as the administrative hub for managing critical Cisco network security solutions. It offers comprehensive and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection. This allows for seamless transitions from managing firewalls to controlling applications, investigating threats, and remediating malware outbreaks.

Cisco Security Analytics and Logging (SAL)

Cisco Security Analytics and Logging (SAL) is a central log management and advanced threat detection service that provides scalable Cisco firewall logging and correlated analytics. It helps in troubleshooting network access issues, monitoring device and network health, and detecting advanced threats. SAL is available as a Software as a Service (SaaS) or on-premises solution, integrating with Cisco Defense Orchestrator for cloud-based management and Secure Network Analytics for on-premises management.

Cisco Secure Web Appliance

The Cisco Secure Web Appliance provides comprehensive web security by blocking risky sites and testing unknown sites before allowing access, ensuring protection against advanced threats. It offers flexible deployment options, including hardware appliances, virtual machines, and cloud-based solutions, to adapt to various organizational needs.

Cisco Secure Malware Analytics

Cisco Secure Malware Analytics, formerly known as Threat Grid, provides advanced sandboxing and threat intelligence to analyze and identify malware in near real-time. It offers a comprehensive view of malware samples and behaviors, enabling organizations to automate malware protection and integrate with existing security technologies for enhanced threat detection and response.

Data Center Security

Protecting your agency's resources is crucial as your workforce accesses them from diverse locations and devices. Cisco's approach aims to safeguard against sophisticated threats like ransomware, phishing, and malware. Our solutions can provide visibility across all devices, helping you detect, respond to, and recover from security incidents quickly. With robust user and device security measures, you can strive to secure access to applications and data, maintain compliance, and support a productive workforce while prioritizing security.

[Learn more about Data Center Security]

[Cisco Secure Workload]

Cisco Secure Workload is a hybrid-cloud workload protection platform designed to secure compute instances in both on-premises data centers and public clouds. It uses machine learning, behavior analysis, and algorithmic approaches to implement micro-segmentation, identify security incidents proactively, and reduce the attack surface by identifying software-related vulnerabilities. Additionally, it provides comprehensive visibility into every workload interaction and uses AI/ML-driven automation to reduce the attack surface, prevent lateral movement, and continuously monitor compliance.

Cisco Secure Firewall

Cisco Secure Firewall provides comprehensive protection against a wide range of threats, ensuring your network's security with superior performance and robust security measures. It integrates seamlessly with other Cisco and third-party solutions to offer a broad portfolio of security products that work together to correlate events, eliminate noise, and stop threats faster. Cisco Secure Firewall is designed to safeguard organizations from encrypted and zero-day threats, harmonizing security across hybrid and multicloud environments with AI/ML-driven capabilities.

Cisco Hybrid Mesh Firewall

The Cisco Hybrid Mesh Firewall is designed to provide distributed enforcement with unified management across hybrid infrastructures, optimizing for zero trust segmentation and application protection in data center, cloud, campus, and IoT environments. It leverages AI-native rule engines to prioritize vulnerabilities and automatically recommend mitigating controls, ensuring applications continue to run smoothly even under threat.

Cisco Hypershield

Cisco Hypershield is an AI-native security architecture designed to provide comprehensive protection across networks, servers, and cloud deployments by embedding security into every software component. It leverages AI to automate security policy lifecycles and infrastructure upgrades, offering deep visibility and enforcement at the kernel level.

Cisco Multicloud Defense

Cisco Multicloud Defense offers unified security for organizations with complex cloud environments, covering major platforms like AWS, Azure, GCP, OCI, and private clouds. Its centralized single-controller approach simplifies management and ensures consistent security policies across all clouds. The solution stops inbound threats, blocks command and control activities, prevents data exfiltration, and hinders lateral movement with multi-directional protection, while enabling strategic placement of security controls through continuous asset discovery.

User and Device Security

User and Device Security is critical in today's environment where you and your employees access agency resources from various locations and devices. Cisco's approach helps to protect users, endpoints, and data from sophisticated threats like ransomware, phishing, and malware. Our solutions can provide you with visibility across managed and unmanaged devices, helping your organization to detect, respond to, and recover from security incidents quickly. By implementing user and device security measures, agencies can work towards creating a secure environment that adapts to the evolving needs of your hybrid workforce.

Learn more about User and Device Security

Cisco Secure Access by Duo

Provides a robust security solution that combines multi-factor authentication (MFA) with advanced endpoint visibility to secure access to applications and networks from any device and location. It supports a zero-trust security model, ensuring that only verified users and trusted devices can access sensitive resources, thereby enhancing overall security posture.

Cisco Secure Client

A modular framework that integrates various components such as AnyConnect VPN, Cisco Secure Endpoint, and Umbrella Cloud Security, among others, to provide comprehensive security solutions. It offers security to user devices on any network from any location, allowing connections to private resources through Zero Trust Access or VPNs, and protects internet resources with DNS-layer security and web security.

Cisco Secure Client's Network Visibility Module (NVM)

Cisco Secure Client's Network Visibility Module (NVM) is a component designed to enhance network security by providing detailed visibility into network traffic patterns. NVM collects telemetry data from endpoints, allowing organizations to gain insights into application usage, network behavior, and potential security threats. This visibility helps in identifying anomalies, optimizing network performance, and improving security posture.

Cisco Secure Email

Advanced email security solution protects against phishing, malware, and business email compromise using sophisticated threat defense capabilities. It secures both inbound and outbound messages, safeguarding sensitive information with end-to-end encryption and preventing data loss.

Cisco Secure Malware Analytics

Cisco Secure Malware Analytics, formerly known as Threat Grid, provides advanced sandboxing and threat intelligence to analyze and identify malware in near real-time. It offers a comprehensive view of malware samples and behaviors, enabling organizations to automate malware protection and integrate with existing security technologies for enhanced threat detection and response.

Cisco Secure Endpoint

Cisco Secure Endpoint, formerly known as Cisco AMP for Endpoints, is a cloud-managed endpoint security solution designed to prevent breaches and rapidly detect, contain, and remediate threats. It provides advanced endpoint protection with features like background scanning, hash-based detection, and retrospective security to help organizations stay ahead of malware threats. Additionally, it offers powerful EDR capabilities, threat hunting, and integrated risk-based vulnerability management, enabling businesses to detect, respond, and recover from attacks efficiently.

Cisco Umbrella for Government

Cisco Umbrella for Government is a comprehensive cloud-native security solution designed specifically for U.S. Federal, State, and Local government agencies. It offers enhanced security features such as Protective DNS integration, PIV/CAC card support, and compliance with FedRAMP Moderate, StateRAMP, and TX-RAMP standards, ensuring robust protection for critical infrastructure.

Cisco Meraki MDM

Cisco Meraki MDM, known as Systems Manager, is a cloud-based mobile device management solution that provides centralized tools for endpoint management, allowing organizations to provision, monitor, and secure all endpoint devices within their network. It offers features such as remote device locking, application management, and certificate management, eliminating the need for on-premises infrastructure.

Threat Detection and Response

Threat Detection and Response is crucial for government agencies facing increasingly sophisticated cyber threats. Cisco's solutions aim to provide comprehensive visibility across your networks, endpoints, and cloud environments, helping you identify and mitigate potential security incidents quickly. By leveraging AI and machine learning, these tools can detect anomalies and correlate data to uncover hidden threats.

[Learn more about Threat Detection and Response]

[Cisco XDR]

Cisco XDR is a cloud-native extended detection and response solution designed to simplify security operations by integrating with the broad Cisco security portfolio and third-party offerings. It enhances threat detection and response capabilities by collecting and correlating data across multiple sources, such as network, cloud, endpoint, email, identity, and applications, providing unified visibility and deep context into advanced threats.

[Splunk Enterprise]

Splunk Enterprise serves as a foundational platform, enabling organizations to collect, analyze, and visualize machine-generated data from various sources, thereby driving informed decision-making and operational insights.

[Splunk Enterprise Security]

Splunk Enterprise Security (ES) builds on this foundation by providing advanced security analytics and threat detection capabilities, empowering security teams to identify and respond to incidents swiftly.

[Splunk SOAR]

Splunk SOAR (Security Orchestration, Automation, and Response) further enhances security operations by automating workflows and orchestrating responses to security threats, improving efficiency and reducing response times.

[Splunk IT Service Intelligence]

Splunk IT Service Intelligence (ITSI) offers a comprehensive approach to IT operations management, utilizing advanced analytics to monitor and optimize the performance and availability of IT services.

[Splunk User Behavior Analytics]

Splunk User Behavior Analytics (UBA) focuses on detecting anomalous behavior patterns that could indicate insider threats or compromised accounts, helping organizations protect their valuable assets.

Security Suites

Cisco Security Suites offer comprehensive solutions tailored to meet the unique security needs of government agencies. By integrating advanced threat detection, user identity protection, and cloud security, these suites provide strong defenses against a wide range of cyber threats. They facilitate compliance with stringent security regulations and frameworks, such as NIST and GDPR, helping to ensure that sensitive data is protected, and operations remain uninterrupted. With Cisco's expertise, your agency can navigate the complexities of modern cybersecurity challenges while maintaining regulatory adherence.

Learn more about Security Suites

Breach Protection Suite

The Cisco Breach Protection Suite provides a comprehensive security framework that integrates detection, prevention, and response capabilities. It leverages AI and cross-domain telemetry to deliver intelligent, integrated protection across email, endpoints, network, and cloud environments. The suite empowers Security Operations Centers (SOC) to quickly detect and respond to advanced threats like ransomware and data exfiltration, ensuring compliance with privacy protection standards. Additionally, it enhances threat detection and streamlines security operations, which are essential for maintaining a strong security posture.

User Protection Suite

The Cisco User Protection Suite provides comprehensive security measures that protect user data and privacy. This suite offers robust protection against various attack vectors targeting users, such as phishing, malware, and credential compromise, while ensuring seamless and secure access to applications and data. By implementing zero-trust principles and integrating advanced threat detection and response capabilities, the suite helps organizations maintain compliance with privacy regulations like GDPR.

Cloud Protection Suite

Tailored for hybrid and multicloud environments, the Cisco Cloud Protection Suite provides the critical capabilities to prevent unauthorized lateral movement and the ability to protect against application vulnerabilities using surgical compensating controls. The also suite delivers foundational security to stop inbound attacks and data exfiltration, as well as advanced protection against zero day exploits and to block malware in encrypted traffic. The Cloud Protection Suite marries simplicity, flexibility, and investment protection for easy adoption of Cisco's Hybrid Mesh Firewall.

Our Experts are Yours Too

Cisco Talos is one of the largest commercial threat intelligence teams in the world, dedicated to protecting Cisco customers and the internet. Talos provides unparalleled protection against known and emerging threats through:

Emergency Response

Rapid incident response to contain and remediate breaches.

This rapid-response service swiftly addresses cyber incidents, providing triage, coordination, investigation, containment, and remediation. Expert teams leverage real-time threat intelligence to deliver tailored solutions, ensuring quick and effective business recovery across various threat types.

Proactive Services

Tailored assessments and recommendations to strengthen your security posture.

These services help organizations assess, strengthen, and evolve their cybersecurity incident response readiness. Offerings include readiness assessments, incident response plan development, customized playbooks, tabletop exercises, and threat hunting, all designed to enhance preparedness for potential security incidents.

Threat Intelligence

Real-time reputation and threat analysis to stay ahead of attackers.

This comprehensive intelligence-gathering platform combines data from multiple sources, including customer telemetry, open-source communities, and internal research. It provides actionable insights, enabling rapid threat detection, analysis, and response across various security products and environments.

Vulnerability Research

Discovering and disclosing vulnerabilities to improve software security.

This team employs a programmatic approach to discover software and operating system vulnerabilities, averaging more than one finding per working day. They provide immediate protection against zero-day threats while affected vendors develop patches, enhancing customer security during critical periods.

Talos' research powers Cisco's security solutions, providing proactive defense and actionable intelligence for government agencies. By staying ahead of emerging threats, Talos helps ensure a more secure digital future.

Learn more about Cisco Talos

Cisco Services for Government Modernization

Cisco Services provide solutions to help your government agency enhance your security posture. These services offer expert guidance, implementation support, and ongoing assistance to optimize security infrastructure, reduce complexity, and mitigate risks. By leveraging Cisco's extensive experience and cutting-edge technologies, you can strengthen your cybersecurity resilience, streamline operations, and support your compliance efforts.

Learn more about Cisco Services

Consulting Services

Expert guidance to assess, design, and implement security solutions tailored to your organization's specific needs and compliance requirements.

Provides expert guidance to align business needs with technology capabilities. It includes program management, architectural governance, lifecycle management, IT optimization, and domain transformation planning. Consultants assist with strategy development, technology adoption roadmaps, and infrastructure evolution across various architectures.

Packaged Services

Pre-defined service bundles designed to accelerate deployment and adoption of Cisco security solutions, ensuring rapid time-to-value.

Pre-defined solutions simplify deployment, operation, and maintenance for specific needs. They offer streamlined ordering, reduced sales cycles, and cost advantages. Packages may include multiple integrated products and features, providing comprehensive functionality for areas like contact centers or network management.

Support Services

Ongoing hardware, software and solution support to keep your security infrastructure running smoothly and up-to-date with the latest threat intelligence.

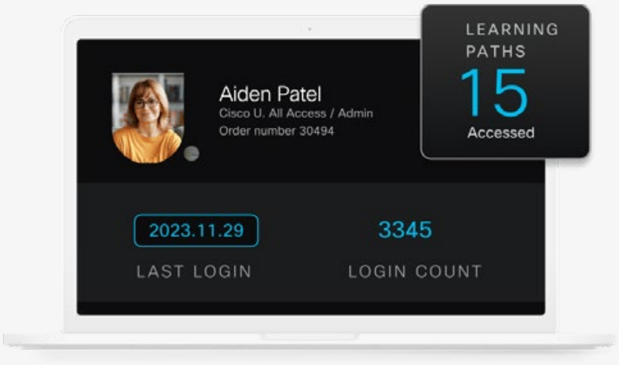
Offers 24/7 access to technical experts, software updates, and online resources. It includes foundational support, issue resolution, and product maintenance to maximize system availability. Options range from basic software support to advanced solution-level services, ensuring smooth operations and ROI for Cisco products.

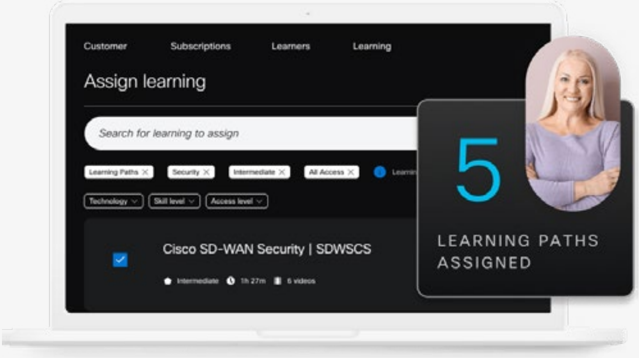
Upskill & Uplevel: Cisco Certifications for Government

Cisco Services for government modernization includes valuable learning and certification opportunities through Cisco Learning Credits (CLCs). These prepaid training vouchers, often bundled with product purchases, enable you to enhance your teams' skills and maximize the value of Cisco solutions. CLCs can be used for instructor-led courses, private training, digital learning, certification prep, exam vouchers, and even attendance at Cisco Live events.

Cisco University, now known as Cisco U., offers a comprehensive digital learning experience tailored to your individual goals. It provides a rich library of technology and certification training, including practice exams and simulators. You can leverage Cisco U. to access a wide range of courses on cybersecurity, networking, programming, and more, ensuring your staff stays current with the latest technological advancements.

By utilizing CLCs and Cisco U. you can efficiently upskill your workforce, accelerate digital transformation efforts, and maintain compliance with evolving security standards. Check out this Cisco Blog on Cisco U.





Get Started

The future of digital government is a continuous journey of innovation and adaptation. As technology evolves, you must remain agile, prioritizing security, compliance, and citizen-centric services. Cisco plays a crucial role in this transformation, providing integrated solutions that enable secure, efficient, and transparent governance.

Key takeaways:

- Embrace AI and automation for enhanced service delivery
- Prioritize cybersecurity and data protection
- Foster cross-border collaboration and interoperability
- Leverage cloud technologies for scalability and flexibility
- Invest in digital skills and literacy for your employees

Remember that digital transformation is an ongoing process. Stay informed and adaptable to meet the evolving needs of your mission.

To learn more about government modernization strategies and solutions:

Visit our Government Modernization webpage

Cisco Partners

Presidio

https://www.presidio.com/

WWT

https://www.wwt.com/

CDWG

https://www.cdwg.com/

Iron Bow

https://ironbow.com/

Red River

https://redriver.com/

ePlus

https://eplus.com/

Netsynch

https://www.netsync.com/

SHI

https://www.shi.com/

Converge Tech

https://convergetp.com/

Additional Resources

Cisco Federal Cloud Computing Strategy Guide

Cisco Federal Government IT Solution Overview

Cisco Solutions for State and Local Government