Cisco Services Catalog: Secure the Enterprise

Prepare, protect, and respond



© 2024 Cisco and/or its affiliates. All rights reserved.

Table of Contents

Assessments/Penetration Testing 6

Technical Security Assessment Services **7**

Cloud and Application Security Assessment Services 7

Security Infrastructure Assessment Services 8

Attack Simulation and Penetration Testing Services 8

IoT/OT Connected Devices Security Assessment Services 9

Strategic Security Advisory Services 10

Cisco Zero Trust Strategy and Analysis Service **11**

Security Advisory Services **11**

Secure Access Service Edge Advisory Service 11

Security Advise and Implement Service 11

Security Segmentation Service 11

Industrial Control Systems Security Assessment 11

Security Program Maturity Assessment 11

Secure Remote Worker SME Consulting Service for Remote Access 11

Automation and Orchestration Services for SecureX 12

Security Risk Management Advisory Services **12**

Information Security Risk Assessment 12

Information Security Risk Program Development 12

Third-Party Risk Program Management Development 12

Third-Party Information Security Assessment 12

Zero Trust Services for Healthcare 13

Security Segmentation Strategy for Medical Devices 13

Secure by Design 13

Data Security and Privacy Framework Service 13

Cisco Lifecycle Services 14

Security Services **15**

Breach Resiliency Service 15

Zero Trust Strategy and Analysis Service 15

Secure Software Supply Chain (DevSecOps) Service 15

Secure Access Service Edge Advisory Service 15

Security Operations Center Services 15

 © 2024 Cisco and/or its affiliates. All rights reserved.

Table of Contents

Plan, Design, and Implement Services 17

Cisco XDR Plan, Design, and Implement Service 18

Cisco Secure Access Service Edge Plan, Design, and Implement Service 18

Cisco Secure Access Strategy and Implementation Service 18

Secure Endpoint Plan and Implement Service 18

Umbrella DNS Security Plan, Design, Implement, and Migrate Service 18

Cloud Security Implementation Service 18

Email and Web Security Implementation Service 19

Next Generation Intrusion Prevention Implementation Service 19

Security Policy and Access Implementation Service 19

Secure Network Analytics Implementation Subscription Service 19

Secure Network Analytics Plan, Design, and Implement Service 19

Network Forensics Automation Service 19

Secure Workload Plan, Design, and Implement Service 20

Secure Workload for SaaS Plan, Design, and Implement Service 20

Secure Workload On-Premises Plan, Design, and Implement Service 20

Security Expert Service 20

Solution Attached Services 21

Secure Firewall Solution Attached Services 22

Identity Services Engine (ISE) Solution Attached Services 22

Cisco Multicloud Defense Plan, Design, and Implementation Service 22

Managed Services 23

Cisco XDR Premier **24**

Secure Managed Detection and Response for Endpoint **24**

Incident Response Services 25

Talos Incident Response Retainer Service **26**

Emergency Response 26

Intel on Demand 26

Incident Response Plans 26

Incident Response Playbook 26

Incident Response Readiness Assessment 26

Tabletop Exercises 26

Compromise Assessment 26

 © 2024 Cisco and/or its affiliates. All rights reserved.

Threat Hunting 26
Cyber Range Training 26
Purple Team Exercise 27
Success Tracks 28
Success Tracks for Integrated Secure Operations 29
Services for Cisco Security Suites 30
Cisco Security Suites Advisory Services 31
Breach Protection Premier 31
Support Services 32
Embedded Support 34
Basic Support 34
Solution Support 34
Enhanced Support 34
Premium Support 34

 © 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Security Services help you stay safe from threats by strengthening your security resilience and reducing complexity and risk so you can deliver uninterrupted, frictionless digital experiences.

The road to achieving security resilience is one littered with challenges from both outside and inside the organization.

The mission of Cisco® Security Services is to help customers like you navigate that road and its challenges to achieve a more robust security program using a lifecycle approach to deliver end-to-end security that meets you where you are in your security maturity.

Our comprehensive security solutions take a three-pronged approach and can help you heighten your security awareness to relative risks (**prepare**), fortify your defenses and turbo-charge security operations (**protect**), and be ready to address the unpredictable (**respond**).

Our services combine human and digital intelligence—so you can prepare, protect, and respond in today's high-risk cybersecurity landscape.

This document is a catalog of Cisco Security Services, organized by category. Each entry includes a high-level description of what the service is, what it does, and the value provided by its outcomes.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Assessments/Penetration Testing

Availability: Global

Assessments and penetration testing services help you prepare for cyberthreats by working to identify vulnerabilities and provide guidance on remediation. Technical assessments can help uncover the gap between perceived versus true security posture. These services are delivered on a project-based consulting basis and can be bought per project, or as a subscription.



 © 2024 Cisco and/or its affiliates. All rights reserved.

Technical Security Assessment Services

These services identify security gaps with the highest risk of breach opportunity, simulate attack scenarios, and execute attack scenarios. Tests contribute to improvements in organizational security posture by identifying security vulnerabilities attackers are likely to exploit. By knowing and addressing your security weaknesses, you are working to prevent future attacks and helping to reduce risk, avoid regulatory fines, and prevent breaches that could potentially be catastrophic.

Cloud and Application Security Assessment Services

Application Penetration Testing

This assessment helps identify and assess an application's immediate attack surface to expose security-related issues and vulnerabilities. We apply a range of analysis techniques and follow a core strategy to document our findings, including prioritized recommendations for your application security and next steps.

Application Security Architecture Assessment

This assessment helps minimize the impact and cost of design decisions that are not secure. We work with you to identify critical architectural vulnerabilities early in your development lifecycle. Through a clear understanding of vulnerabilities, your team can describe an application's risk profile more accurately. You benefit from a secure analysis at the beginning of application development—which helps you avoid costly repairs later in the lifecycle, after development is complete.

Software Development Lifecycle Assessment

This assessment provides an analysis of your application development program. It spans the entire Software Development Lifecycle (SDLC), including security policy development, operational security response planning, and tactical program implementation. This all-encompassing assessment is customized for your environment. We analyze security components within your existing development program and compare your current state to industry best practices. Then, we conduct a risk-based analysis in which we enumerate gaps and create a plan that outlines short-term to long-term improvement objectives.

Cloud Application Migration Assessment

This assessment reviews both the application targeted for migration and the cloud environment being migrated to identify and mitigate insecure design decisions and risks. Through artifact reviews and workshops, we compare your current implementation to the migration plan and target environment to identify where pain points might occur and how to prevent additional risks. By performing this assessment prior to an application's migration, you can prevent costly vulnerabilities before implementation.

DevOps Security Assessment

This assessment evaluates the security of DevOps processes and technologies. It reviews the CI/CD process and systems, testing key components and artifacts. It can include discovering vulnerabilities in application dependencies, code repositories, artifact repositories, build systems, testing environments, infrastructure-as-code, and secrets management, as well as the operations that drive these components.

Cloud Security Architecture Assessment

This assessment evaluates the security of cloud use, architecture, and deployment. It exhaustively identifies the attack surface of cloud-native functionality and systems to reveal high-risk deviations from industry security standards, helping you avoid a cloud-initiated breach.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Security Infrastructure Assessment Services

Network Security Architecture Assessment

This assessment provides a security-focused evaluation of network-based computing environments and concentrates on the security of your network from both an architectural and operational perspective. It helps identify vulnerabilities that exist at the design, deployment, and operational levels of the network.

Device Configuration Security Assessment

This assessment provides a deep dive into the configuration of critical or common builds, to help harden your device configurations against exploits and malicious threats. Cisco experts deploy detailed analysis tools and conduct manual investigation of specific configurations identified by tools and humans. With our findings, you can understand current weaknesses and potential sources of threats in the future. We also help you reliably and safely identify weaknesses that are hard to pinpoint at the network level, so you can prioritize resources where most needed.

Vulnerability Triage

With this assessment, you can offload the tedious work of prioritizing vulnerability remediation. Cisco experts will analyze your vulnerability scan data using machine learning and manual techniques to identify false positives and adjust risk scores—so your team can focus on addressing the vulnerabilities that matter, faster.

Attack Simulation and Penetration Testing Services

Network Penetration Testing

Internal and External Network Penetration Testing provides a practical security evaluation of a specific network by trying to access valuable systems and data to identify exploitable vulnerabilities. This helps uncover vulnerabilities often missed by vulnerability scanning. These tests contribute to improvements in organizational security posture by demonstrating the security weaknesses attackers are likely to exploit and provides the opportunity to remediate them.

Wireless Penetration Testing

This security penetration test identifies weaknesses in wireless configurations that an attacker is likely to exploit and attempts to gain access to your internal assets. The results of the testing help you identify where to strengthen your wireless LAN (WLAN) access to better protect your business.

Physical Penetration Testing

We conduct internal and external network penetration testing that provides a practical security evaluation of a specific network by trying to access valuable systems and data to identify exploitable vulnerabilities. This helps uncover vulnerabilities often missed by vulnerability scanning. These tests contribute to improvements in your organizational security posture by demonstrating the security weaknesses that attackers are likely to exploit.

Social Engineering and Phishing Assessment

This assessment executes simulated phishing campaigns, using text- or voice-based communications to identify individuals likely to be phished, evaluate your prevention measures, and gather metrics on the effectiveness of your organization's security awareness training. We carefully construct each campaign to evaluate perimeter defenses with your oversight, providing an opportunity for your personnel to learn how to avoid becoming a victim of one of the most popular ways remote attackers use to infiltrate networks. At the end of this exercise, your organization will be better prepared for phishing exploits.

Attack Surface Mapping Assessment

This assessment simulates the same discovery methods used by attackers to reveal systems and data that you may not realize are exposed to the internet. It enumerates all organizational legal entities and brands to construct an inventory of exposed on-premises and cloud systems and users, including often forgotten attack vectors like remote workers, supply chain attacks, and wireless. By letting you see what attackers see, this inventory is the first step to ensuring that all your assets exposed to the internet are adequately protected.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Authentication Assessment

This assessment executes simulated credential-guessing attacks to identify default, weak, and breached passwords commonly used to compromise organizations. It uses machine learning to perform advanced credential-stuffing attacks. It can also identify MFA configuration weaknesses and validate if you're able to detect evasive password-spraying attacks. At the end of the assessment, you will have a better understanding of where and how attackers could try to circumvent your perimeter's strongest protection: authentication.

Red Team Threat Simulation

This service models the threat of real-world cybercriminals, but without the risks of a real-world attack. Cisco Security experts use innovative hacking techniques and unique proprietary and public tools to extract sensitive organizational information and test your defenses. Information gained will help drive future security investment where you need it most, to bolster your security posture.

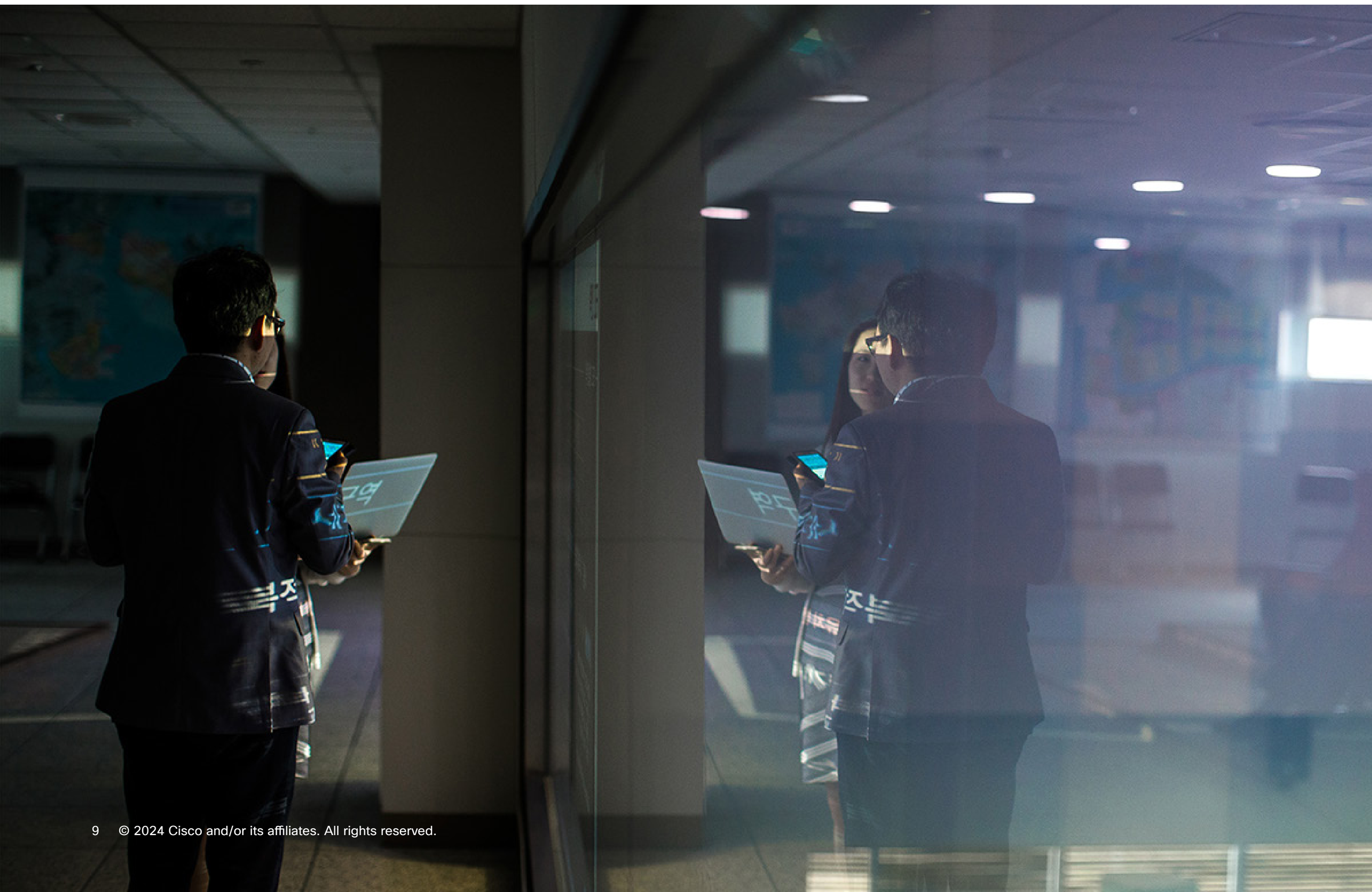
IoT/OT Connected Devices Security Assessment Services

IoT/OT Penetration Test

This penetration test simulates attacks against system components ranging from chips to cloud services. It identifies security issues within the target environment using real-world attack techniques. We investigate these issues and develop remediation strategies to prepare your organization for potential attacks.

IoT/OT Architecture Review

This service performs architecture and code reviews, vulnerability assessments, and application and network penetration tests on your IoT solution. We identify vulnerabilities that exist at the design, deployment, and operational levels so that your organization can apply resources appropriately.



 © 2024 Cisco and/or its affiliates. All rights reserved.

Strategic Security Advisory Services

Availability: Global, except as noted

With this category of security services, Cisco experts work with you strategically through projects to identify and assess IT risks and develop custom security strategies to adapt with your business. These services help you protect your organization from cyber incidents by helping you develop proactive defense systems.



 © 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Zero Trust Strategy and Analysis Service

Availability: AMER only

Our service streamlines your shift to Zero Trust, starting with a detailed assessment of your IT environment. We then tailor a strategic plan to your vision, minimizing financial risks and optimizing costs while enhancing user experience. You receive an analysis of your security, a future-ready architecture, and a concise plan for robust threat protection.

Security Advisory Services

These advisory services deliver holistic views of various IT risks and their potential impact on your operational and financial strategies.

Secure Access Service Edge Advisory Service

Availability: AMER only

This advisory service helps stakeholders understand Secure Access Service Edge (SASE) and relate it to their business requirements. We identify where your organization is already aligned to the SASE model and where an evolved SASE model is most greatly needed, plus we deliver the optimized and personalized strategy to get you there. Outcomes include strategy and analysis alignment, current-state assessment, and product alignment. Additionally, we design a personalized SASE journey roadmap for you, based on the capture and summary of your business requirements. Our service focuses on developing strategies that maximize your alignment with the SASE model, so you can get the most benefit from this powerful framework.

Security Advise and Implement Service

This advisory service helps you develop and deploy a comprehensive security strategy to protect both your data and infrastructure while also addressing your complex business requirements. Working closely with your staff, we assist you in uncovering the existing risks in your network. Then, based on detailed analysis, planning, and change management activities, we recommend actions to strengthen your position.

Security Segmentation Service

This advisory service uses workshops, interviews, and feedback as we work with you to develop a high-level architecture design for your enterprise network security using our Security Segmentation Architecture Design methodology. This analysis helps you create a secure segmentation strategy to protect your network, data, and assets.

Industrial Control Systems Security Assessment

Industrial Control Systems (ICS) assessments evaluate management and strategic processes, operational processes, and technical controls, as well as security risk, compliance, and architectural assessment offerings. Cisco assessment expertise is beneficial for any industry where ICS and IoT are used. Cisco ICS security risk and compliance assessments are vendor agnostic, exceed typical enterprise IT assessment scope, and span multi-industry best practices and national/international standards. Following the assessments, you get recommendations for design and risk mitigation improvements including technologies, device configurations, security controls, segmentation, and zero trust security postures.

Security Program Maturity Assessment

This security assessment reviews your business requirements and assesses the maturity of your security program. With this knowledge, you can confidently move forward to make course corrections or enhancements.

Secure Remote Worker SME Consulting Service for Remote Access

This advisory service provides Cisco Subject Matter Experts (SME) to analyze your existing VPN deployments, determine capacity planning and configurations, and help you manage the incremental workload on your VPN Remote Access network. Our work is based on your current environment and business goals, regardless of the stage of implementation, complexity of your environment, or level of expertise you need. At the end, you get a report with our findings and recommendations aligned with your business objectives and technical requirements.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Automation and Orchestration Services for SecureX

This advisory service helps guide your team in connecting, integrating, and optimizing your security practices while simultaneously accelerating your success with SecureX™. We ensure your SecureX strategy, implementation, and optimization projects are tailored to achieve your business outcomes. The result is a stronger security posture that leverages automation.

Security Infrastructure Advisory

This advisory service identifies the vulnerabilities in your organization's IT infrastructure, network architecture, and configuration and helps you protect information and valuable assets. Service components include assessments for:

- Infrastructure Security Assessment
- Network Security Architecture Assessment
- Configuration Security Assessment

Security Risk Management Advisory Services

These services deliver a holistic view of IT risks and the potential impact on your operational and financial strategies.

Information Security Risk Assessment

This advisory service works with your key IT and business stakeholders to understand your business and technology strategies, objectives, and other critical IT dependencies. Relevant industry trends in technology strategies, regulatory and legal trends, and information security and external threat trends are all considered as we work to mitigate strategic and operational security risks. You get a detailed report that identifies information security risks and provides expert recommendations for improvement. The report covers business processes risk identification, IT architecture, infrastructure, and operational processes that support critical IT asset analysis. It also provides risk treatment options and recommendations for improvements with a roadmap.

Information Security Risk Program Development

This advisory service is customized specifically to your objectives and the status/maturity of your current program. Considering both external and internal risk factors, we gather input from your risk management, compliance, and legal representatives to identify perceptions, behaviors, and obligations concerning IT risk management. You get a detailed report with expert recommendations to close identified gaps. It also covers detailed process enhancements, IT risk reporting, and suggested updates to reporting templates.

Third-Party Risk Program Management Development

This service can help your organizations better understand and manage third-party risk, including the multiple vendors your organization may rely on to support business operations. Through a comprehensive approach, your organization can better understand and manage third-party risk. We help identify the information needed to balance risk and opportunity through due diligence, program development, and assessment services. You receive a detailed report with expert insights on the current state of third-party risk management processes, a prioritized risk profile and sample relationships overview, and a third-party risk management improvement roadmap.

Third-Party Information Security Assessment

This assessment examines your organization's business context, data, products, and services through a questionnaire and reviews of relevant documentation related to security. It also covers the performance of an assessment at a third-party facility, including inspections, interviews, observation of controls, and validation of questionnaire responses. The result is an assessment report that provides a third-party security scorecard, detailed assessment findings with prioritized risks and recommendations, and detailed control findings.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Zero Trust Services for Healthcare

Availability: AMER

This advisory service can help your healthcare organization understand and visualize what a zero trust future can look like. We factor in the uniqueness of your organization's environment, analyze current capabilities, and advise on the best zero trust approach. Your staff gains access to Cisco experts who examine your current infrastructure and map your capabilities to your end-state goals. Our services help you identify areas for improvement as well strategic opportunities for business growth.

Security Segmentation Strategy for Medical Devices

Availability: AMER

This advisory service helps healthcare organizations secure their Internet of Medical Things (IoMT) by minimizing the risk and liability caused by cyberattacks, protecting critical business and patient operations, and preventing medical device breaches. Cisco can help your organization design and build secure, segmented networks to better protect administrative and research networks, medical devices, guest wireless devices, and more from cybersecurity threats. This helps your organization maintain a robust security posture and keep assets and reputation safe.

Secure by Design

Availability: EMEA

This assessment examines your organization's current and planned technology investments to ensure maximum return and avoid non-strategic investments. We go through a series of analyses and steps to help rapidly develop a strategic implementation plan that maximizes investment and adoption, aligns technology to specific security standards (such as NIST and MITRE) and meets your desired strategic outcomes. At the end of the engagement, you get a prioritized implementation and adoption plan to help ensure that each technology is integrated and contributes towards the same outcome, while also outlining key strategic technology gaps.

Data Security and Privacy Framework Service

Availability: EMEA

This service helps architect an industry-aligned data security and privacy program to meet your needs with solutions that enable your business objectives. Using a prioritized and cost-effective approach, the framework provides a roadmap and overall categorization and progress tracking of your desired cybersecurity activities and outcomes, designed to be intuitive to enable simple, non-technical communication between multi-disciplinary teams. The result is a cybersecurity and data privacy program that meets the changing requirements of your risk, regulation, operations, and business objectives.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Lifecycle Services

Availability: Global, unless otherwise noted

With Cisco Lifecycle Services experts on your side, we help fortify and secure your network for resiliency and agility, so you can prepare and protect your organization from threats and vulnerabilities.

We begin by helping translate your IT initiatives into measurable business outcomes and KPIs that strengthen security across the infrastructure. To get to outcomes faster, our experts provide an outcomes-based journey customized to your unique needs. We also share digital insights, including telemetry-based AI/ML, tools, automation, and best practices to pinpoint security gaps. And our measurement and reporting tools provide the data needed to continually monitor progress and validate results.

Our flexible engagement model lets you choose how you engage with Cisco. Our experts can advise you, work alongside your IT experts and partner teams, or direct and manage the entire engagement. Plus, you gain access to the right expertise, resources, capabilities, and technologies at each step of your journey.



 © 2024 Cisco and/or its affiliates. All rights reserved.

Security Services

Breach Resiliency Service

This service identifies security vulnerabilities with the highest breach potential to minimize risk and improve your security posture. It also simulates and executes attack scenarios, providing assessments and prioritized recommendations to effectively address business risk and gaps in your security portfolio.

Zero Trust Strategy and Analysis Service

This service kickstarts your zero-trust journey by examining your organization's IT infrastructure, current capabilities, and environment (campus, data center, off-premises, cloud, etc.). With your desired future state as a guide, we help develop a multi-year strategy to achieve your zero-trust goals. Outcomes include a reduction in financial risks, an optimized business model (CapEx to OpEx), and enhanced user experience. This service can also assess your organization's current security capabilities and target architecture and provide a roadmap to ensure you have the most comprehensive and up-to-date protection against potential threats.

Secure Software Supply Chain (DevSecOps) Service

This service is built on an organizational software engineering culture and fabric that combines and automates the practices of development (Dev), security (Sec), and operations (Ops). Our goal is to help you achieve agile and safe deployments. Our service can help you speed the time to change/deploy and achieve regulatory compliance faster with built-in security. With robust automation, your IT teams can minimize risk to improve operational efficiencies and scale faster, freeing up time to focus on more complex matters.

Secure Access Service Edge Advisory Service

This service helps you understand Secure Access Service Edge (SASE) and align it with your current business requirements. To begin, we asssss where your organization is already aligned to the SASE model and determine where SASE model improvements are needed. We then deliver a customized strategy and solution roadmap to get you where you need to be and help you realize maximum benefit from this powerful framework. Service outcomes include strategy and analysis alignment, current-state assessment, and product alignment.

Security Operations Center Services

With our Security Operations Center (SOC) Services, your IT teams benefit from Cisco's deep security expertise to ensure your SOC is effective, efficient, and optimized for your business. Through workshops and ongoing reviews with experienced SOC experts, we help you create an optimal SOC solution that allows you to vigilantly prepare, protect, and respond to security threats and breaches.

SOC Automation Readiness Assessment Service

Availability: EMEA

A Security Operations Center (SOC) is an in-house or outsourced team of IT security professionals tasked with monitoring, detecting, and responding to cyberthreats. To assess your SOC's readiness for automation, our experts continuously analyze your network and systems for suspicious activity and look for opportunities to increase response times to potential issues that arise. Service features include automation playbooks, reporting capabilities, and automation tools to create and maintain automations.

SOC Optimization Service

Availability: EMEA

This service provides a comprehensive assessment of your Security Operations Center (SOC), including its potential for automation. Our experts use a collaborative educational approach, including workshops and reviews with security operations experts, to assess the capabilities of your SOC. Your team gets an actionable roadmap and recommendations to mitigate weaknesses and optimize SOC performance, along with a playbook aligned with automation standards.

 © 2024 Cisco and/or its affiliates. All rights reserved.

SOC Capability Assessment Service

Availability: EMEA

This service provides an independent assessment and coaching workshop to document the capabilities and performance of your Security Operations Center (SOC). We gather details about your organization's SOC requirements, situation, and performance. Our documented findings are provided to you in an actionable plan and roadmap that you can use to mitigate SOC-related issues swiftly.

SOC Planning Service

Availability: EMEA

This planning service provides a Security Operations Center (SOC) strategy and roadmap, based on your organization's desired outcomes and the SOC services required to deliver the strategy. Through a series of collaborative workshops and reviews, our SOC experts work with you to identify gaps and opportunities in your strategy to optimize your SOC solution. We also provide a three-year roadmap, SOC vision and mission statements, high-level SOC service catalog, and detailed insights into compliance monitoring to maximize resiliency.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Plan, Design, and Implement Services

Availability: Global, unless otherwise noted

Plan, Design, and Implement (PDI) Services help you protect against cyberthreats by providing expert guidance to assist your organization with proactive technology refreshes and migrations.



 © 2024 Cisco and/or its affiliates. All rights reserved.

Cisco XDR Plan, Design, and Implement Service

This service helps ensure that your Cisco Extended Detection and Response (XDR) deployment excels in effectiveness, efficiency, and optimization. We deliver expert guidance for planning, design, and implementation, tailored specifically to your organization's unique needs. Our seasoned specialists stand ready to bolster your security posture with comprehensive expertise in Cisco XDR, across all critical areas: endpoints, email, cloud, network, and applications. The result? A powerful Cisco XDR security solution built for you.

Cisco Secure Access Service Edge Plan, Design, and Implement Service

Availability: AMER only

This service provides your organization with expert guidance into Secure Access Service Edge (SASE) core functions and elements, and we work to implement and integrate a SASE solution that meets your unique business needs. Our service helps you accelerate your journey to a SASE in a secure and agile manner.

Cisco Secure Access Strategy and Implementation Service

This service helps ensure a flawless, effective deployment of Cisco Secure Access. Tailored to your specific business and technical requirements, our experts provide guidance and recommendations for strategic planning, precision design, and effortless migration of a zero-trust security solution.

Secure Endpoint Plan and Implement Service

This service addresses common risks to a successful Secure Endpoint deployment, such as unfamiliarity with a new product, incomplete feature activation, and slow time to value. It is offered in an easy, fixed-price, limited scope for both large and small deployments.

- **Large deployment:** We deploy, configure, tune, and test a pilot implementation of Secure Endpoint and perform a connector package push to up to 25,000 endpoints as an initial production deployment.
- **Small deployment:** Cisco experts deploy, configure, tune, and test a pilot implementation of Secure Endpoint and perform a connector package push to up to 5,000 endpoints as an initial production deployment.

With either option, you can significantly improve your security operations effectiveness by eliminating complexity and enhancing staff productivity.

Umbrella DNS Security Plan, Design, Implement, and Migrate Service

This service provides the expert assistance you need to get your organization's Umbrella DNS deployment right, aligned to your business goals, the first time. Cisco experts closely work with you through design development and planning, pilot implementation, testing, and migration to help ensure success and accelerate time to value of your cloud security solution.

Network Device Security Assessment

The Network Device Security Assessment (NDSA) helps protect your organization against old and new threats. Consultants with extensive security experience and expertise review your Cisco infrastructure and configurations to help determine gaps in your security. We use best-in-class tools and methodologies, and our highly experienced security engineers have knowledge of your industry and vertical and understand your Cisco products inside and out. Their guidance can help you take advantage of all the sophisticated security features in your Cisco infrastructure, with immediate and ongoing support so you can better protect your organization's assets.

Cloud Security Implementation Service

This implementation service brings the expertise you need to support your cloud security project. Our experts work with you to understand your business and technical goals and develop a consensus set of requirements that guide the implementation. Then, using our knowledge gained from millions of installations globally, we use Cisco best practices to develop the designs, plan, provide documentation, perform testing and migration, and educate your team—all of which underpin a successful implementation project.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Email and Web Security Implementation Service

This service assists in gathering your organization's requirements to help design and implement a secure email and/or web solution. The email solution is based on Cisco Secure Email (formerly Email Security Appliance, or ESA) and, optionally, a Content Security Management Appliance (CSMA). This may include integration with Cisco Registered Envelope Service (CRES). The web solution is based on a Cisco Secure Web Appliance (formerly Web Security Appliance, or WSA). This service reduces adoption times by getting your technology installed, migrated, and adopted quickly. And with frequent updates from Cisco Talos® threat intelligence, your organization can feel secure.

Next Generation Firewall Implementation Service (Transactional)

This implementation service delivers expertise to help you get your Next Generation Firewall (NGFW) security solution up and running quickly and successfully. We work based on your current environment and business goals, regardless of the stage of implementation, complexity of your environment, or level of expertise you need. We help you tune the firewall settings for optimal performance, so you can achieve your operational goals. If we identify gaps between your requirements and the implemented solution, we work to address them and make sure you get the most from your investment. You gain the value of the full range of Cisco expertise available to you at any point in your implementation.

Next Generation Intrusion Prevention Implementation Service

This service helps accelerate the time to value of your Next Generation Intrusion Prevention System (NGIPS) security solution by providing expert assistance across the breadth of the project. From design development and implementation planning through installation, we work with you to configure and optimize your network security technologies. With Cisco expert support for implementation, migration, and final testing, you can rest assured that your security solution works right the first time and is in place to bolster your security posture.

Security Policy and Access Implementation Service

This service can help you quickly get your new policy and access solution—such as Identity Services Engine (ISE) and AnyConnect® VPN—up and running quickly. Our expert security consultants use tested sets of tools and best practices and plan your implementation project, starting from understanding your requirements through to post-project consulting, if you desire. By leveraging Cisco expertise, you can ease the strain on your internal team and help ensure a fast, cost-efficient implementation project that bolsters your defenses.

Secure Network Analytics Implementation Subscription Service

This service helps you implement your Cisco Secure Network Analytics (SNA) solution with expert Cisco assistance. We help you develop implementation plans as well as install, configure, and integrate SNA in your environment. This service also addresses common risks to a successful implementation, such as lack of expertise, incomplete product knowledge, and time constraints. Leveraging this service, you can better realize SNA's complete value in your security strategy.

Secure Network Analytics Plan, Design, and Implement Service

This service helps get your network or cloud Cisco Secure Network Analytics (formerly Stealthwatch®) solution deployed, configured, and tuned properly. We assist with initial planning, installation, integration, maintenance, and troubleshooting. Our mission is to help you achieve the most value from your purchase and accelerate visibility and other key outcomes strongly aligned with your unique business requirements.

Network Forensics Automation Service

This service extends the value of your Cisco Secure Network Analytics solution by helping enable threat hunting, incident response, audit, and compliance. Cisco experts help you quickly define and implement automation use cases that will deliver the maximum value for your unique workflows. With our service, you can scale your solution, accelerate tasks, and deliver better outcomes.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Secure Workload Plan, Design, and Implement Service

With this implementation service, we help you transform your operations from perimeter-only to more pervasive, enterprise-wide security with the expert implementation of Cisco Secure Workload (formerly Tetration®). We help you secure your environment using firewalls at the workload level, across your entire infrastructure, so you can defend beyond the perimeter by closing significant visibility gaps and healing critical vulnerabilities to prevent attacks.

Secure Workload for SaaS Plan, Design, and Implement Service

This service helps ensure that your Secure Workload (formerly Tetration) solution is designed for your environment, answers your challenges, meets your needs, and helps you achieve the best results from its visibility and enforcement capabilities. We work with you to understand your business objectives and technical requirements and select the applications to be placed under enforcement and visibility. We document this in a Solution Requirements Document. Then, we conduct a comprehensive remote design workshop and draft a solution design based on the findings. You receive a Solution Design Document that describes the applications, workloads, and how Cisco will deploy Secure Workload in this context and aligned with the Solution Requirements Document.

After reviewing information and conducting a workshop to discuss implementation strategy and finalize scenarios, we implement your Cisco products to specification, implement Secure Workload policy and visibility on selected applications, and perform integrations. And we continue providing consultative support and knowledge transfer to you after implementation, helping set your team up for success. This service is delivered by our experts in a fixed, price-limited scope deployment.

Secure Workload On-Premises Plan, Design, and Implement Service

Cisco Secure Workload On-Premises Predefined Solution Plan, Design, and Implement Service (Large) helps ensure that your organization's Secure Workload (formerly Tetration) solution is designed for your environment, addresses your challenges, and meets your needs. Delivered by our experts in a fixed, price-limited scope deployment, this service helps you achieve the best results from Secure Workload's visibility and enforcement capabilities.

Security Migration Service

This migration service helps take you from your current security environment to a more innovative security infrastructure. We strive to provide proactive ongoing protection as we work to give you a clear understanding of the risks in your current environment and deliver what we believe to be your best migration strategy.

Security Expert Service

This service addresses your needs for Cisco Security products when you don't have in-house expertise. Hiring, training, and retaining talent with specialized security skills is costly. So, if you're not using a specialty on a regular basis, it just makes more sense to bring in a highly qualified, deeply experienced expert for only the times you need it. You can use our experts for staff augmentation and hands-on assistance for internal projects, as well as reactive support for breaches, outages, and other network emergencies.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Solution Attached Services

Availability: Global, restrictions apply

Cisco Solution Attached Services are consulting-led, year-round subscription services that provide strategic expert guidance for your Cisco solution, from planning and design to implementation and more. You choose the service level that best fits your organization's needs: select Advise Me to get strategic guidance from Cisco experts, Do It With Me for collaborative execution by your team along with Cisco, or Do It For Me if you want Cisco to handle it all.



 © 2024 Cisco and/or its affiliates. All rights reserved.

Secure Firewall Solution Attached Services

These services expedite adoption and optimize the value of Cisco Secure Firewall, equipping you to tackle your urgent security challenges and realize maximized returns on your investment. You gain year-round access to Cisco experts who are focused on streamlining onboarding and continually optimizing your operations – helping you rapidly adapt and improve your defenses against the most sophisticated cybersecurity threats.

Identity Services Engine (ISE) Solution Attached Services

These services facilitate rapid adoption and full utilization of your ISE security solution by ensuring that your network access policies are robust, adaptive, and address your most critical challenges. From onboarding through continuous enhancement of your network and security operations, our expertise helps you extract maximum value from ISE, so you can stay agile and vigilant against the latest threats.

Cisco Multicloud Defense Plan, Design, and Implementation Service

Our service guarantees that your Cisco Multicloud Defense deployment achieves unparalleled consistency, efficiency, and optimization. We provide specialized expertise in planning, designing, and implementing solutions that are custom-fitted to your organization's unique hybrid or multicloud strategy. Our experienced professionals are committed to streamlining and automating your security across every environment, ensuring vigilant protection that is tailored to your needs.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Managed Services

Availability: Global, restrictions apply

Cisco Managed Services SecOps offers combine elite teams of researchers, investigators, and responders with integrated threat intelligence to detect and contain threats faster while delivering relevant and prioritized response actions.

Our services leverage defined investigations and response playbooks supported by Cisco Talos threat research. With our managed SecOps offers, you can protect against cyberthreats and safeguard from damage to your organization's assets or reputation.



 © 2024 Cisco and/or its affiliates. All rights reserved.

Cisco XDR Premier

This premier license tier provides Managed Extended Detection and Response (MXDR) powered by Cisco and delivered by an elite team of Cisco security experts. Using a combination of Cisco's elite team of researchers, investigators, and responders, Cisco XDR, integrated tool sets, and additional Cisco security technologies, our MXDR solution monitors for and responds to potential cyberthreats and breaches. This service includes integration support for Cisco security solutions and Cisco-curated integrations with select third-party security tools, as well as Cisco Software Support Services (SWSS) Enhanced. It also provides security assessment, validation, and enhancement through Cisco Technical Security Assessment (CTSA) and select Cisco Talos Incident Response (Talos IR) services.

Secure Managed Detection and Response for Endpoint

Secure Managed Detection and Reponse (MDR) for Endpoint is a managed offer that monitors telemetry from the Secure Endpoint, 24x7x365, from Cisco's global Security Operations Centers. Secure MDR for Endpoint combines human and machine intelligence to reduce endpoint detection and response tasks and times. Secure MDR for Endpoint accelerates threat detection and response and delivers relevant, prioritized response actions to bolster your organization's response to known and emerging cyberthreats.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Incident Response Services

Availability: Global, restrictions apply

The Talos Incident Response (Cisco Talos IR) Retainer Service is a suite of proactive and emergency services to help your organization robustly respond to and recover from a security incident.

We can help you gain greater visibility into threats from our vast telemetry sources, access threat intelligence and insights, and develop operational rigor and faster response capabilities to bolster your security posture.



 © 2024 Cisco and/or its affiliates. All rights reserved.

Talos Incident Response Retainer Service

Availability: Globally, with restrictions

Retainer hours can be allocated to the services described below.

Emergency Response

This service provides emergency response support to assist you during security incidents. We will be available within hours to triage, coordinate, investigate, and provide expert guidance on containment and remediation activities for a security incident. This helps your organization recover quickly and gracefully to minimize harm to your reputation or bottom line.

Intel on Demand

This service empowers your team with relevant security knowledge. We work along with Talos Intelligence Analysts to provide you with the latest threat intelligence and net-new, custom research based on your organization's relevant contextual factors. With this information, you can bolster your security team's defenses.

Incident Response Plans

This service helps you develop or improve your incident response plans, tailored to your organization's needs, to support coordinated response and communication processes in case of a security incident. These incident response plans are foundational to enable your organization to work together, as one team, to respond effectively to an incident.

Incident Response Playbook

This service helps your team plan for responding to security incidents. We help you develop or improve playbooks to document step-by-step response workflows for common threats relevant to your organization. By leveraging Talos IR's real-world expertise and industry-leading best practices for playbooks, you can feel confident that your organization is well-prepared for a variety of common threats.

Incident Response Readiness Assessment

This service helps you assess how ready your organization is to respond effectively to security incidents. We assess the current state of your organization's incident response capabilities by identifying strengths and opportunities. You receive actionable recommendations to optimize your security posture and improve your organization's overall incident readiness.

Tabletop Exercises

This service allows your team to put your incident response processes into practice. We design and facilitate scenarios, based on real-world incidents, to enable various levels of your organization to practice their roles. These scenarios also familiarize them with documented processes and identify improvements for the overall incident response strategy.

Compromise Assessment

This service helps you identify potential indicators of compromise on your network and its systems. We partner with you to perform a high-level assessment, and then we provide a final report with detailed results and prioritized recommendations that your team can implement.

Threat Hunting

This service provides a review of specific areas of your organization's network and its systems for potential indicators of compromise. Our hypothesis-driven threat hunting is backed by the most current threat intelligence available from Cisco Talos.

Cyber Range Training

This service provides an immersive three-day, hands-on workshop with practical, real-world exercises to prepare defenders to respond to security incidents using digital forensic and incident response techniques. Your team will learn necessary skills and techniques to better combat cyberthreats, improve analysis collaboration, and improve your organization's incident response capabilities.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Purple Team Exercise

This service empowers your team to enhance your prevention, detection, and response capabilities. Your team will collaborate side-by-side with us to identify simulated adversarial activity. By leveraging Talos IR, your team can better understand your available detection methods as well as increase familiarization with specific adversarial tactics, techniques, and procedures.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Success Tracks

Availability: Global, restrictions apply

Success Tracks is a comprehensive suite of customer success services designed to expedite adoption and maximize value realization by bringing six critical success factors to IT: visibility, insights and analytics from advanced AI/ML, premium support, use case-driven guided journeys, on-demand access to expertise, and contextual learning. You gain access to Success Tracks capabilities through CX Cloud, our unified digital experience platform.



 © 2024 Cisco and/or its affiliates. All rights reserved.

Success Tracks for Integrated Secure Operations

Success Tracks helps you quickly adopt and maximize the value of your Cisco Secure Endpoint investment and accelerate business value. We do this by delivering the right expertise, insights, learning, and support with a guided lifecycle journey through CX Cloud, our one-stop unified digital experience. You gain more knowledge and insights in a completely new way, taking you from a reactive mindset to addressing problems to being more proactive and predictive in managing IT operations throughout your product lifecycle.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Services for Cisco Security Suites

Availability: Global, restrictions apply

Cisco Security Suites are focused collections of prescribed point products that help customers reach a security outcome in their technical environments: Breach Protection, User Protection, Cloud Protection.

CX has aligned the Enhanced and Premium tiers of the Cisco Software Support Services (SWSS) offer to the initial Suites (August 2023). SWSS helps you fast-track Security Suite solution value by shortening the onboarding timeline and technology adoption to accelerate realization of business value and return on security investment. And should there be a problem, the Cisco Support TAC coordinates multiproduct issue support to solve complex issues fast.

In addition, Cisco Advanced Services has both Strategic Advisory Services and Plan, Design, and Implement offers that can help you develop custom strategies as well as manage technology refreshes and migrations.



 © 202 Cisco and/or its affiliates. All rights reserved.

Cisco Security Suites Advisory Services

These advisory services offer specialized guidance to help you optimize your specific Cisco Security Suites deployment. Our services accelerate deployments through project definition, assessments, and process documentation to help you effectively achieve your desired security objectives while maximizing your investment returns. Cisco experts navigate you through understanding the Suites, aligning to your goals and objectives, and developing an agreed-upon roadmap on how to best deploy Suites capabilities. Through a partnership with us, you can enhance your operational agility and secure the delivery of successful outcomes.

Breach Protection Premier

This premier license tier provides Managed Extended Detection and Response (MXDR) powered by Cisco. Cisco MXDR monitors for and responds to potential security threats and breaches by leveraging a combination of Cisco's researchers, investigators, and responders with Cisco XDR, integrated tool sets, and additional Cisco security technologies. Delivered by an elite team of Cisco security experts, this service includes integration support for Cisco security solutions and Cisco-curated integrations with select third-party security tools. It also includes Cisco Software Support Services (SWSS) Enhanced; security assessment, validation, and enhancement through Cisco Technical Security Assessment (CTSA); and select Cisco Talos Incident Response (Talos IR) services.

 © 2024 Cisco and/or its affiliates. All rights reserved.

Support Services

Availability: Global

Cisco offers Support Services for hardware, software, and solutions. We can help you protect your organization from cybersecurity threats by maintaining system uptime, solving complex multi-vendor issues, and providing a top-notch user-experience.



 © 2024 Cisco and/or its affiliates. All rights reserved.

← Is service available á la carte? →

Security Subscriptions	Embedded (8x5 online only)	Basic (24x7 TAC)	Solution Support	Enhanced	Premium
Secure Firewall (On-Prem)		Yes		Yes	Yes
Secure Firewall Virtual (FTDv)	Yes		Yes		
Secure Workload TaaS	Yes		Yes		
Secure Email (On-Prem and Cloud)		Yes	Yes	Yes	Yes
Cloud Mailbox Defense		Yes	Yes	Yes	Yes
Secure Web		Yes	Yes	Yes	Yes
Secure Endpoint		Yes	Yes	Yes	Yes
Secure Malware Analytics SaaS		Yes	Yes	Yes	Yes
Secure Network Analytics	Yes		Yes	Yes	Yes
Secure Cloud Analytics	Yes		Yes		
SAL (On-Prem)		Yes	Yes		
SAL SaaS	Yes		Yes		
Telemetry Broker (CTB)				Yes	Yes
Cisco Identity Services Engine (ISE)		Yes		Yes	Yes
Cisco Umbrella®		Yes		Yes	Yes
Cisco Cloudlock®		Yes		Yes	
Cisco Secure Access by Duo	Yes (Duo-specific)		Yes	No	Yes
Cisco AnyConnect®		Yes		Yes	Yes
Kenna Security	Yes (Kenna-specific)			Yes	Yes

 © 2024 Cisco and/or its affiliates. All rights reserved.

Embedded Support

This support level provides Cisco Technical Assistance Center (TAC) access for support and troubleshooting via online tools and web case submission only. Telephone case submission is not included with this option.

It also includes access to Cisco. com. This system provides technical and general information on Cisco products and access to Cisco's online Software Central library. Cisco may sometimes identify access restrictions.

Basic Support

This support level provides all the features of Embedded Support, plus Cisco TAC access 24 hours per day, 7 days per week, to assist you with application software use and with troubleshooting issues, either by telephone or via online tools/web cases. Support cases are prioritized over cases associated with Embedded option.

Solution Support

This support level provides all the features of Basic Support, **plus:**

- When technical Support Services for the product are bundled with Solution Support, Cisco will provide the services described in the Cisco Responsibilities of the relevant technical support Service Descriptions for the Cisco products that comprise the solution.
- To the extent allowed by our Solution Support Alliance Partners, Cisco will provide technical issue management for issues encountered with the solution.
- In the event Cisco determines escalation to a Solution Support Alliance Partner for Third Party Product support is necessary, Cisco will work with you and the applicable Solution Support Alliance Partner to open a case in the Solution Support Alliance Partner's case management system using your entitlement to support with the Solution Support Alliance Partner.

Enhanced Support

This support level provides all the features of Solution Support, **plus:**

- Direct access to skilled engineer with solution level expertise
- Multiproduct/multivendor support coordination
- Entitlement for guidance for Smart Account structure setup and software license activation
- Configuration Support to provide advice and process guidance for maintaining consistency of the application software performance in your IT environment
- Routing of all software issue resolution TAC cases submitted to a team of TAC experts for reactive case handling
- Initial meeting to understand your desired outcomes to define an IT and InfoSec Adoption Plan
- Periodic technical status reviews (at Cisco's discretion)
- Entitlement for support associated with integrating the application software into your IT environment
- Ongoing guidance to your help desk personnel in providing internal support to users of the application software

For security, access to certain deliverables such as activation support, configuration guidance, and periodic technical status reviews may be provided digitally or by a technical resource depending on the minimum spend, which is set at each product level.

Premium Support

This level provides all the features of Enhanced Support, **plus:**

- Designated Service Management (DSM) of the covered products by a technical subject matter expert during local business hours
- Entitlement for support under DSM, which utilizes customer information such as current environment, software configuration, operation workflows, and IT and Infosec adoption plan to provide technical consultations
- Advanced entitlement for support for lifecycle management

 © 2024 Cisco and/or its affiliates. All rights reserved.

Support Service	Technical Support Coverage	**Response Time** Objective for Case Severity 1 and 2	**Response Time** Objective for Case Severity 3 and 4
Embedded	Email/web	N/A	Within next business day, local standard business hours
Basic	24x7 via phone and email/web	Within 1 hour	Within next business day
Solution Support	24x7 via phone and email/web	Within 30 minutes	Within 1 hour*
Enhanced	24x7 via phone and email/web	Within 30 minutes	Within 2 hours*
Premium	24x7 via phone and email/web	Within 15 minutes	Within 1 hour*

*For Severity 3 and Severity 4 calls received outside of Business Hours, Cisco will respond within the Next Business Day (NBD).

 © 2024 Cisco and/or its affiliates. All rights reserved.

Learning and Certifications

Cisco Learning and Certifications provide the training and skills validation that IT practitioners need to take part in security and cybersecurity teams, and to help your organization prepare, protect, and respond to cybersecurity threats.



 © 2024 Cisco and/or its affiliates. All rights reserved

Understanding the full scope of a technology roadmap must include knowing what skills are present within your teams. Planning an as-is/to-be technology transformation must include how the implementation will be performed, and by whom. By analyzing this with a Cisco Learning BDM, you can understand what services are most needed—now and in the future.

Cisco-trained technicians also lead to faster business outcomes, quicker troubleshooting resolution, and reduced downtime. When working together with Cisco CX teams, Cisco training creates a common vocabulary among our team and your IT practitioners, improving communication and reducing risks. The best way to reduce skills gaps is to contract the required skills with Cisco CX and, at the same time, build in-house skills with Cisco Learning and Certifications, to help realize better business and technical outcomes, such as:

- Urgent use cases are addressed rapidly.
- Skills gaps are quickly resolved.
- Faster, smoother transformations get started while in-house practitioners are trained.
- ROI is realized sooner and with clearer visibility of future technical and skill needs.
- In-house technicians who receive needed training are much more likely to remain.
- In-house practitioners have the necessary vocabulary to work closely with Cisco engineers for better outcomes, now and in the future.
- There's reduced troubleshooting since both Cisco and your teams are skilled in deployed technologies.
- Knowledge transfers are far easier and more complete.

Cisco U.

Give your team the sharpest skills with Cisco U., the source for learning about Cisco and adjacent tech. Cisco U. combines the knowledge of experts and the support of a community with personalized recommendations, so your team can learn as efficiently as possible.

With Cisco U., your team can get answers to real-world questions, improve their tech skills, and be part of a growing network of like-minded tech learners and pros. Invest in your teams to give your business an edge, and help them gain knowledge for tomorrow's technology needs, today.

Grow your team's knowledge into your greatest business asset with Cisco U.

Cisco Learning Credits

Cisco Learning Credits (CLC) are prepaid vouchers you can use to plan and pay for Cisco training and exams. They're an ideal way to allocate training dollars toward immediate and long-term training goals. CLCs make it easy to include training as part of a total solution with the purchase of Cisco products and services. Organizations can budget for training needs by making decisions at the point of the product/technology sale or saving CLCs to plan for training later based on the type of training you need, specific timeline, and who will attend.

We all know it's easier to get CapEx budget at the time of infrastructure purchase when you are buying the complete solution and not waiting for those hard-to-get OpEx funds to come through. Furthermore, each CLC comes with a Learning BDM who serves as a subject matter expert to help you determine training, create plans to ensure your success, and assist in redeeming your CLCs.

Course and skills-validation highlights for security and cybersecurity include:

- Cisco Security Course Overviews
- Cisco Security Certifications Overview
- CyberOps Training
- The Cisco Learning Network: CyberOps Training Videos
- Cisco Security Community
- Cisco CyberOps Community

 © 2024 Cisco and/or its affiliates. All rights reserved.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.