Modernising Cybersecurity for EU and UK Public Sector

Contents

Protecting Essential Services and Public Trust

Public sector organisations across Europe and the United Kingdom deliver essential services that communities depend on every day, from healthcare and transportation to education and public administration. As these services become increasingly digital and interconnected, cybersecurity has become foundational to service continuity, public safety, and trust in public institutions.

Modernisation is expanding connectivity across cloud services, legacy systems, shared platforms, and third-party providers—improving efficiency while also increasing cyber risk. Service disruption, data compromise, or loss of availability can have immediate societal impact, placing pressure on public sector organisations to protect critical services while meeting stringent regulatory expectations and operating within complex governance environments.

This solution brief is designed to help public-sector leaders, security practitioners, and IT teams navigate cybersecurity modernisation with clarity and confidence. It outlines key risks shaping today's environments and presents practical approaches to strengthening security and resilience—supporting essential services and sustaining public trust as digital platforms evolve.

Navigating the Compliance Maze

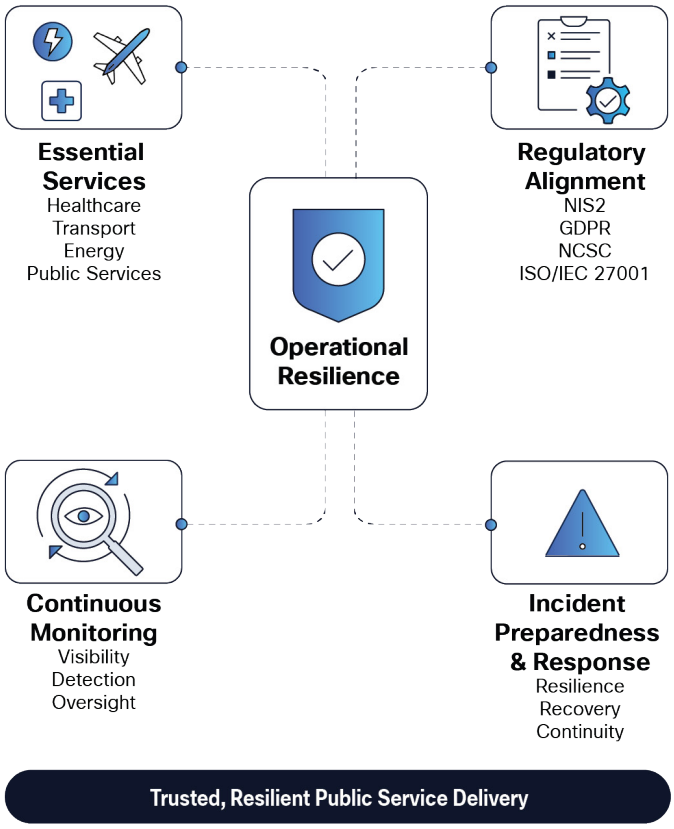
Public sector organisations across the EU and UK operate within a complex and evolving regulatory landscape designed to protect essential services, sensitive data, and public trust. Cybersecurity obligations span EU directives, national guidance, and international standards, with a shared emphasis on risk management, resilience, and accountability—requiring organisations to balance strong protections with operational flexibility.

The NIS2 Directive introduces a strengthened framework for improving cybersecurity and operational resilience across essential and important entities, with increased focus on incident management, supply-chain risk, and governance. Alongside NIS2, GDPR continues to define requirements for protecting personal data and ensuring transparency across both EU member states and the UK. In the UK, NCSC guidance provides authoritative direction on secure architecture, risk management, and operational practices for public-sector organisations.

To manage this complexity, many public-sector organisations align regulatory requirements to internationally recognised standards such as ISO/IEC 27001, establishing a common foundation for security governance, control alignment, and audit readiness. At the same time, organisations are monitoring emerging European initiatives—including ENISA-led assurance frameworks, evolving cybersecurity certification schemes, and regulatory measures such as the Cyber Resilience Act—which aim to strengthen trust and consistency across digital services and supply chains—while supporting risk-based digital sovereignty rather than rigid, one-size-fits-all controls.

As regulatory expectations continue to evolve, public-sector organisations are increasingly focused on operationalising compliance—embedding security, monitoring, and resilience into everyday operations instead of treating compliance as a point-in-time exercise. This approach supports sustained resilience, reduces manual effort, and enables secure modernisation as public sector services and digital platforms expand.

Operational Resilience as a Foundation



Zero Trust as a Foundation

As public sector organisations continue to modernise, traditional perimeter-based security models are no longer sufficient. Cloud adoption, hybrid environments, shared services, and third-party integrations have dissolved clear network boundaries, increasing exposure to risks such as credential compromise, lateral movement, and service disruption. In this context, implicit trust based on location or network access introduces unacceptable risk for essential public services.

Zero Trust provides a practical, risk-based approach by replacing assumed trust with continuous verification. Access decisions are informed by identity, device posture, application context, and observed behaviour—helping organisations reduce risk while maintaining service availability and regulatory accountability. This model aligns closely with EU and UK cybersecurity expectations, which emphasise proportional controls, resilience, and governance rather than static, one-time compliance.

Core Zero Trust Principles

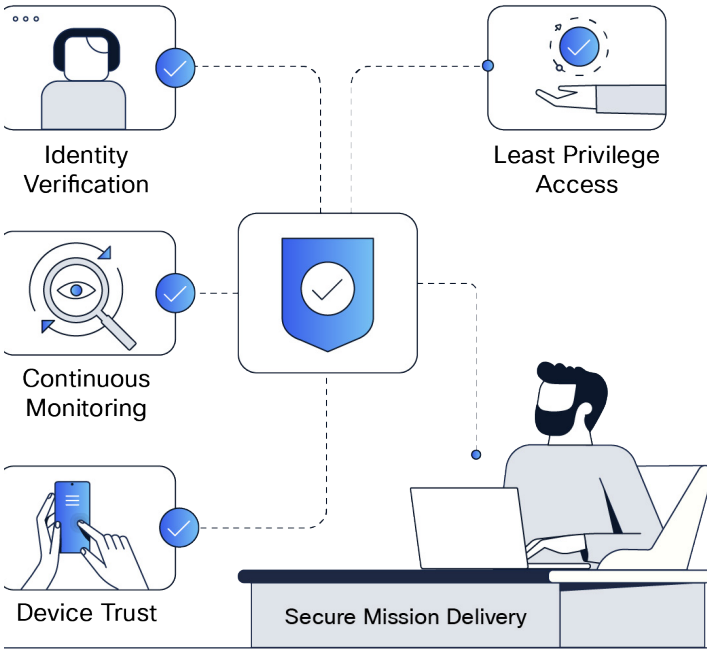
When applied consistently, Zero Trust helps public sector organisations strengthen security and resilience by focusing on a small set of foundational principles:

- **Verify explicitly** using identity, device, and context
- **Apply least-privilege access** to limit exposure
- **Assume breach** and design for detection, containment, and recovery

These principles support risk-based digital sovereignty, enabling organisations to maintain control and oversight across distributed environments without resorting to rigid or isolating security models.

.

Zero Trust as a Foundation



From Policy Alignment to Operational Practice

Zero Trust is most effective when it moves beyond policy guidance and becomes part of everyday operations. Continuous monitoring, shared visibility, and automation enable organisations to evaluate risk dynamically, adapt controls in real time, and respond consistently across hybrid and shared environments.

For public sector organisations, operationalising Zero Trust supports broader objectives such as service continuity, regulatory alignment, and sustained public trust. By embedding Zero Trust principles across identity, access, and security operations, organisations can apply controls proportionate to risk while maintaining secure, resilient public services as digital platforms and regulatory expectations evolve.

Zero Trust Adoption

While Zero Trust principles are broadly recognised, adoption across public sector organisations is shaped by diverse operating environments, shared services, and varying levels of digital maturity. Rather than a single prescriptive architecture, Zero Trust is most effective when implemented as a progressive, risk-based approach that can be adapted across departments, agencies, and service providers..

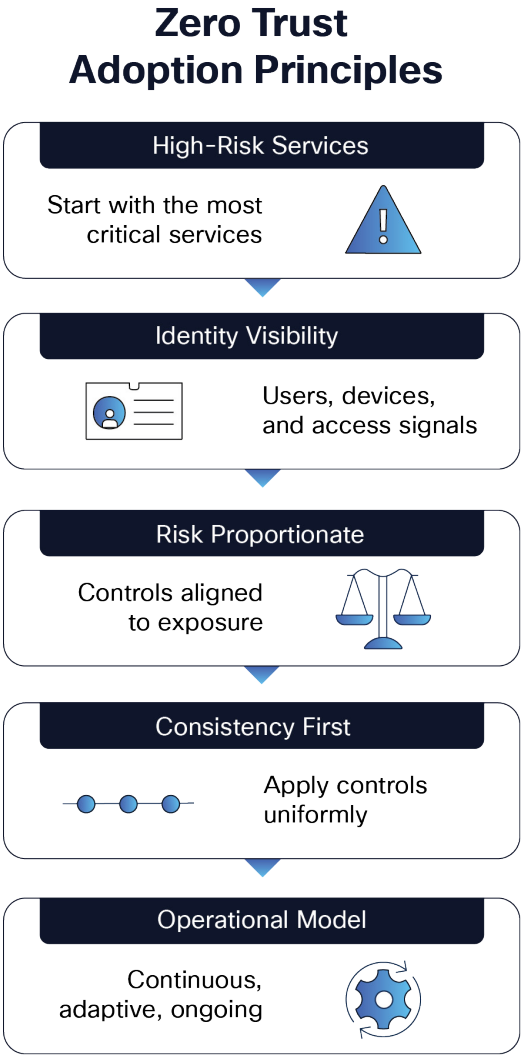
Public sector organisations typically align Zero Trust implementation to established security architecture concepts and regulatory expectations, applying controls proportionate to risk and service criticality. This allows organisations to strengthen security and resilience while maintaining flexibility and avoiding unnecessary complexity or disruption.

Implementing Zero Trust in Practice

Zero Trust adoption in public sector environments commonly focuses on phased improvements that support operational priorities and regulatory accountability. Typical areas of focus include:

- Strengthening identity and access controls to ensure only trusted users and devices can access services
- Improving visibility across environments to support monitoring, detection, and oversight
- Applying consistent policies across cloud, on-premises, and shared platforms
- Expanding automation and response capabilities as maturity increases

This phased approach allows organisations to demonstrate measurable progress, align security controls to evolving requirements, and improve resilience over time. By treating Zero Trust as an ongoing operational model rather than a one-time initiative, public sector organisations can reduce risk across interconnected environments while sustaining secure, reliable service delivery as digital services continue to expand.



Cyber Risks at National and Sector Scale

Public sector organisations face cyber risks whose impact extends beyond individual systems to affect essential services, economic activity, and public trust. As digital services become more interconnected, cyber risk must be assessed and managed at both organisational and sector scale.

Ransomware and Service Disruption

- Disruption of essential services
- Pressure for rapid recovery
- Societal and economic impact

Legacy and Hybrid Environment Complexity

- Aging infrastructure dependencies
- Inconsistent security controls
- Limited end-to-end visibility

Supply Chain and Third-Party Risk

- Dependency on external providers
- Inherited platform vulnerabilities
- Limited third-party visibility

Shared and Cross-Sector Services

- Interconnected public services
- Expanded incident blast radius
- Complex response coordination

Identity and Credential Compromise

- Phishing and account takeover
- Diverse user populations
- Weak access signal correlation

Resource Constraints and Skills Gaps

- Limited specialised resources
- High alert volumes
- Manual investigation effort

Integrated Security by Design

Public sector organisations operate complex digital environments spanning identity systems, networks, cloud platforms, applications, and shared services. Securing these environments requires more than isolated controls—it requires an integrated security approach that delivers shared visibility, context, and coordinated action across the entire service landscape.

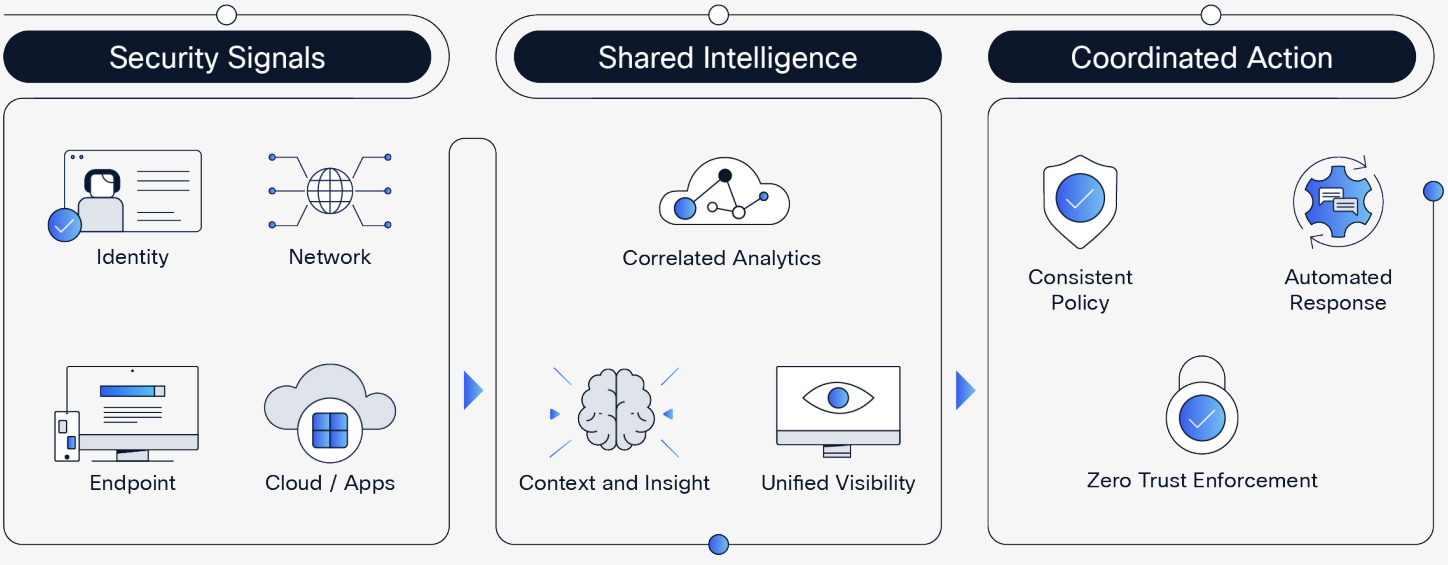
Integrated security by design embeds protection, monitoring, and response into everyday operations. By connecting security signals and controls across environments, organisations can reduce fragmentation, apply policies consistently, and support continuous oversight aligned to risk-based regulatory expectations.

An integrated security approach enables organisations to drive coordinated action across environments by:

- Unifying visibility across environments
- Applying policies consistently
- Correlating risk in context
- Coordinating detection and response
- Reducing operational complexity

Built on a platform-based model, integrated security allows organisations to move from isolated insight to coordinated action—strengthening Zero Trust adoption, improving resilience, and maintaining service continuity across hybrid and shared environments.

Turning Security Signals to Coordinated Action



From Intelligence to Coordinated Action

Visibility alone is not sufficient in complex public sector environments. Organisations must be able to translate security intelligence into timely, coordinated action across users, devices, networks, applications, and data.

By correlating signals across security domains, organisations gain context that enables faster detection, more consistent policy enforcement, and effective response—reducing disruption and supporting the continuity of essential services.

The Value of an Integrated Platform

An integrated security platform helps organisations manage complexity while improving outcomes. By connecting protection, analytics, and response capabilities, organisations gain a shared operational view of risk across hybrid and shared environments.

An integrated platform enables organisations to:

- Unify visibility across domains
- Respond faster with context
- Apply policies consistently
- Reduce operational overhead

This approach allows security teams to focus on protecting services rather than managing disconnected tools.

Foundation for Service-Ready Security

Integrated security serves as the foundation for service-ready protection, ensuring that availability, resilience, and trust are prioritized rather than sacrificed for delivery speed. By embedding security into everyday operations, organisations can strengthen Zero Trust adoption and maintain oversight as environments evolve.

This foundation supports secure service delivery across shared platforms, third-party dependencies, and hybrid infrastructure while remaining aligned to risk-based regulatory expectations.

Cisco Security Reference Architecture

Cisco's approach is guided by the Cisco Security Reference Architecture, an outcomes-focused framework that aligns security capabilities across identity, network, endpoint, cloud, and application domains.

Rather than prescribing implementation specifics, the architecture helps organisations understand how controls, visibility, and response work together as a system—supporting consistent enforcement, prioritised risk management, and coordinated action across public sector environments.

Service-Ready Security Solutions for Public Sector Resilience

Public sector organisations require security solutions that not only protect against evolving threats, but also support service availability, regulatory accountability, and public trust. As digital services increasingly rely on cloud platforms, shared infrastructure, and third-party providers, security must operate consistently across environments—without compromising sovereignty, control, or transparency.

Cisco delivers a service-ready security portfolio designed for highly regulated public-sector environments. Built on open architectures and interoperable platforms, Cisco's approach supports risk-based digital sovereignty—enabling organisations to maintain control over data, policy, and operations while continuing to benefit from cloud innovation and global technology ecosystems.

Cisco Security Cloud

At the core of this approach is Cisco Security Cloud, a unified, open platform that connects security capabilities across identity, network, cloud, applications, and operations. By bringing together shared telemetry, analytics, and policy enforcement, Cisco Security Cloud enables organisations to understand risk in context and take coordinated action across distributed environments.

Cisco Security Cloud helps organisations:

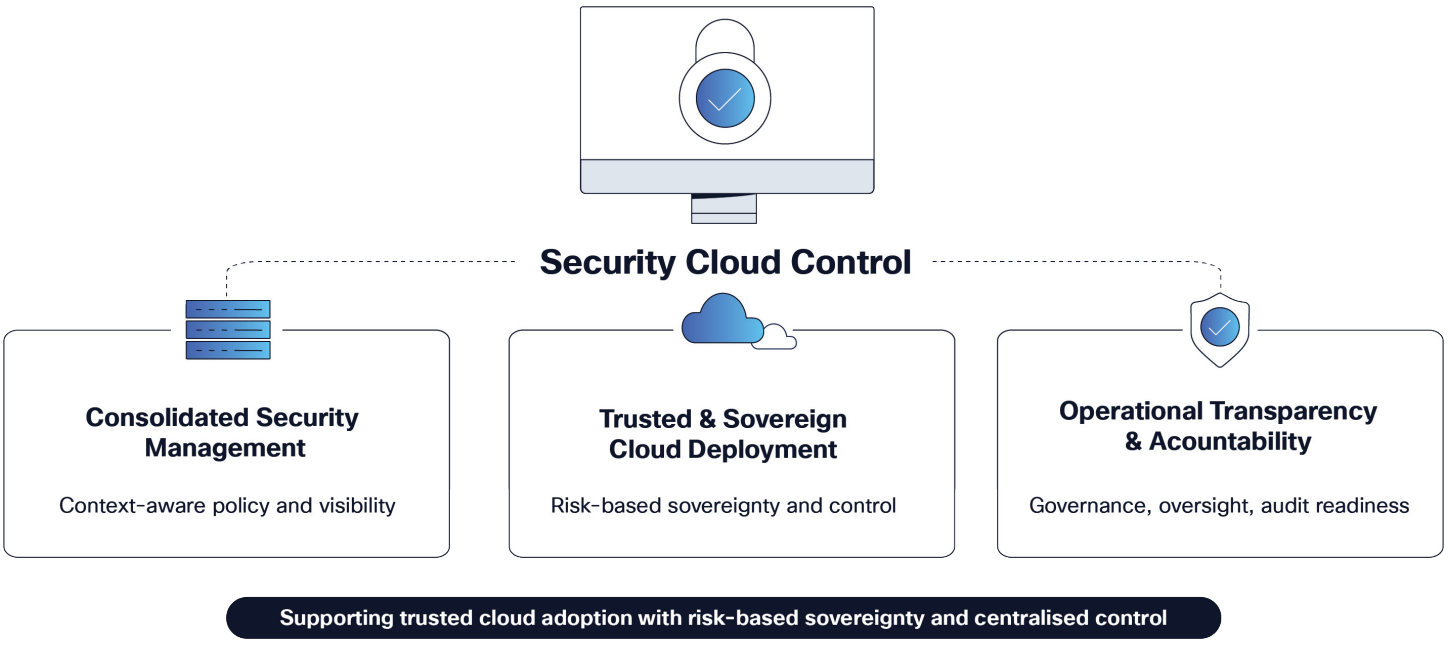
- Unify security operations
- Apply consistent policies
- Correlate risk across domains
- Accelerate detection and response
- Reduce operational complexity

Supporting Trusted and Sovereign Cloud Strategies

Across Europe and the UK, public sector cloud strategies increasingly prioritise trust, transparency, and sovereignty. Cisco's security solutions are designed to support a wide range of deployment models—including sovereign, hybrid, and multi-cloud environments—while maintaining consistent security controls and governance.

By enabling strong security and visibility regardless of where workloads reside, Cisco helps public sector organisations demonstrate accountability, support regulatory expectations, and preserve operational choice. This risk-based approach to sovereignty allows organisations to modernise securely without isolating themselves from innovation or interoperability.

Together, Cisco's service-ready security solutions provide a resilient foundation for modern public services—supporting secure modernisation, trusted cloud adoption, and sustained public confidence as digital environments continue to evolve.



The Cisco Security Portfolio

Cisco delivers a comprehensive, integrated security portfolio designed to support cybersecurity modernisation across complex, hybrid environments. Built to operate as a cohesive system rather than isolated tools, the Cisco Security portfolio helps organisations apply consistent Zero Trust principles, strengthen visibility, and reduce operational complexity as services, threats, and environments continue to evolve.

The following sections highlight how Cisco's security capabilities are organised to support public sector needs, including:

- **Network, cloud, and application security** to protect highly distributed infrastructures
- **Identity, access, and user security** to support Zero Trust-aligned access decisions
- **Threat detection, response, and analytics** to accelerate investigation and response
- **Integrated security suites** that simplify deployment and operational consistency

Together, these capabilities provide the building blocks needed to operationalise Zero Trust, support compliance, and maintain resilience—while allowing security to scale as needs and requirements change.

Network, Cloud, and Application Security

Public sector organisations operate distributed environments spanning on-premises infrastructure, cloud platforms, and shared applications. Cisco's network, cloud, and application security capabilities provide consistent protection and visibility to support resilient service delivery across hybrid environments.

Cisco Secure Firewall
Provides advanced threat prevention, intrusion detection, and policy enforcement across on premises, cloud, and hybrid environments with unified management and AI driven detection.

Cisco Hybrid Mesh Firewall
Delivers consistent security enforcement and centralised policy management across distributed environments, simplifying segmentation and threat protection at scale.

Cisco Security Cloud Control
Centralises management and policy enforcement across Cisco security technologies deployed on-premises and in the cloud. By providing unified visibility and orchestration, Security Cloud Control helps organisations manage security operations more consistently across distributed environments.

Cisco Identity Services Engine (ISE)
Provides centralised identity and access control by enforcing policy decisions based on user identity, device posture, and contextual signals. ISE supports Zero Trust-aligned access enforcement across wired, wireless, and remote access environments.

Cisco Multicloud Defense
Enables centralised security policy enforcement and visibility across AWS, Azure, and GCP environments, supporting consistent controls in multicloud architectures.

Cisco Umbrella
A cloud-delivered security service that provides DNS-layer protection, secure web gateway, firewall, and cloud access security functionality. Umbrella helps block malicious destinations early in the attack chain and supports consistent policy enforcement for users across distributed environments.

Cisco AI Defense
Helps organisations address risks associated with the use of artificial intelligence by monitoring, protecting, and governing AI-driven applications and workflows. By providing visibility into AI usage and enforcing policy controls, AI Defense supports responsible adoption and operational oversight of AI technologies in regulated environments.

Cisco Secure Workload
Provides deep visibility and zero trust microsegmentation for applications across data center and cloud environments, reducing attack surfaces and limiting lateral movement.

Cisco Hypershield
Provides distributed, kernel-level enforcement using eBPF technology to deliver high-performance, context-aware segmentation and protection across modern, highly dynamic environments.

Cisco Web Application and API Protection (WAAP)
Protects web applications and APIs from threats such as DDoS attacks, API abuse, and automated attacks across hybrid and multicloud deployments.

Cisco Secure DDoS Protection
Helps mitigate denial-of-service attacks that target network and application availability, supporting resilient mission operations across hybrid environments.

Identity, Access, and User Security

Public sector organisations rely on identity-centric security to control access to critical systems and services. Cisco's identity and access capabilities help verify users and devices, reduce credential-based risk, and support Zero Trust-aligned access across distributed environments.

Cisco Duo
Provides phishing resistant multi-factor authentication and device trust to ensure only verified users and healthy devices can access regulated systems and applications. Duo supports adaptive, risk-based access decisions aligned to Zero Trust principles.

Cisco Secure Access (SSE)
A cloud-delivered secure access service that combines Zero Trust Network Access (ZTNA), secure web gateway, CASB, and firewall as a service capabilities to protect users, data, and applications regardless of location.

Cisco Secure Client
Delivers unified secure connectivity, posture assessment, and Zero Trust access for users across any device or location, supporting regulated work environments and mission continuity.

Cisco Secure Endpoint
Provides advanced endpoint detection and response (EDR) capabilities to detect, investigate, and remediate malware and advanced threats in real time.

Cisco Secure Email Threat Defense (ETD)
Helps protect users from phishing, credential theft, and account-based attacks that commonly target email as an initial access vector. By detecting malicious email activity and reducing identity compromise, ETD supports stronger user trust signals and helps limit the risk of unauthorised access in regulated environments.

Threat Detection, Response, and Analytics

Effective threat detection and response in public sector environments requires visibility across multiple security domains. Cisco and Splunk help organisations correlate activity, prioritize risks, and respond more efficiently—supporting service continuity with limited resources.

Cisco XDR
Correlates telemetry across endpoint, network, cloud, email, and identity domains to accelerate detection, investigation, and response using automation and AI driven analytics.

Cisco Secure Network Analytics (SNA)
Delivers agentless network visibility and behavioral analytics to detect threats across on premises and cloud environments, including encrypted traffic.

Cisco Secure Malware Analytics
Provides advanced malware analysis by detonating suspicious files in a controlled environment to observe behavior and indicators of compromise. These insights help security teams better understand threats and support investigation and response activities.

Cisco Telemetry Broker
Enables organisations to collect, normalize, and distribute network telemetry across security and analytics tools. By improving access to high-quality data, Telemetry Broker helps support visibility, analytics, and informed decision-making across complex environments.

Cisco Security Analytics and Logging
Centralizes security telemetry and log management to support investigations, compliance reporting, and analytics driven operations.

Splunk SOAR
Automates security workflows and incident response through playbooks and orchestration, reducing response times and analyst workloads.

Splunk Enterprise Security (ES)
Splunk's SIEM solution provides AI-powered analytics to support detection, investigation, and response across complex environments. ES correlates data from infrastructure, applications, and security tools to improve visibility and support informed security operations at scale.

Splunk User Behavior Analytics (UBA)
Uses machine learning to identify insider threats, compromised accounts, and abnormal behavioral patterns across users and entities.

Visibility, Intelligence, and Operational Insight

Strong cybersecurity operations depend on visibility beyond individual tools. Cisco's visibility and intelligence capabilities help organisations gain insight across networks, cloud services, and external dependencies to support informed, timely decisions.

Cisco Talos Threat Intelligence
Talos Threat Intelligence provides real time global threat intelligence that informs detection, prevention, and response across Cisco security technologies.

ThousandEyes
ThousandEyes delivers end to end visibility across networks and cloud services, helping organisations distinguish between performance issues and security incidents affecting service delivery.

Cisco Security Suites

Cisco Security Suites simplify adoption and operations for public sector organisations by delivering integrated security capabilities in cohesive offerings. These suites reduce complexity while supporting consistent enforcement and scalable Zero Trust adoption.

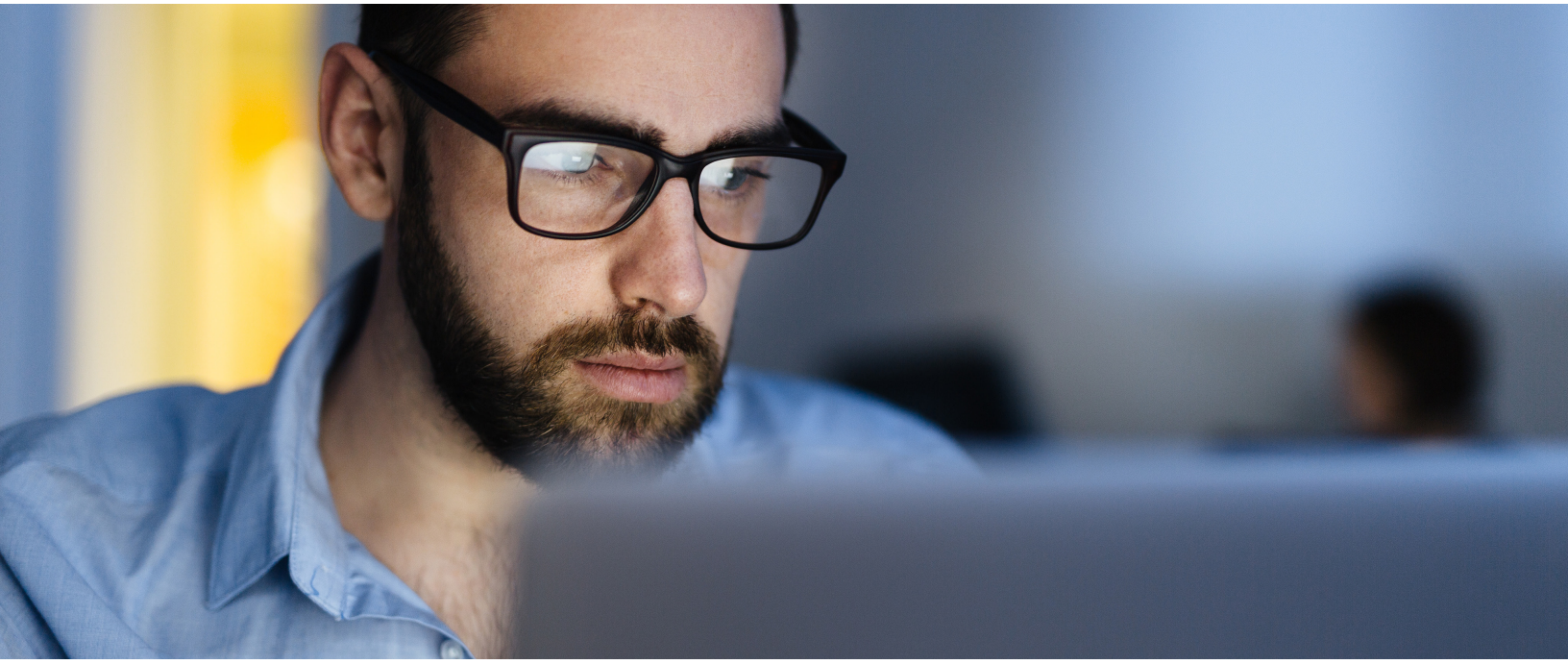
Cisco Breach Protection Suite
Provides threat detection, investigation, and response across endpoints, network, email, identity, and cloud environments using AI-assisted analytics and shared telemetry. By correlating signals across domains, the suite helps organisations prioritise threats and support more efficient incident response.

Cisco User Protection Suite
Combines identity protection, secure access, and endpoint defences to help reduce credential-based risk and unauthorised access. The suite supports adaptive access decisions aligned with Zero Trust principles across distributed environments.

Cisco User and Breach Protection Suite
Combines identity protection and advanced threat detection into a single integrated offering. By correlating telemetry across users, endpoints, networks, and cloud environments, the suite supports unified visibility and more coordinated response while reducing operational complexity.

Cisco Cloud Protection Suite
Provides integrated security controls to protect applications and data across hybrid and multicloud environments. The suite supports segmentation, gateway-based protection, and consistent policy enforcement to reduce attack surfaces and limit unauthorised access.

By simplifying security operations across distributed environments, the suite helps maintain visibility and apply Zero Trust–aligned controls consistently.



Cisco Services: Turning Strategy into Action

Cisco Services help government agencies translate cybersecurity strategy into effective, day-to-day operations. Delivered across a unified services portfolio, Cisco Services support organisations at key points in the security lifecycle—helping them assess risk, design secure architectures, and respond confidently to evolving threats.

By combining deep public sector expertise with AI-driven insights from CiscoIQ, Cisco Services help organisations better understand their environments, prioritise actions, and continuously improve security outcomes across complex, regulated infrastructures.

Advisory and Assessment Services

Helps organisations evaluate their current security posture, identify gaps and risks, and define actionable roadmaps aligned to regulatory drivers.

- **Zero Trust Advisory**
  Helps organisations assess current Zero Trust maturity and define a practical roadmap. The engagement identifies strengths, gaps, and dependencies across identity, devices, applications, and networks, and delivers prioritised recommendations to support incremental, enforceable adoption.

- **Advanced Persistent Threat Resiliency Assessment**
  Evaluates defensive readiness against sophisticated adversaries using threat-informed analysis. This assessment identifies architectural weaknesses, policy gaps, and exposure pathways, translating technical findings into prioritised actions that strengthen resilience and reduce attack surface.

- **AI Security Trust and Assurance Program**
  Provides visibility into AI usage, including shadow AI, unmanaged models, and undocumented pipelines. Cisco experts assess security controls, data flows, and risk posture, delivering a clear, data-driven roadmap to support secure, trusted, and scalable AI adoption.

Plan, Design, and Implement Services

Provides hands-on expertise to design and implement security capabilities that align to Zero Trust and resiliency objectives across hybrid environments.

- **Application Microsegmentation Service**
  Helps organisations design and implement application-level segmentation policies to protect critical workloads on-premises and in the cloud. This service reduces lateral movement, limits blast radius during incidents, and supports consistent enforcement without disrupting operations.

Incident Response Services

Helps organisations prepare for, respond to, and recover from cyber incidents—combining readiness activities, real-time intelligence, and expert-led response to minimize impact and restore operations quickly.

- **Talos Incident Response**
  Rapid, expert support during active cyber incidents. Cisco Talos Incident Response provides 24x7x365 access to experienced responders who assist with triage, investigation, containment, and remediation—working alongside response teams and across shared environments when incidents span multiple organisations.
- **Talos Proactive Services**
  Structured services designed to assess, plan, and test incident response readiness. These services include readiness assessments, tabletop exercises, threat hunting, logging reviews, and tailored incident response playbooks to help organisations strengthen preparedness before incidents occur.
- **Talos Threat Intelligence**
  Real-time threat analysis and reputation data to help organisations stay ahead of emerging threats. Cisco Talos intelligence combines large-scale telemetry with open-source and proprietary research to support faster detection, investigation, and response across security operations.
- **Talos Vulnerability Research**
  Continuous discovery and responsible disclosure of software and operating system vulnerabilities. Talos researchers provide early protection against zero-day threats while fixes are developed, strengthening overall security and resilience.

Flexible Engagement Models

Cisco Services are available through flexible engagement models, including subscription-based services for ongoing needs and project-based engagements for targeted initiatives. This flexibility allows organisations to align service delivery with mission priorities, budgets, and acquisition requirements—while maintaining ownership of architecture decisions and compliance outcomes.

To engage Cisco Services and learn more about available offerings, organisations can work with their Cisco account team or an authorised Cisco partner.

Public Sector Cloud Trust and Authorizations

Public sector organisations establish trust in cloud services through a multi-layered assurance model, rather than a single central authorisation program. Cloud trust is grounded in regulatory obligations, national guidance, recognised standards, and operational transparency—supporting risk-based decision-making, accountability, and confidence in digital services.

Public sector cloud trust is typically supported by:

- **Regulatory Obligations**
  EU and national regulations—including NIS2 and GDPR—define baseline requirements for cybersecurity risk management, resilience, and data protection across essential and important entities.

- **National Guidance and Oversight**
  Authorities such as the UK National Cyber Security Centre provide practical guidance on secure cloud adoption, architecture, and operational practices for public sector environments.

- **International Standards**
  Frameworks such as ISO/IEC 27001 offer a common foundation for security governance, control alignment, and audit readiness across diverse organisations and jurisdictions.

- **Emerging European Assurance Initiatives**
  ENISA-led frameworks, cybersecurity certification schemes, and regulatory measures such as the Cyber Resilience Act aim to improve consistency, transparency, and trust across cloud services and digital supply chains.

Together, these layers enable a risk-based approach to digital sovereignty—supporting strong oversight and control while allowing organisations to retain flexibility, choice, and access to innovation as cloud strategies evolve.

Public Sector Cloud Trust and Assurance

Regulatory Obligations

fining requirements for ecurity, resilience, and data protection

National Guidance and Oversight

Providing principles for secure cloud adoption and operations

International Standards

Aligning governance and controls across jurisdictions

Emerging European Assurance Initiatives

Improving consistency and transparency across cloud services

Cloud trust is built on regulation, standards, and operational transparency.

Upskill & Uplevel: Building Public Sector Cyber Skills

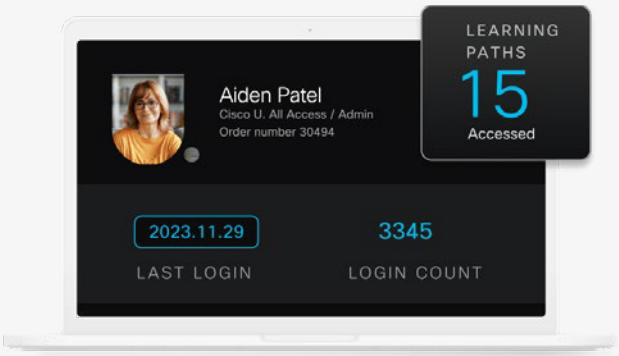
Effective cybersecurity depends not only on technology, but on the skills and capabilities of the people who operate it. Public sector organisations across the UK and Europe face growing pressure to strengthen cyber resilience while managing constrained resources, evolving regulatory requirements, and increasingly complex digital environments.

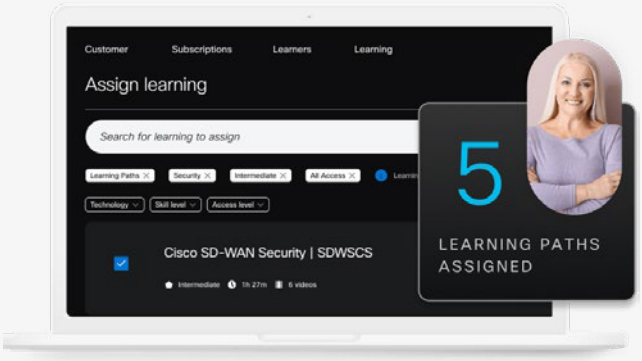
As services become more distributed and security models shift toward Zero Trust, organisations require skills spanning networking, identity, cloud, security operations, analytics, and incident response. Developing these capabilities helps reduce risk, improve response effectiveness, and support long-term resilience.

Cisco supports public sector upskilling through flexible learning programmes aligned to real-world operational needs. Cisco Networking Academy helps organisations develop foundational cybersecurity and networking skills, while Cisco U. provides role-based learning paths, hands-on labs, certification preparation, and continuous learning opportunities for technical teams.

By investing in ongoing skills development, public sector organisations can strengthen their security posture, support regulatory expectations for competence and preparedness, and enable teams to operate with confidence across modern, integrated environments.

Explore learning opportunities for skills development, industry-recognised certification, and direct product training to help your organisation thrive in today's digital economy.





Getting Started with Cisco

Modernising cybersecurity is an ongoing effort that must evolve alongside public sector services, technologies, and regulatory expectations. As digital environments become more distributed, organisations benefit from a practical, phased approach that prioritises essential services, manages risk proportionately, and strengthens resilience over time.

Cisco supports organisations by helping assess current security capabilities, identify priority risks, and align integrated security architectures to operational and compliance needs. This approach enables organisations to modernise securely while maintaining transparency, control, and continuity of service.

Next Steps

Public sector organisations can begin or advance their cybersecurity modernisation journey by focusing on incremental, risk-based improvements rather than large-scale transformation initiatives. By prioritising high-impact services and shared environments, organisations can make measurable progress while limiting disruption.

Working with Cisco and its partner ecosystem, organisations can align integrated security platforms, trusted cloud strategies, and skills development to support Zero Trust adoption, operational resilience, and regulatory accountability. This approach enables secure modernisation that remains flexible as technologies, threats, and policy requirements continue to evolve.

Resources

- Cisco Sovereign Critical Infrastructure
- Cisco in Government
- Cisco Modernizing Government Cybersecurity
- Cisco Framework Mappings

Cisco Partners

Cisco works with a broad ecosystem of authorised partners to support organisations across planning, deployment, and ongoing operations. To find a qualified public sector partner, visit the Cisco Partner Locator on our website.