cisco SECURE

Modern, efficient cybersecurity for Government

Cisco Secure Architecture for the Federal Government

Service to your citizens is your mission

Government networks are vital, and technology is everywhere. Your job is to keep systems running so that nothing interrupts vital services to your citizens. Cybersecurity, privacy, compliance are on your plate too. So is planning for a future of endless growth and constant change. That's asking a lot of you and your small team.

You can do it, and we can help.

The Cisco Secure Architecture for the Federal Government combines advanced security with modern networking, making it simple, scalable, and manageable. Whether in the cloud or on premises – or both – we'll help you build and grow the safe and secure learning environment you need for today and tomorrow.

It’s not complicated

Architecture sounds imposing, but it really isn’t. While we have a lot to offer, we first listen to your needs and help you prioritize. You can dramatically improve your security posture today with targeted investments. Just take it a step at a time.

Already have something specific on your mind? Click the chart to learn about it right now.

Or read on, and we’ll quickly guide you through our security architecture. You’ll see how simple it is.

Cloud

User & endpoint

- Device security
- Strong authentication
- Mobile device management
- Modern VPN client

Email & web

- Phishing prevention
- Ransomeware defense
- Web content filtering
- CIPA compliance

On-premises

Network security

- Software-defined access
- Secure remote access
- Firewall & DDos migration
- Visibility & analytics

Physical security

- Smart cameras

It's based on zero trust

Remember when we thought we could trust everything inside our networks? Today, we assume the opposite. We think and act like attackers are always present on our networks.

That's why we built our security architecture on zero trust principles. We ensure people are who they say they are, we check devices for threats, and we apply least privilege access everywhere.

And we continually monitor and verify trust: Any unusual or suspicious activity automatically triggers trust level changes that limit potential threats without having to shut things down.

Establish Trust

- Multi-factor authentication
- Device posture & vulnerabilities

Continuously Verify Trust

- Risk behavior monitoring
- Dynamic trust level changes

Enforce Trust-Based Access

- Least privilege authorization
- Workload communications

Cloud security

No doubt you're already adopting cloud-based applications for communication, payroll, HR and more. It makes sense: Cloud vendors say they have the resources and expertise to continually deliver the latest features, maintain system uptime, and scale without limit.

Cisco Secure cloud solutions deliver on those promises.

We design and build the most advanced, modern cloud security solutions for your community. You can achieve the security posture you've always dreamed about, without the budget nightmares that have always held you back.

Umbrella

Block harmful web content from reaching employee. It's the security centerpiece of our Secure Access Service Edge (SASE) solution.

Secure Email Cloud Mailbox

Stop advanced email threats with our solution that's fully integrated into Microsoft Office 365. It catches what Office 365 misses.

Secure Access by Duo

Prevent stolen credentials from becoming big problems with multifactor authentication. The Duo Mobile app helps keep mobile devices secure too.

SecureX

Integrate and automate your security solutions in one place with our built-in platform -- at no added cost. Radically reduce dwell time and human-powered tasks.

On-premises security

Despite cloud adoption, your local network is here to stay. Your users will always have things to connect on premises, and you're bringing more IoT devices online too. Bandwidth needs never stop growing, and no one needs to remind you about the importance of remote access for everyone.

Through it all, security is front and center. You must keep hackers out, defeat pranksters, and quickly detect and eradicate real threats that get inside. Even legitimate users and devices can be unwitting sources of the next cyber attack. Can you do it all?

Definitely. Cisco Secure on-premises solutions save the day.

Identity Services Engine (ISE)

Know about everyone and everything that's connected to your network. Authenticate and control what they do and where they can go.

Secure Client (AnyConnect)

Enable frictionless, highly secure network connectivity for those who need VPN access. It verifies devices against your security policy too.

Secure Firewall

Take control with consistent policy, stateful and deep packet inspection, intrusion prevention and internal segmentation through our world-class firewall.

Secure Network Analytics.

Get complete network visibility by baselining activity, spotting anomalies, and use it with ISE to enforce dynamic, adaptive access policy.

User and endpoint security

Hackers target people and their devices to gain a foothold into your network. A trick then a click: that's all it takes, anyone can be fooled.

Device security

Use Cisco Secure Endpoint to protect devices from malware and ransomware. It's a key part of our extended detection and response (XDR) platform for fast detection and confident responses.

Strong authentication

Everyone knows passwords are easily stolen, so you need a second factor to validate identity. Secure Access by Duo makes multifactor authentication simple and easy for everyone.

Mobile device management

Anyone who's managing large quantities of user devices needs Meraki Systems Manager to provision, monitor, and secure them.

Modern VPN client

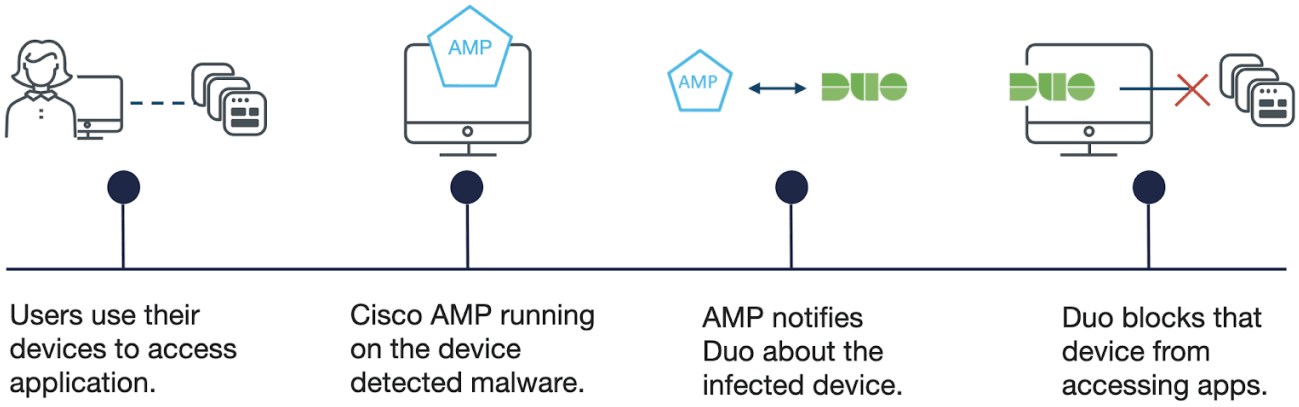
Cisco Secure Client (AnyConnect) works with Duo to verify user identity, validate device posture, and encrypt sensitive communications. It even protects devices when they're off the VPN with Umbrella-powered DNS security.

Integration Spotlight:

Secure Endpoint and Duo

Picture this: An administrator uses a device compromised with malware, yet still tries to access municipal systems with it. If allowed to proceed, the infected device could spread malware and lead to a major cyber incident.

Now let's Cisco Secure it: The administrator's device is protected with Cisco Secure Endpoint, which automatically spots the malware, quarantines it, and notifies the security team about it. It also alerts Duo, which denies all authentication requests from the infected device, effectively stopping the malware before it can spread. Immediate action: That's the power of Cisco Secure integrations. Read more here.



Email and web security

Email and web are top attack vectors, so it's vital to securitize and filter harmful content.

Phishing prevention

Stop harmful email from reaching your staff and other users. Cisco Secure Email defends against phishing, malicious embedded links or attachments, and business email compromise.

Ransomware defense

Most ransomware attacks use DNS, so Cisco Umbrella is a must. Ilt supports a variety of device platforms, and it protects both on and off your network.

Web content filtering

Cisco Secure Web Appliance is our comprehensive content inspection and filtering solution. Features include full proxy mode with optional TLS 1.3 decryption, dwell time control, and Application Visibility & Control (AVC).

Network security

Securing your network has long been your top priority, but now you have too many different products from multiple vendors that don't always play nice together. Wouldn't it be great to build security directly into your network, rather than bolting it on?

Software defined access

Cisco ISE and Cisco DNA Center are the key components that orchestrate network and security operations, streamlining security and IT operations and making them more efficient. It's the heart of our zero trust solution for the workplace.

Firewall & DDoS mitigation

Cisco Secure Firewall is our modern, high-performance firewall with integrated IPS, DDoS mitigation, and encrypted web traffic inspection.

Secure remote access

Cisco Secure Client (AnyConnect) provides secure VPN access to authorized users, but only after verifying both user identity and device trust.

Visibility and analytics

Cisco Secure Network Analytics baselines network activity, spots anomalies, and works with ISE for dynamic policy enforcement.

Solution Spotlight:

Cisco Secure Firewall

The traditional perimeter is a bit hazy these days, but you still need an internet-facing firewall to protect your network. Cisco Secure Firewall delivers advanced, modern firewalling capabilities:

Internet defense

- Stateful access control
- Deep packet inspection
- Web content filtering
- DDoS protection
- Malware C2 control

Intrusion prevention

- High-efficacy threat detection and mitigation
- Network-level file inspection
- Malware protection
- Visibility into high-priority vulnerabilities

Secure access

- IPSec or SSL VPN head end capabilities
- Anyconnect posture validation
- Zero trust access control with ISE integration

Demilitarized zone (DMZ)

- Public-facing web and email service protection
- Safe zone between your network and the internet

Internal segmentation

- Traffic control with Scalable Group Tag (SGT) support
- Consistent segmentation with ISE and SD-Access

Threat Spotlight

Denial of Service attacks

Halting services to citizens. Choking networks. Sometimes attackers just want disruption. With readily available hacking tools, nearly anyone can launch Denial of Service attacks these days.

Distributed Denial of Service (DDoS) attacks are harder to defend since the source isn't clear. Botnets and spoofed addresses make attacks seem like they're coming from everywhere.

Aside from pleading with your service provider, what more can you do?

Get Cisco Secure DDoS Protection.

Our adaptive, behavioral-based algorithms block never-before-seen attacks with the lowest false positive rate in the industry. Achieve the highest system availability even when you're under attack.

You can also choose the DDoS protection that fits you best: cloud, on-premises, or Cisco Secure Firewall appliances with Virtual DefensePro.

Physical security

Workplace safety certainly doesn't end with effective cybersecurity. Agencies around the country are investing in cloud-based cameras that enable safety teams to monitor office grounds, deter crime. identify vandals, and so much more.

Smart cameras

Meraki MV smart cameras bring enterprise video to the security world. They're cloud-managed with solid state storage with multiple cloud storage options. They sip on bandwidth, using less than 50kbps when footage is not being viewed

Our experts are yours too

Cisco Talos® is our talented and experienced team of world-class researchers, analysts and engineers. They're supported by unrivaled telemetry and sophisticated systems to create accurate, rapid and actionable threat intelligence for all Cisco customers, products and services. Talos is one of the largest commercial threat intelligence teams in the world.

With Cisco Secure solutions backed by Talos, our experts are yours too.

But they don't hide behind technology. Cisco Talos Incident Response services can help you prepare, respond and recover from a breach. Before you're attacked, they'll help you strengthen your security posture through planning, assessments, and testing. And in an emergency, they're there for you with 24/7/365 rapid assistance.

Do you have a security emergency right now?
Call us at 1-844-831-7715.

The SecOps team you wish you had

Incident response is critical, but what about detection? Most agencies don't have the resources to proactively monitor security devices or hunt for threats. There's no round-the-clock SOC. And that sets the stage for small cyber problems to become big ones.

You need Cisco Managed Detection and Response (MDR).

Our MDR service combines an elite team of researchers, investigators, and responders with threat intelligence, automation and response capabilities, all backed by Talos. It provides fast detection, analysis, investigation and response – essentially the world-class SecOps team you wish you had but didn't think you could afford.

Problem solved. With Cisco MDR, you can.

Cisco
Customer Experience

Reduce time to detect and respond

Manage and prioritize alerts

Gain greater visibility through analytics

We’re a trustworthy partner

Supply chain attacks are all over the news, so it’s natural to be skeptical of all technology vendors these days.While no organization is completely immune to cyber threats, we’re working tirelessly to earn your trust. At Cisco, we’re transparent and accountable. And we prove it.

Visit our Trust Center or click a box to learn more.

Data Management

Transparency

Trustworthy solutions

Trust principles

Let us secure your federal agency

Cisco Secure Architecture for the Federal Government is a simple yet modern and comprehensive approach to securing your environment.

We can’t wait to talk with you about your needs and how we can help.

Thanks for reading

Modern, efficient cybersecurity for Government

Learn more about our portfolio:
https://www.cisco.com/go/cybergov
Cisco SAFE guides:
https://www.cisco.com/go/safe