Cisco AMP for Endpoints (FedRAMP℠ Ready)

What it is

Key capabilities

Why AMP for Endpoints

Next Steps

Empower relentless breach defense

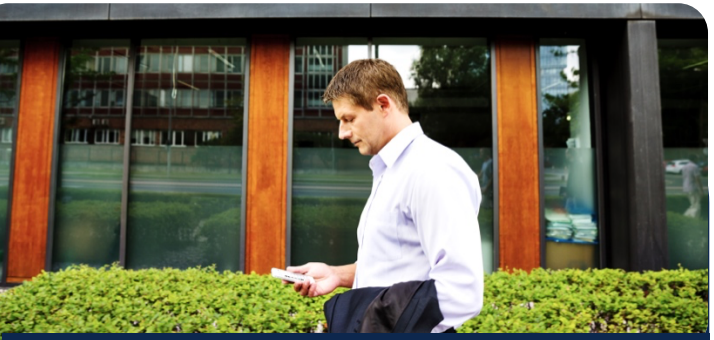
For Public Sector agencies, the consequences of a data breach can be significant. From the compromise of critical data, strain on IT personnel, and a potential violation of public trust, the fallout can be far reaching.

In response, Federal, State and Local agencies must begin deploying Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) technologies. EPPs can deliver next-generation antivirus that stops today's complex attacks. And EDR offers more advanced capabilities like detecting and investigating security incidents, coupled with the ability to quickly remediate endpoints.

That's why we developed Cisco® Advanced Malware Protection (AMP) for Endpoints. This FedRAMP Ready offering combines the power of EPP and EDR to create a unified and more responsive cybersecurity solution for government agencies like yours. AMP leverages multiple protection engines fueled by Cisco Talos threat intelligence to block threats before they target you. It also integrates seamlessly with other security technologies so you can respond to threats holistically.

How it adds value:

- **Protects:** Blocks known malware by automatically leveraging the best global threat intelligence, and enforces Zero Trust by blocking access by risky endpoints.
- **Detects:** Runs complex queries and advanced investigations across all endpoints, and continuously monitors all file activity to detect stealthy malware.
- **Responds:** Rapidly contains attacks by isolating infected endpoints and remediating malware across PCs, Macs, Linux, servers, and mobile devices (Android and iOS).



Enable your agency with advanced capabilities

The Public Sector can now deploy cloud-delivered endpoint protection with advanced detection and response to help stop breaches. As a FedRAMP Ready offering, Cisco AMP for Endpoints lets you rapidly detect, contain and remediate advanced threats that evade your front-line defenses. Plus, it can replace your agency's legacy antivirus completely.

- Supports Zero Trust workforce security
- Faster detection, investigation and response
- Continuous endpoint behavior analysis
- One-click endpoint isolation
- Powerful prevention engines
- Advanced endpoint detection and response
- Full antivirus replacement.

Cisco AMP for Endpoints provides a holistic approach to Public Sector IT security, fueled by Cisco Talos global threat intelligence.

Why government should use AMP

Block threats before they target you

Your agency's endpoint protection is only as good as the intelligence it acts on. That's why Cisco employs machine learning and multiple protection engines fueled by Cisco Talos, the world's largest non-governmental threat intelligence organization.

FedRAMP Ready Cisco AMP for Endpoints finds more vulnerabilities than other vendors and pushes out protection before the bad guys can exploit them. This gives your agency the advantage. And because we're such a trusted leader in networking, Talos sees more network traffic than anyone else. This reach helps drive our holistic approach to security because it means we see more threats, no matter where they begin (Internet, email or another network). Our cloud-based global telemetry sees a threat once, anywhere in the world, and blocks it everywhere, across AMP for Endpoints and our entire security platform.

Know everything about every endpoint

Our FedRAMP Ready solution simplifies threat hunting for Public Sector IT by automating advanced investigative queries across any or all of your endpoints. Whether you're doing an investigation as part of incident response, threat hunting, IT operations, or vulnerability and compliance, AMP gets you the answers you need.

It also has preloaded scripts so you can leverage the expertise of our Talos threat hunters or even customize your own. AMP provides deeper visibility on what happened to any endpoint at any given time by taking a snapshot of its current state. And it continuously monitors and analyzes the behavior of your endpoints, giving you everything you need to investigate and respond quickly to threats.

Plus, if a file that appeared clean upon initial inspection ever becomes a problem, AMP can provide a full history of the threat's activity to catch, isolate, contain and remediate at the first sign of malicious behavior.

Respond completely and holistically

Cyberthreats against our national government are not one dimensional. Your response to them must reflect that. That's why we built our endpoint security with out-of-the-box integration with the rest of the Cisco security platform. This lets your agency block, detect, investigate and respond to threats across your entire environment.

Cisco's holistic approach to security means it works together, not piecemeal, to streamline your security operations. This makes a security investigation faster and easier. You'll get to the root cause fast and be able to automate actions to stop the threat in its tracks.

Cisco AMP for Endpoints lets Federal, State and Local agencies respond to attacks at the first sign of malicious behavior using "one-click" isolation of any endpoint, everywhere. Plus, our solution gives you the ability to broaden control beyond just the endpoint. We instrument our endpoint security to leverage threat intelligence from web, email, cloud and network security solutions. Plus use multi-factor authentication integration for Zero Trust.

Next Steps

- Contact your Cisco sales representative or channel partner to learn more about protecting your agency with Cisco AMP for Endpoints.
- Visit cisco.com/go/fedramp for more info.