AT&T

AT&T Government Trusted Internet

Comply with Trusted Internet Connections (TIC) 3.0 requirements, fully integrated into AT&T Managed Trusted Internet Protocol Service (MTIPS)

Potential Benefits

- Superior security protection for federal agencies, through adherence to TIC 3.0

- Expands coverage to remote and branch locations and integrates into the traditional AT&T TIC 2.2, while creating an inclusive hybrid work environment

- 24/7 fully managed security service including change management, incident management, policy management, and transport capabilities

- Security Operations Analysis Center (SOAC) provides 24x7x365 service covering threat analysis and incident response

- Threat correlation to AT&T Alien Labs Open Threat Exchange® (OTX™) global threat sharing community

- Improved user experience reaching the internet, cloud service providers, applications, and headquarters assets due to branch office and remote users proximity to enforcement nodes

Continuously managing risk in a hyper-connected world

The adoption of mobile and cloud environments enables agencies to keep pace with technology. It also exposes a cybersecurity gap that Trusted Internet Connections (TIC) 3.0 seeks to mitigate. Building upon earlier TIC versions, TIC 3.0 addresses modern environments and technologies. Its guidance aims to secure federal data and networks and provide visibility of cloud and remote users, while also supporting the White House Executive Order on Improving the Nation's Cybersecurity.

The TIC 3.0 guidance is descriptive, not prescriptive, which provides agencies greater flexibility to implement solutions best suited to their unique environments and risk tolerances. Managing TIC and other cybersecurity solutions can be made easier through AT&T, as your single source provider.

Expanded environment needs

The Cybersecurity & Infrastructure Security Agency (CISA) outlined several use cases with TIC 3.0, which AT&T Government Trusted Internet addresses:

Traditional Use Case

This use case is the default use case, which defines how network security can be applied when an agency routes traffic from an agency campus to the web, trusted external partners, or partner government agencies through a traditional TIC access.
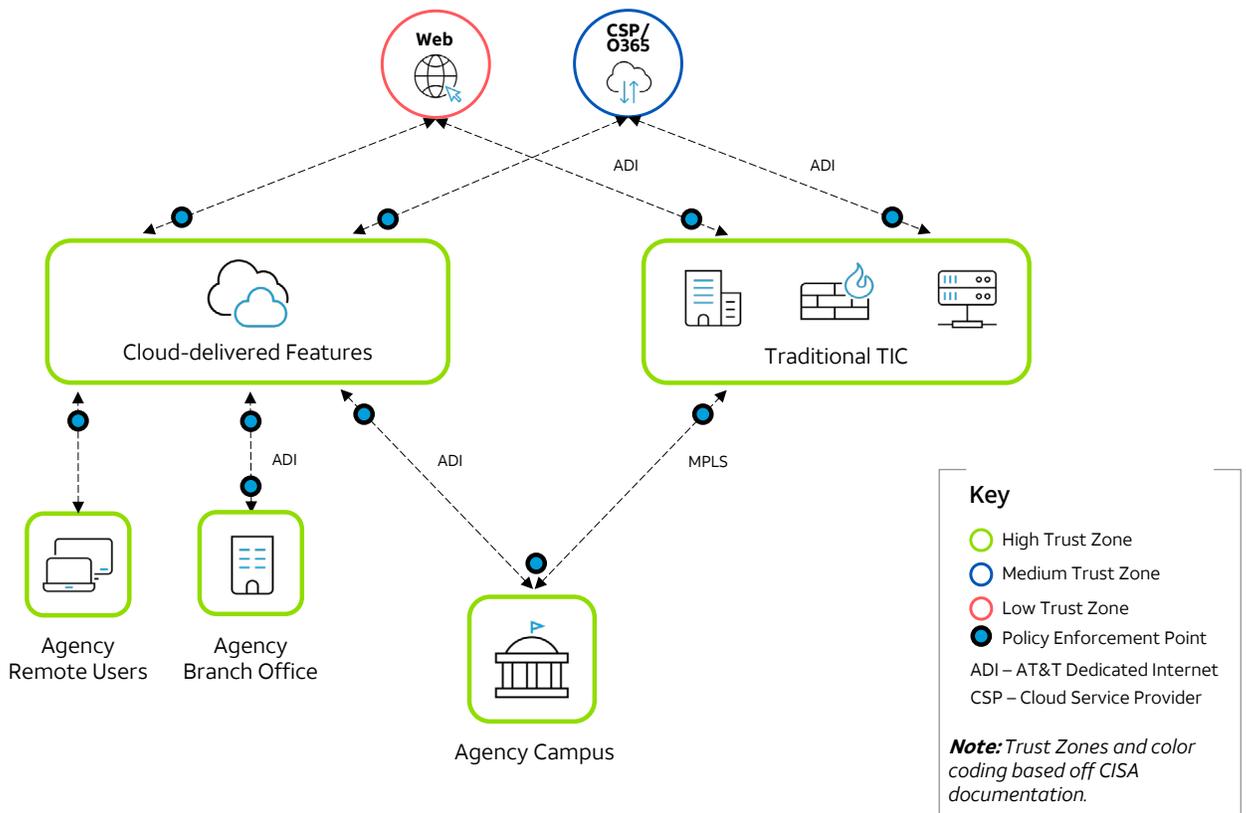
Branch

This use case assumes there is a branch office of an agency that is separate from the agency headquarters (HQ) and uses the HQ for the majority of its services, including generic web traffic. This use case includes SD-WAN enablement.

Remote Users

This use case is an evolution of the original FedRAMP TIC Overlay (FTO) activities. It demonstrates how a remote user connects to the traditional network of an agency, cloud, and internet using government-furnished equipment (GFE).

A fully managed security service with consistent control regardless of customer location

Key

- ○ High Trust Zone
- ○ Medium Trust Zone
- ○ Low Trust Zone
- ● Policy Enforcement Point

ADI – AT&T Dedicated Internet
CSP – Cloud Service Provider

Note: *Trust Zones and color coding based off CISA documentation.*

AT&T Government Trusted Internet

A fully managed, CISA-compliant, and scalable cloud-delivered security service, AT&T Government Trusted Internet adheres to the TIC 3.0 initiative while providing security protection for federal agency connections. In addition to significant security capabilities, our solution includes a multitude of capabilities, including the CISA standard on TIC capabilities and optional Zero Trust Network Access (ZTNA). AT&T Government Trusted Internet uses AT&T Direct Internet (ADI) as its transport mechanism for branch offices. Features apply to traffic that has been forwarded to the service.

Core security features include:

- Next-Gen Firewall (FWaaS)
- Cloud Access Security Broker (CASB) functionalities including Shadow IT
- Data Loss Prevention (DLP)
- AT&T Secure Web Gateway
- Enhanced Protection from unknown threats with cloud protection
- Intrusion Prevention System (IPS)
- Threat detection with advanced analysis
- IPsec VPN and SSL decryption
- Traffic logging for visibility, compliance, and correlation
- Threat correlation to OTX
- URL filtering
- Transparent DNS security
- Traditional use case - security features available under AT&T MTIPS
- The cloud delivered component is a FedRAMP accredited solution

Additional AT&T Cybersecurity offers:

- ✔ Zero Trust Network Access (ZTNA)
- ✔ Inbound access to branch hosted applications
- ✔ Additional log feeds to agency destinations with log receipt implementation service
- ✔ Distributed Denial-of-Service (DDoS) attack security
- ✔ Custom reporting
- ✔ Network interconnect (user-to-branch, branch-to-branch access)
- ✔ AT&T Consulting

To learn more about how AT&T Government Trusted Internet can help fortify your security, contact your AT&T Public Sector professional.

[About AT&T Cybersecurity] AT&T Cybersecurity helps reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our Software-as-a-Service (SaaS)-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and Security Operations Center (SOC) analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.