LevelBlue

SOLUTION BRIEF

LevelBlue Managed Government Trusted Internet Protocol Service

Comply With Trusted Internet Connections (TIC) 3.0 Requirements, Fully Integrated Into LevelBlue Managed Government Trusted Internet Protocol Service

Continuously Managing Risk in a Hyper-Connected World

The adoption of mobile and cloud environments helps agencies keep pace with evolving technology. However, it also reveals cybersecurity gaps that Trusted Internet Connections (TIC) 3.0 aims to address. Building on earlier 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 LevelBlue, as your single source provider.

Expanded Environment Needs

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

Potential Benefits

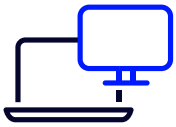
- Superior security protection for federal agencies, through adherence to TIC 3.0
- Expands coverage to remote and branch locations and integrates into the traditional LevelBlue TIC 2.2, while creating an inclusive hybrid work environment
- 24/7 fully managed security service including change management, incident management, policy management, and transport capabilities
- Security Operations Analysis Center (SOAC) provides 24/7 service covering threat analysis and incident response
- Threat correlation to LevelBlue 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

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

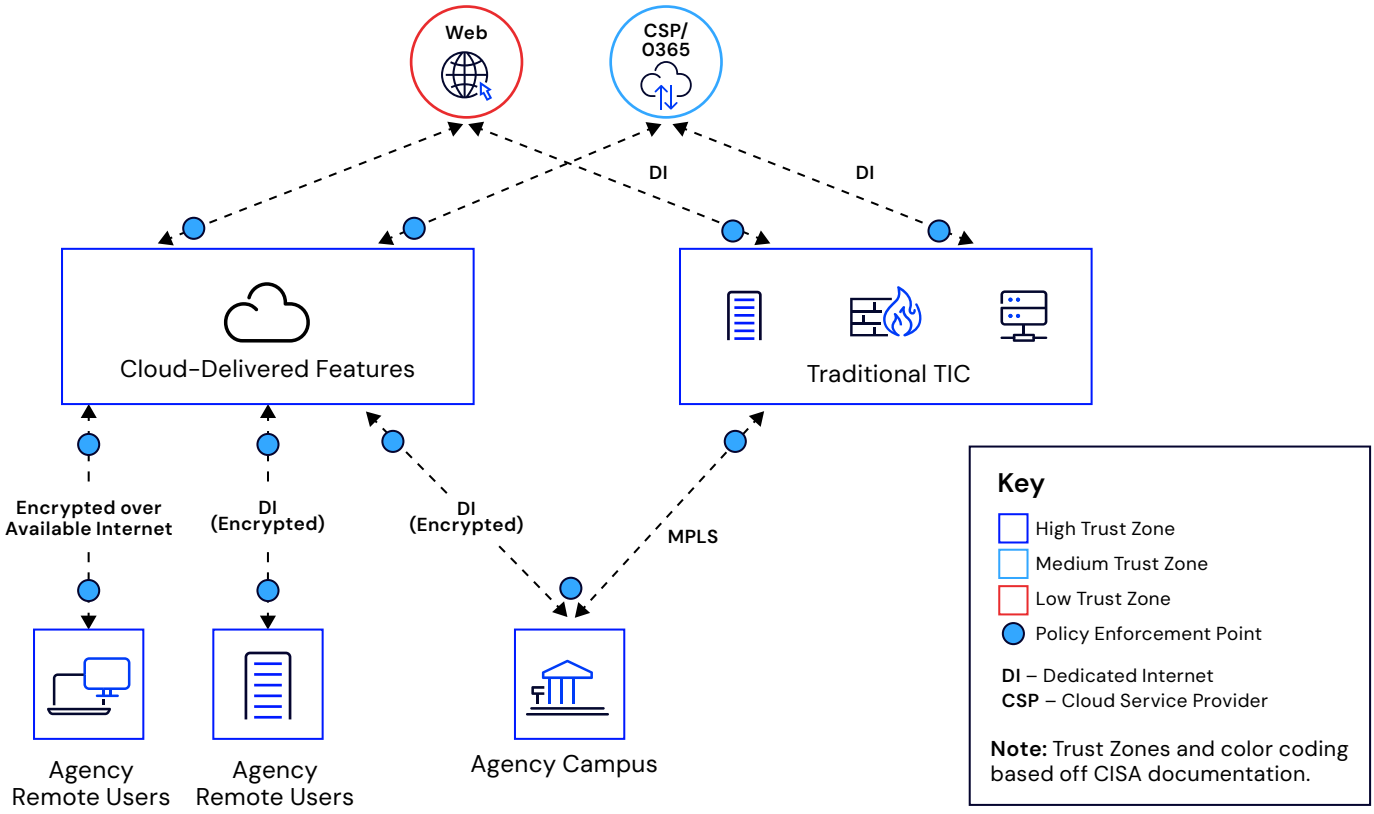
This use case assumes there is a branch office of an agency that is separate from the agency headquarters (HQ) and uses the HQ for the majority of its services, including generic web traffic. This use case includes SD-WAN enablement.



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



Managed Government Trusted Internet

A fully managed, CISA-compliant, and scalable cloud-delivered security service, 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). Government Trusted Internet uses dedicated internet (DI) as its transport mechanism for branch offices. Features apply to traffic that has been forwarded to the service.

Core security features include:

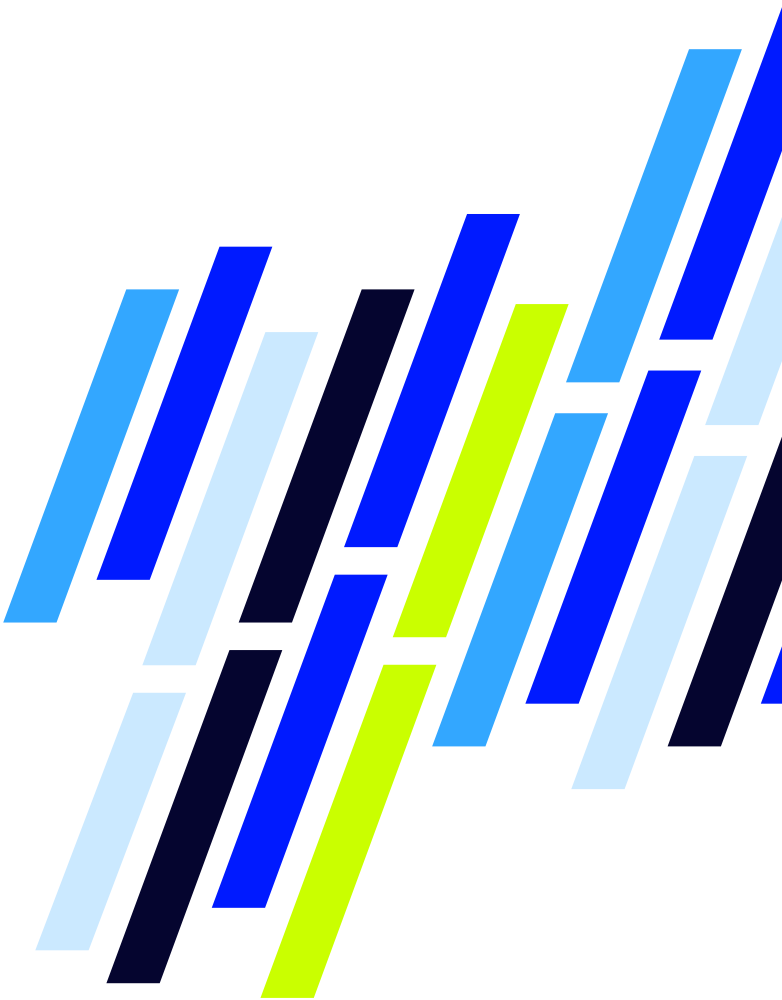
- Next-Gen Firewall (FWaaS)
- Cloud Access Security Broker (CASB) functionalities including Shadow IT
- Data Loss Prevention (DLP)
- Secure Web Gateway
- Enhanced Protection from unknown threats with cloud protection
- Intrusion Prevention System (IPS)

- 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
- The cloud delivered component is a FedRAMP accredited solution

Additional LevelBlue 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)
- ✓ LevelBlue Consulting

To learn more about how LevelBlue Government Trusted Internet can help fortify your security, contact your LevelBlue Public Sector Professional.



LevelBlue

About LevelBlue

LevelBlue is a joint venture between AT&T and WillJam Ventures to form a new, standalone managed cybersecurity services business.

At LevelBlue, we simplify cybersecurity through award-winning managed services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence, which enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us to learn more, or speak with your LevelBlue sales representative.