SOLUTION BRIEF

TIC 3.0 – Securing the Government Cloud Edge

Through modernization of the Trusted Internet Connection, agencies can employ new Policy Enforcement Points (PEP) to increase cloud adoption and embrace cloud use cases.

Key Use Cases

- Detect, monitor, and restrict unsanctioned cloud services within the agency and remote endpoints
- Perform Tenant Restrictions for Enterprise SaaS Services, such as, Office 365
- Provide collaboration control to prevent agency data from inadvertent disclosure
- Secure agency sanctioned cloud services by detecting compromised accounts, insider threats, and malware
- Provide zero trust and contextual access controls for agency enterprise applications in the cloud
- Audit and remediate cloud workload misconfigurations to prevent unauthorized access

Connect With Us

Business Problem

The Trusted Internet Connection (TIC) initiative has sought to improve the cybersecurity posture of the Federal Government by reducing the total number of internet Points of Presence (POP), and introducing network security technologies at the perimeter that detect threats and protect agency networks. The traditional network perimeter continues to erode thanks to new collaboration technologies and the advent of cloud service providers. As a result, agency data no longer resides in fixed silos behind the network firewall. Alternative approaches to protecting agency data stored at the endpoint or in sanctioned cloud service providers is needed.

With the recent increase of teleworking, the utilization of agency sponsored cloud solutions require cloud-native compensating security controls to provide new mechanisms for monitoring cloud services, protecting agency data, and the ability to remediate incidents as they occur. The demand for remote work has stretched legacy VPN infrastructure capacity to its limits. New technologies for protecting end users and endpoints should be employed to complement an agency's traditional Trusted Internet Connection (TIC). Due to significant increased demand of teleworkers DHS Cybersecurity and Infrastructure Security Agency (CISA) released the TIC 3.0 Telework Use Case. This guidance enables agencies to incorporate new technologies to improve agility, scale, and reduce reliance on on-premise resources. McAfee has developed the Government Cloud Edge to address these gaps.

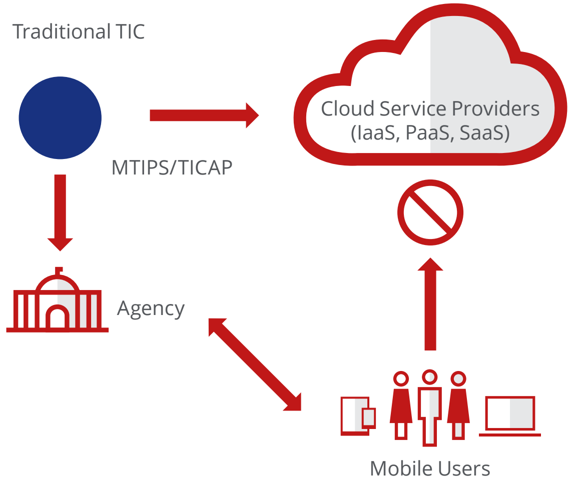

Figure 1. Traditional Trusted Internet Connection (TIC)

McAfee Government Cloud Edge (GCE)

In order to fulfill the requirements outlined in the TIC 3.0 security capabilities handbook new Policy Enforcement Points (PEP) are needed that address the goals of maintaining consistent protection of agency users, devices, and data. McAfee's Government Cloud Edge is comprised of three foundational technologies that ensure TIC 3.0 use cases are solved:

- MVISON Cloud (CASB)
- Web Protection
- Data Loss Prevention (DLP)

Attempting to manage or maintain these disparate solutions from multiple vendors creates significant overhead and is prone to misconfiguration errors. Investigating any security event across disparate solutions requires manually stitching together reports from individual products and repositories to identify the source of the incident.

Utilizing McAfee's Government Cloud Edge, you can achieve:

- Consistent Visibility and control over data from device to cloud
- Integrated access control and threat protection for the cloud and web
- Cloud-native and hybrid architectures with enterprise scale and resilience

The TIC 3.0 Teleworking Use Case is accelerating a shift beyond the network to a new cloud edge. McAfee's Government Cloud Edge enables remote users to operate with maximum productivity while ensuring appropriate security policies and governance are in place as they would be for the traditional TIC.

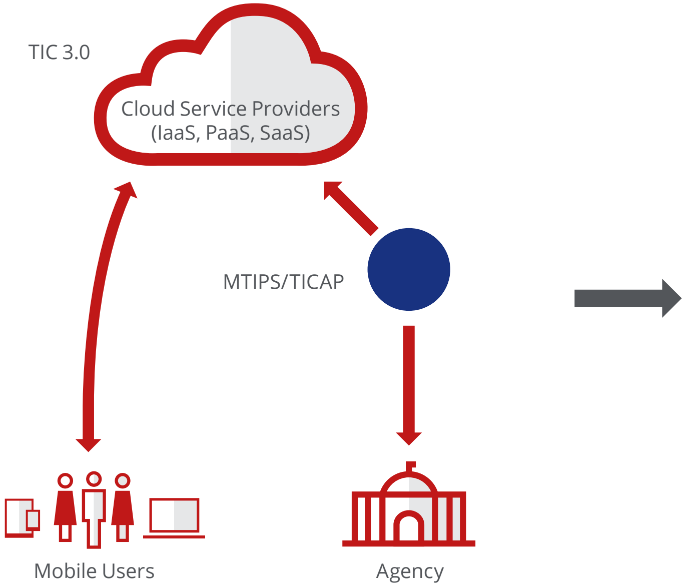

Figure 2. Modernized Trusted Internet Connection (TIC) 3.0

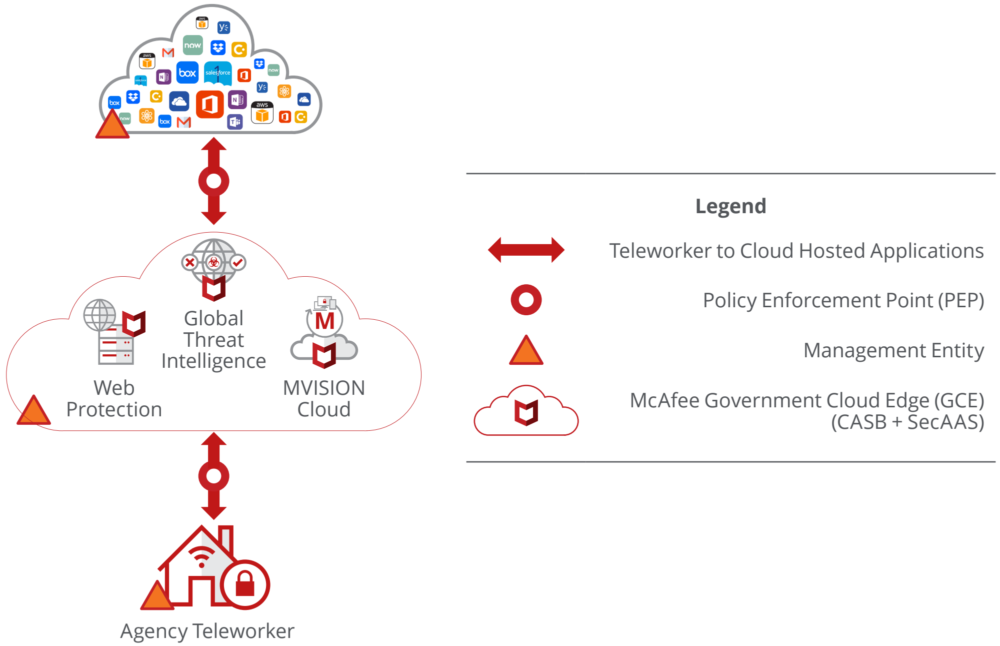

Figure 3. TIC 3.0 – Teleworker Use Case

Consistent Visibility and Governance over Agency Data from Device to Cloud

As cloud adoption continues to shift agency resources and data from the network perimeter to cloud provider environments, the primary control points for data protection shift. Devices can access cloud data from anywhere, and data can be created in the cloud and shared cloud-to-cloud without ever residing on a device or passing through a traditional TIC stack. This makes the device and cloud focal points for data protection, with web traffic in the network remaining as a useful mechanism to control unsanctioned cloud services, prevent malware, and manage general internet access while honoring the original intent of the TIC. Many agencies have established DLP programs for their on-premise environments, where significant time has been invested defining classifications for what data is sensitive to their agency, working with multiple stakeholders, such as, counsel, privacy officers, and data owners to gather data protection requirements.

Implementing Data Protection in the cloud used to require rebuilding these DLP classifications in the cloud. This resulted in excessive time spent replicating pre-existing work already completed for data on devices and in the network, with potentially inconsistent policy enforcement from different DLP engines. Data loss through collaboration or shared links in the cloud was invisible to on-premises DLP. McAfee Government Cloud Edge streamlines the implementation of DLP in the cloud by sharing data classifications and DLP engines between all policy enforcement points (PEP): the device, network, and cloud. Utilizing McAfee ePolicy Orchestrator (ePO) software as the starting point for creating and managing classifications, you can then synchronize your classifications between on-premises DLP and CASB, applying them to policy for any cloud service and cloud-to-cloud traffic that would otherwise bypass your network. All devices, whether in or out of your managed network, can all be protected by the same DLP rules.

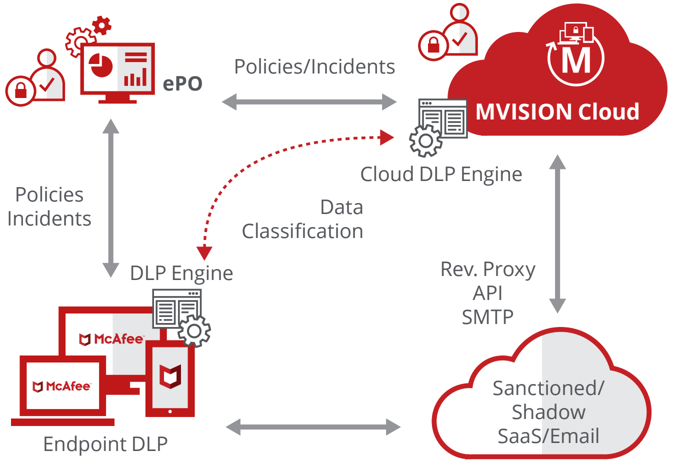

Figure 4. Comprehensive Data Protection Across Agency Devices, Network, and Cloud

Performing data protection management in a centralized location saves time - enabling faster investigations and better reporting while eliminating the need to combine multiple data sources. Investigations and reports are more accurate, with fewer opportunities for mistakes made from manually combining data. Instead, data is combined automatically by McAfee ePO software. Incident data is all-encompassing and consistent, using the same DLP engines and classifications across each enforcement point and combining their event data.

Unified Access Control and Threat Protection for the Cloud and Web

Cloud services come with various levels of risk and can be accessed by both managed and unmanaged devices (BYOD). Enterprise cloud services, such as, Microsoft Office 365 have published application programming interfaces (APIs), which allow Cloud Application Security Brokers (CASBs) to connect directly for visibility and control over data that enters the service, data created in the cloud, data shared cloud-to-cloud, or anywhere externally. Cloud-native threats that occur within these services can be detected by user and entity behavioral analytics (UEBA) that correlate activity across all cloud services agencies have authorized. Recently allowed by the TIC 3.0 guidance, personal devices can access agency instances of Office 365, but be restricted from downloading sensitive agency data by the CASB preventing data exfiltration.

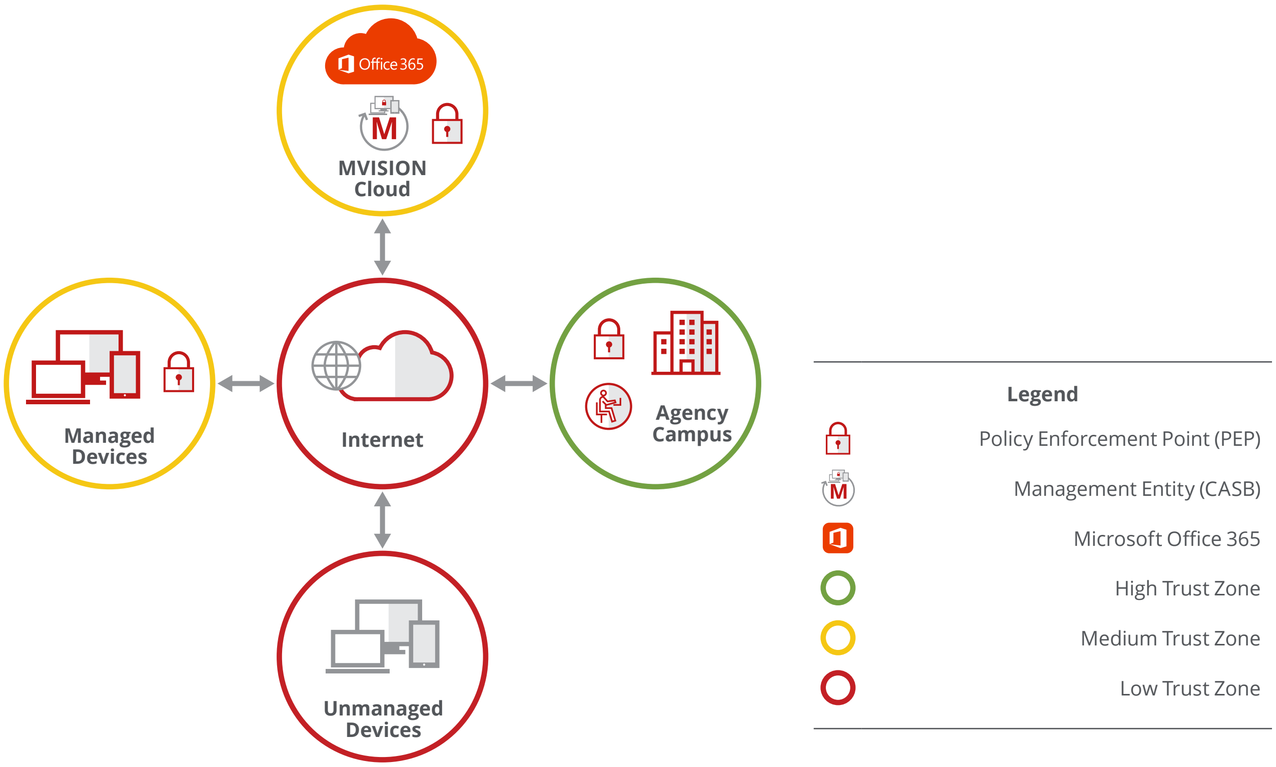

Figure 5. Monitoring and Protection of Enterprise Software as a Service (SaaS) Applications

In addition to enterprise SaaS applications, agencies must ensure that applications which have been migrated or built in Infrastructure as a Service (IaaS) public cloud providers, such as, Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP) are properly monitored and have compensating security controls to allow for direct connections.

McAfee's Government Cloud Edge (GCE) CASB solutions acts as a Policy Enforcement Point (PEP) Management Entity to provide the additional controls listed:

- Security Configuration Monitoring: Identify IaaS and PaaS resources with non-compliant security settings to remediate misconfigurations that coud lead to cloud workload or data compromise
- Confidential Data Visibility: Gain visibility of regulated / high-value data stored in cloud data storage services, such as, AWS S3 Buckets or Azure Blob Storage
- Advanced Threat Protection: Detect compromised users accounts, insider or privileged user threats, and malware
- Activity Monitoring and Forensics: Capture and categorize an audit trail of all activities that occur within the CSP for forensic investigations

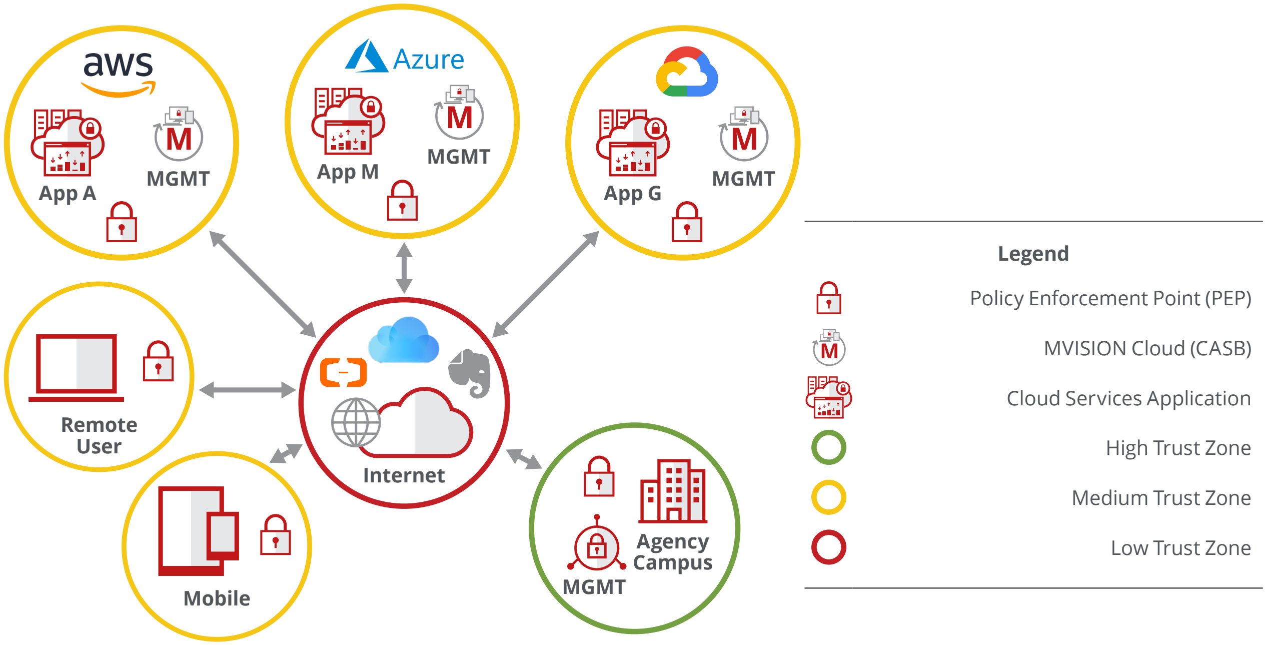

Figure 6. Monitoring and Protection of Agency Infrastructure as a Service (IaaS) public cloud service providers and enterprise applications

Most agencies believe they use less than 50 cloud services — McAfee has determined that agencies oftentimes use closer to 2,000. That is a wide range of services to protect. However, 90% of data lives in the enterprise services that agencies sanction, with 42% living in collaboration services like Office 365 alone. The remaining 10% of data lives in unsanctioned services, which are often referred to as "Shadow IT." Despite holding a fraction of sensitive data, they typically pose the highest risk, meaning they don't meet security requirements like encrypting data at rest or achieving compliance certifications, such as, FedRAMP.

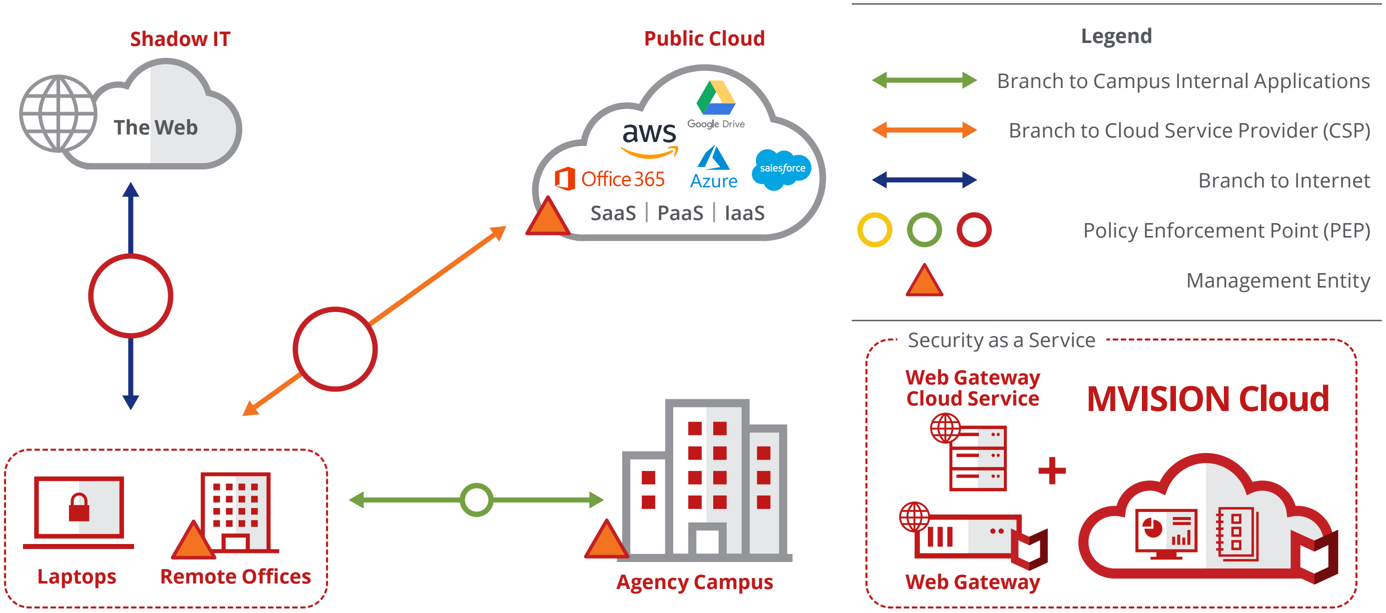

Figure 7. Secure Web Gateway enhanced with Shadow IT Detection for secure access to agency sanctioned cloud service providers

McAfee Government Cloud Edge (GCE) allows you to control access to all cloud services and protect against threats that occur within them. Leveraging both Web Protection, CASB, and DLP technologies enables agencies to provide comprehensive policy enforcement points to fulfill TIC 3.0 capabilities.

Additional controls from the convergence of CASB and Web Protection within McAfee Government Cloud Edge include:

- Zero-day malware prevention: Zero-day malware from any cloud service or website is detected and removed by our high-efficacy machine-learning based engine.
- Cloud application controls: Control features of individual cloud services, like the ability to post or upload documents.
- Tenant restrictions: Differentiate between personal and corporate accounts of cloud services like Office 365, blocking personal accounts and guiding to the agency account under your visibility and control.

McAfee GCE utilizes a CASB to perform its sanctioned cloud service visibility and control via API and reverse proxy. For unsanctioned cloud services and the web, it uses a Secure Web Gateway (SWG) to enforce its policy via forward proxy.

Cloud Smart and Direct-to-Cloud Architecture with Enterprise Scale and Resilience

The network-centric security model of the traditional TIC no longer provides adequate visibility and control over devices that can be anywhere, and cloud services that aren't operated by the agency. Access from devices to the cloud operate over web protocols, providing a layer of control for web proxies to enforce un-sanctioned services policy, scan for sensitive data in motion, and block malware. Traditional TICs use hardware appliance proxies in their data center that capture traffic from remote sites over wide-area network techniques, including multiprotocol label switching (MPLS). Both the hardware and MPLS network carry cost and capacity limits. McAfee's GCE offers a flexible architecture that support for on-premise virtual appliances, Infrastructure as a Service (IaaS) public cloud service providers, or a cloud-native web gateway cloud service managed by McAfee. Utilizing this approach greatly reduces the cost of hardware and MPLS routing can be reduced with capacity constraints replaced with the scale of the cloud. Taking this approach for TIC 3.0 allows any device or physical site to connect directly to the cloud and open internet with increased levels of control over data and threats through McAfee GCE.

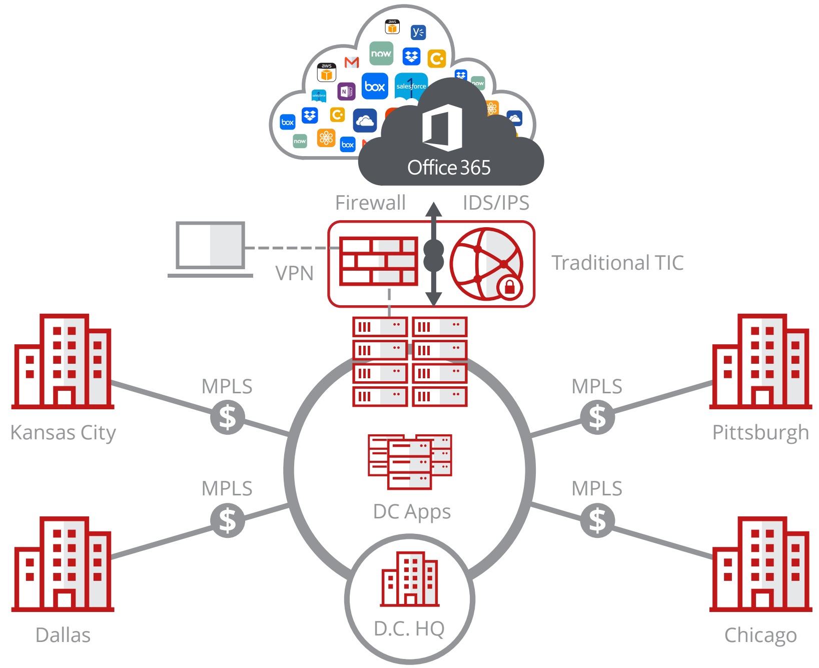

Figure 8. Before – TIC 2.x – Traditional Architecture Hub and Spoke

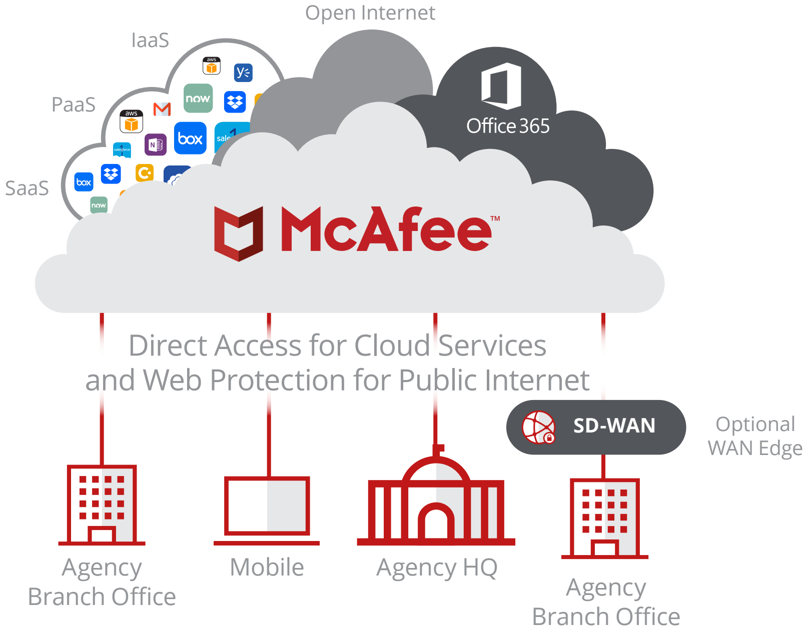

Figure 9. After – TIC 3.0 – Direct to Cloud

TIC 3.0 – Telework Use Case - McAfee Alignment

	TIC 3.0 – Telework Use Case															
	Files	Email				Networking		Intrusion Detection		Enterprise	Unified Communications and Collaboration	Data Protection				
McAfee Solutions	Anti-malware	Anti-phishing Protections	Data Loss Prevention	Malicious URL Protections	URL Click-Through Protection	Network Segmentation	Micro-segmentation	Adaptive Access Control	Encpoint Detection and Response	Remote Desktop Access	UCC Data Loss Prevention	Access Control	Protections for Data at Rest	Prtections for Data in Transit	Data Loss Prevention	Data Access and Use Telemetry
MVISION Cloud (CASB)	■		■			■	■	■			■	■	■	■	■	■
Web Protection	■			■	■	■				■		■	■	■	■	■
Data Protection (DLP/Encryption)			■			■						■	■	■	■	■
Endpoint Security	■			■	■											
MVISION Mobile	■			■	■											
Endpoint Detection and Response (EDR)	■	■							■							
Network Security Platform (NSP/nNVP)	■					■	■									
Malware Sandboxing (ATD & TIE)	■															

About McAfee MVISION Cloud (Cloud Access Security Broker)

McAfee MVISION Cloud provides agencies the comprehensive visibility and consistent control they need to embrace the cloud to augment and support their mission. MVISION Cloud is a cloud-native security platform specifically designed for the cloud, integrates seamlessly with cloud service providers, enables employees and developers to leverage cloud services and at the same time protects confidential data and addresses threats in SaaS, PaaS, and IaaS cloud services.

About McAfee Web Protection

McAfee Web Protection uses secure gateway technology to protect every device, user, and location from sophisticated threats. McAfee Web Protection is a unified solution combining on-premises McAfee Web Gateway and cloud-delivered McAfee Web Gateway Cloud Service. When deployed together, both on premises and cloud solutions can be managed with a single console and with a single shared policy that is applied to devices wherever they travel.

About McAfee Data Loss Prevention (DLP)

McAfee Data Loss Prevention software delivers the highest levels of protection for sensitive data, while greatly reducing the cost and complexity of safeguarding business-critical information. McAfee data protection is delivered through the McAfee ePO platform, for streamlined deployment, management, updates, and reports.

Learn More

Visit us at
www.mcafee.com/publicsector

McAfee

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com