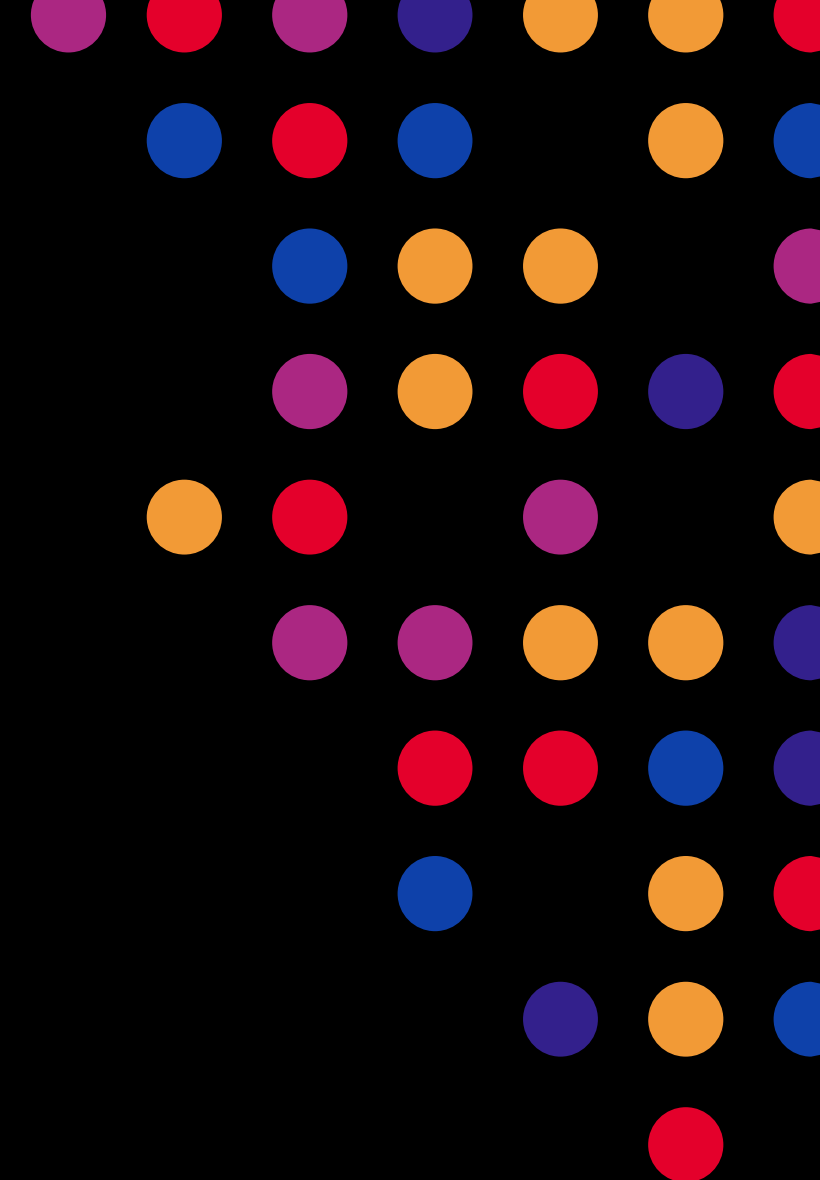




F5 Solutions for Zero Trust

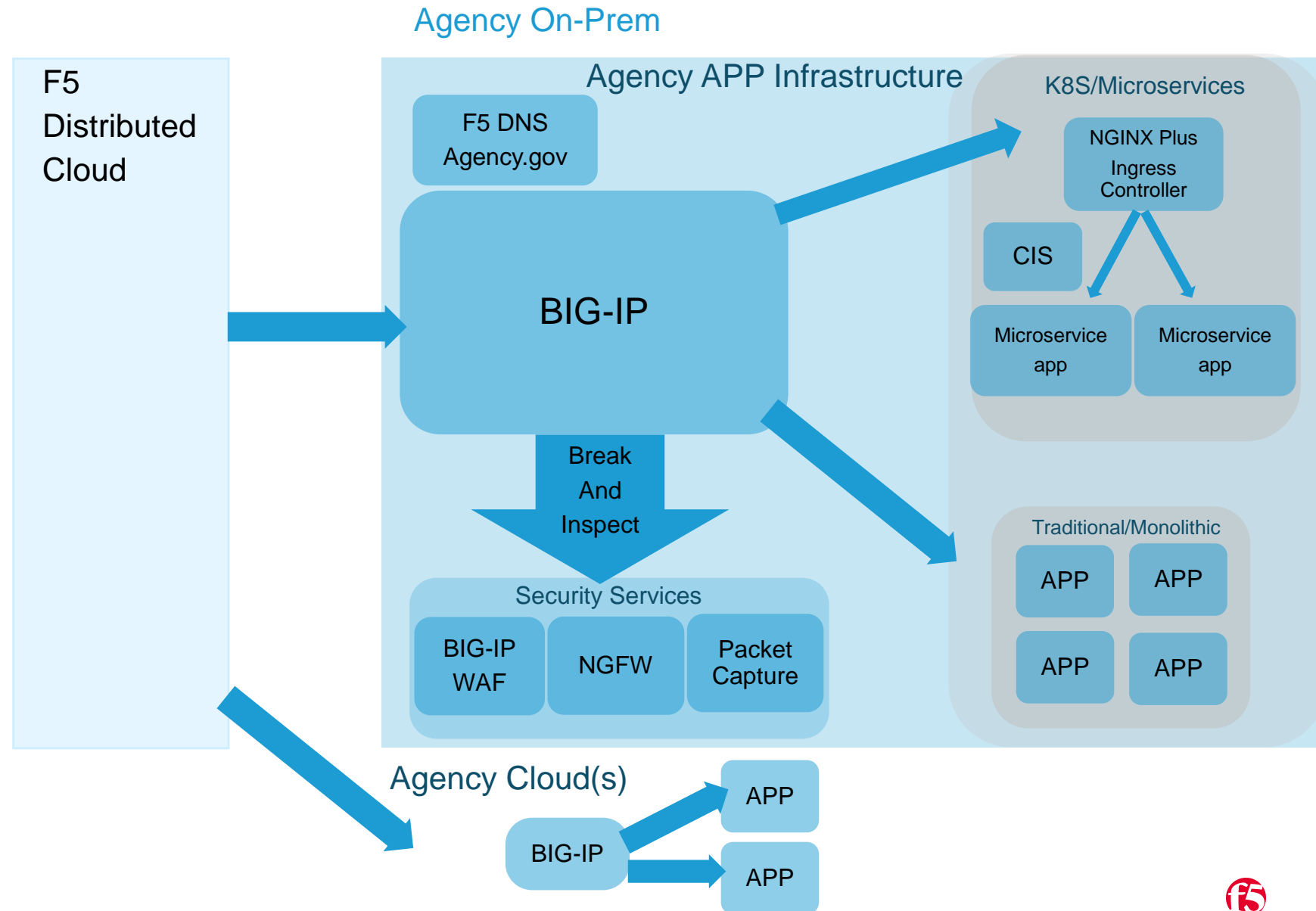
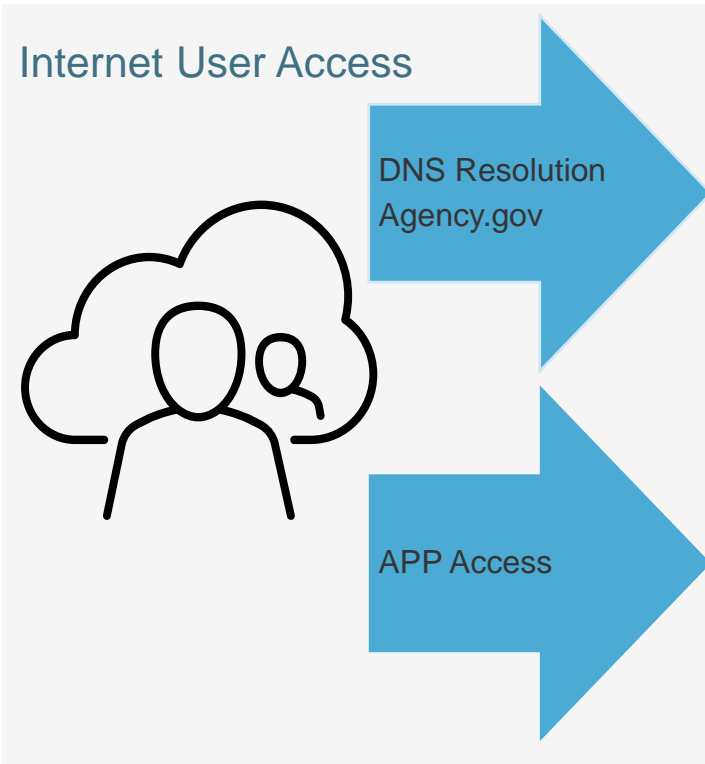
Ryan Johnson, Solutions Engineering Manager, F5
rj@f5.com

Dung Lam, Sr. Solutions Engineer, F5
dung.lam@f5.com



F5 Overview—We protect and deliver applications

As related to Zero Trust



What F5 does for Zero Trust

Public User



Public APP Access



Agency User

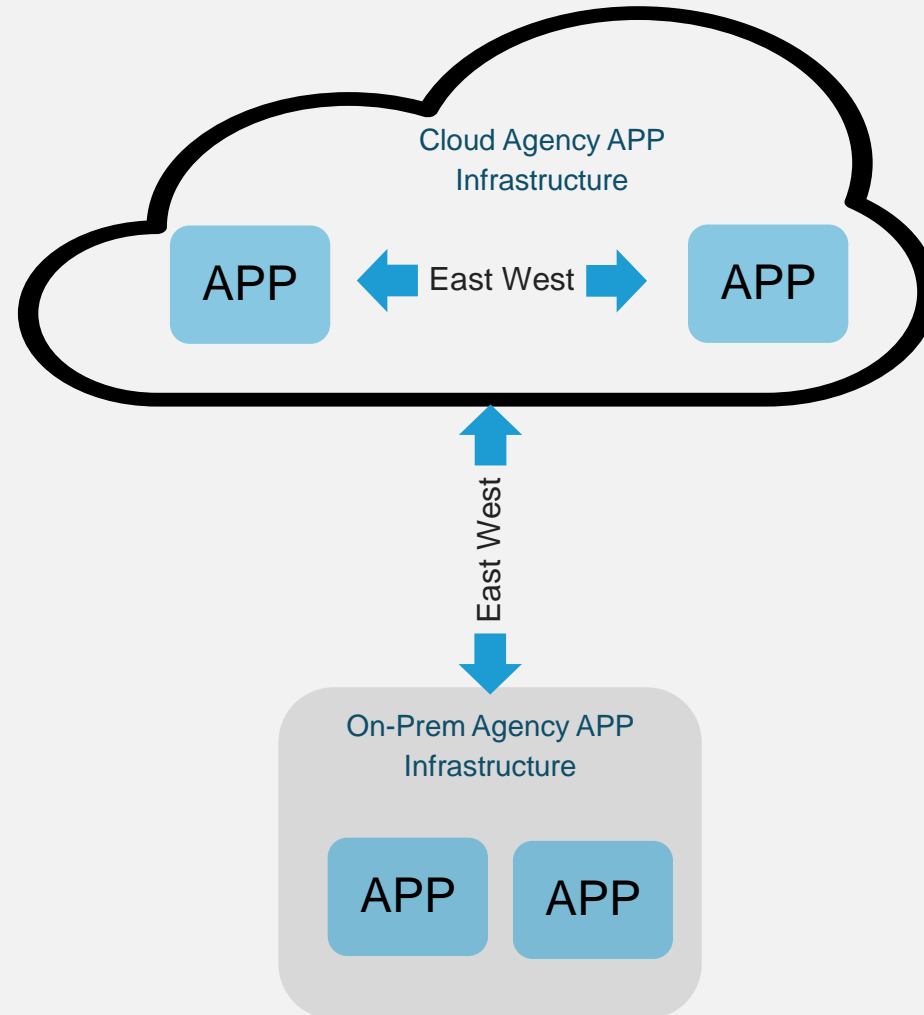


Agency User App Access

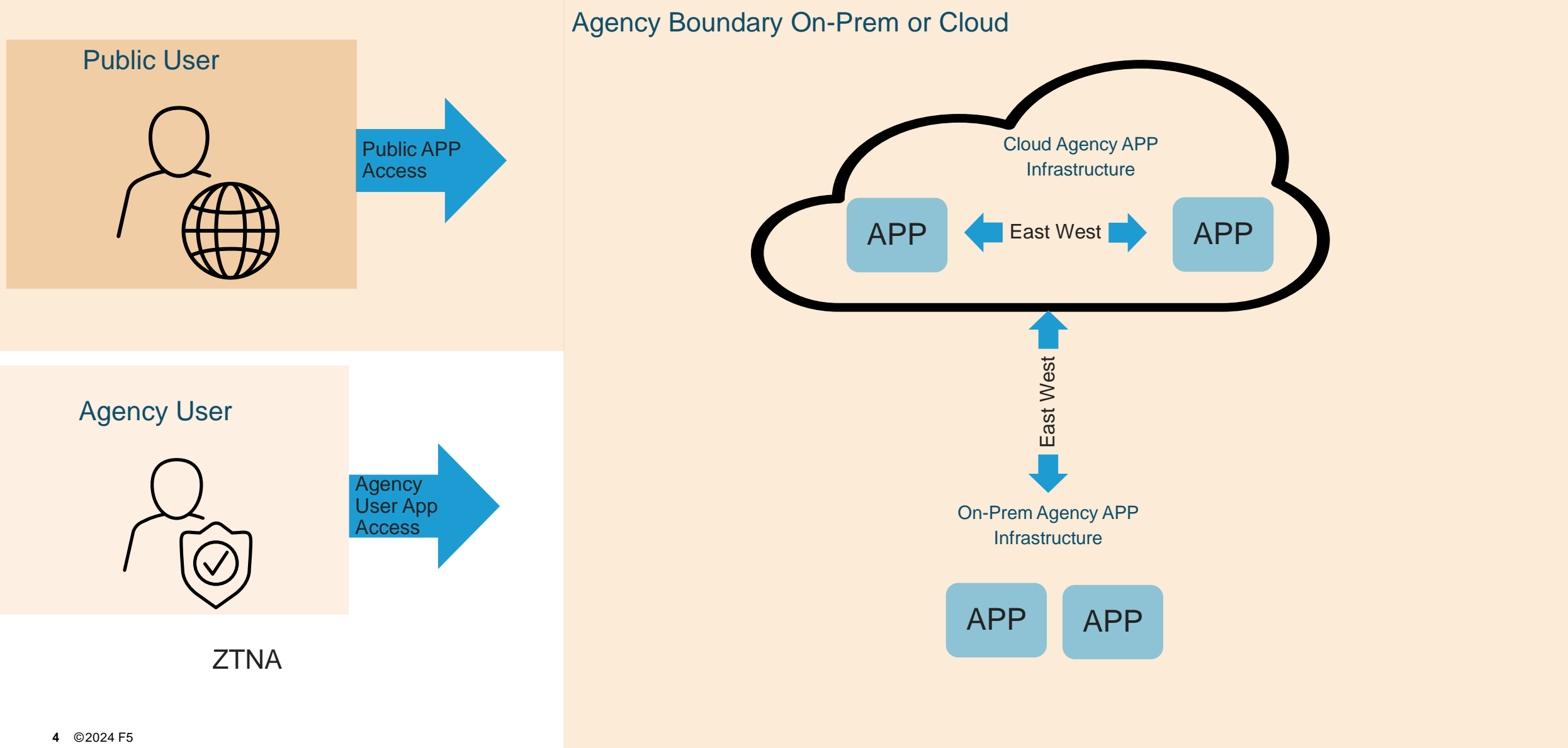


ZTNA

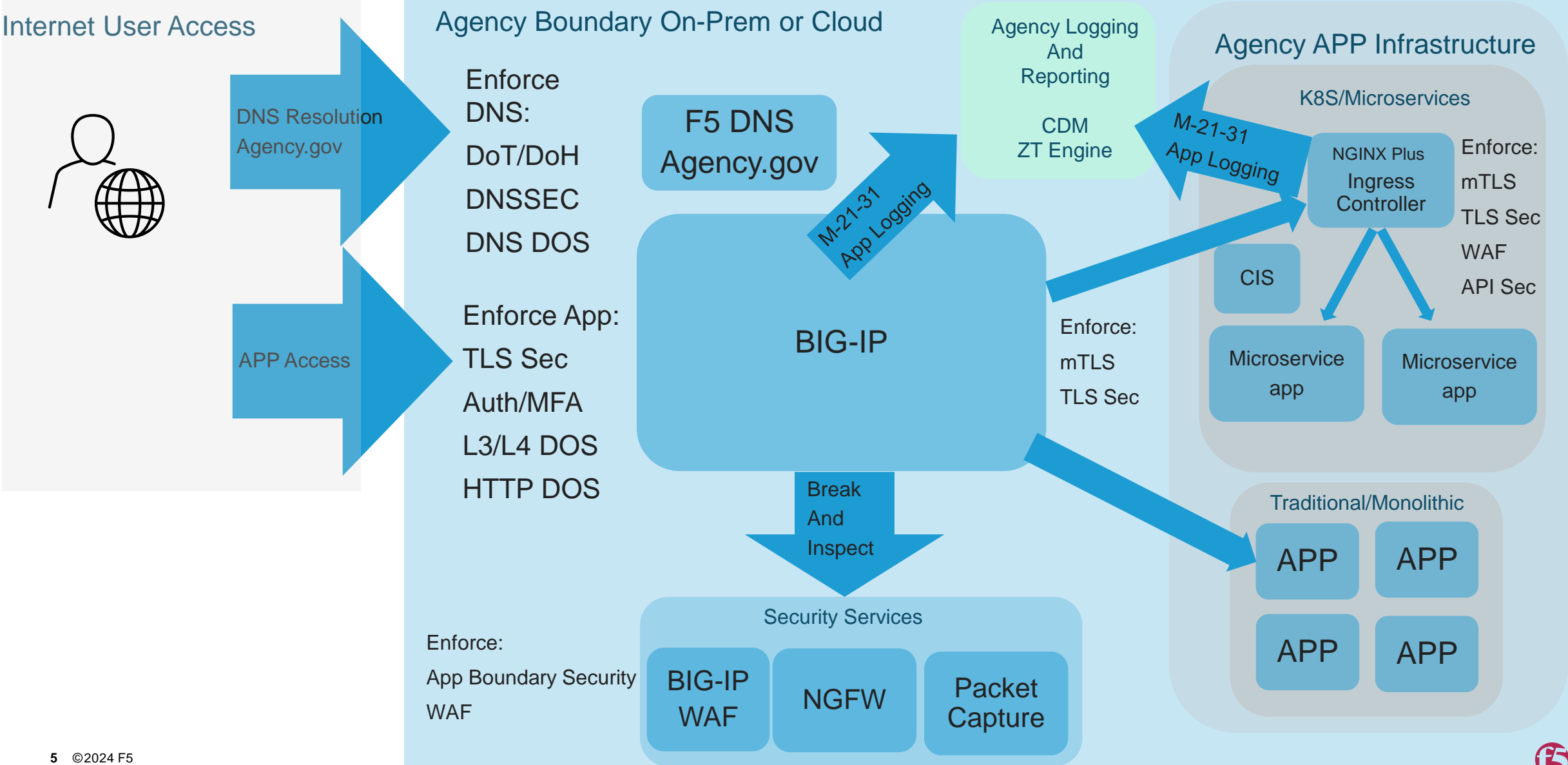
Agency Boundary On-Prem or Cloud



What F5 does for Zero Trust—Highlighted

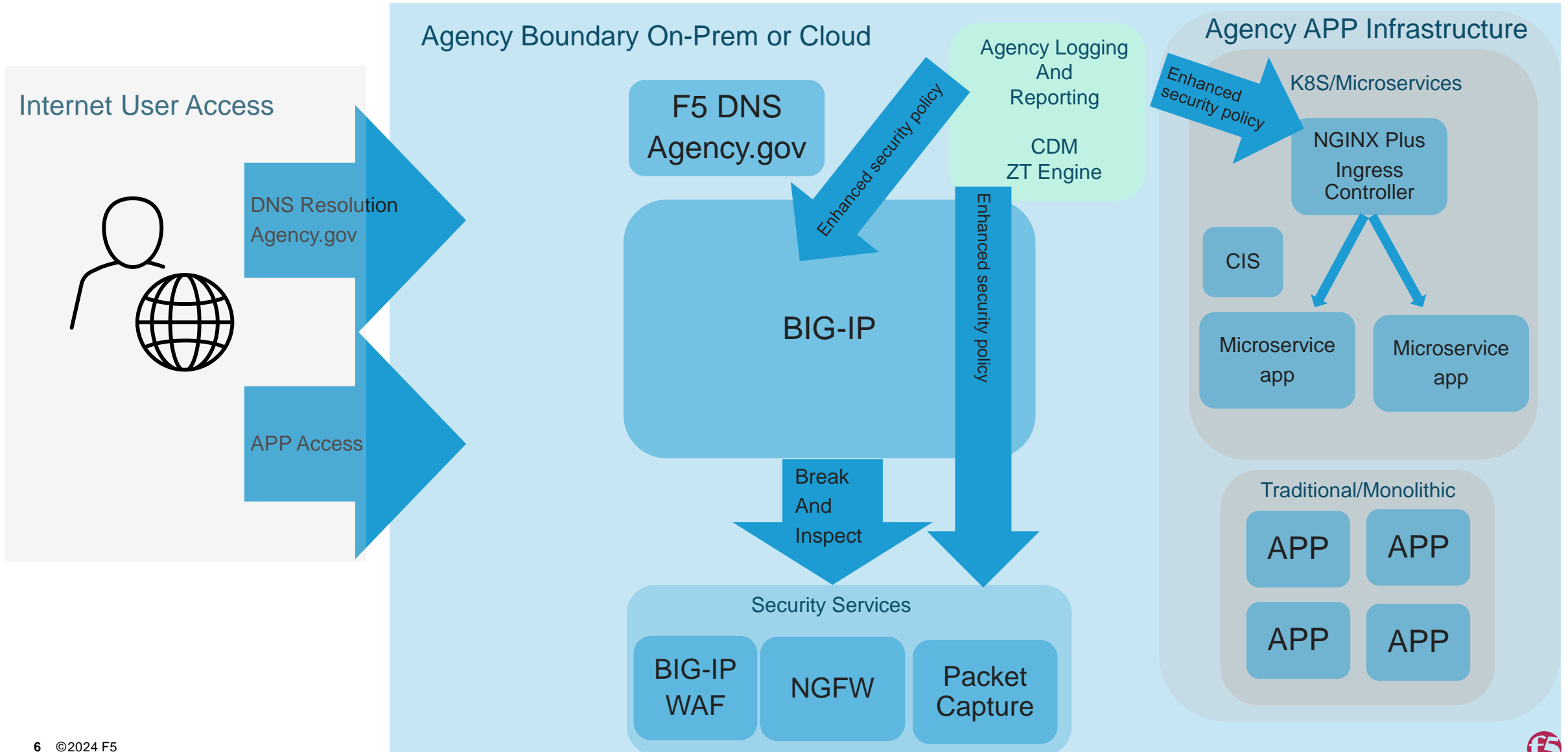


How F5 Provides Zero Trust



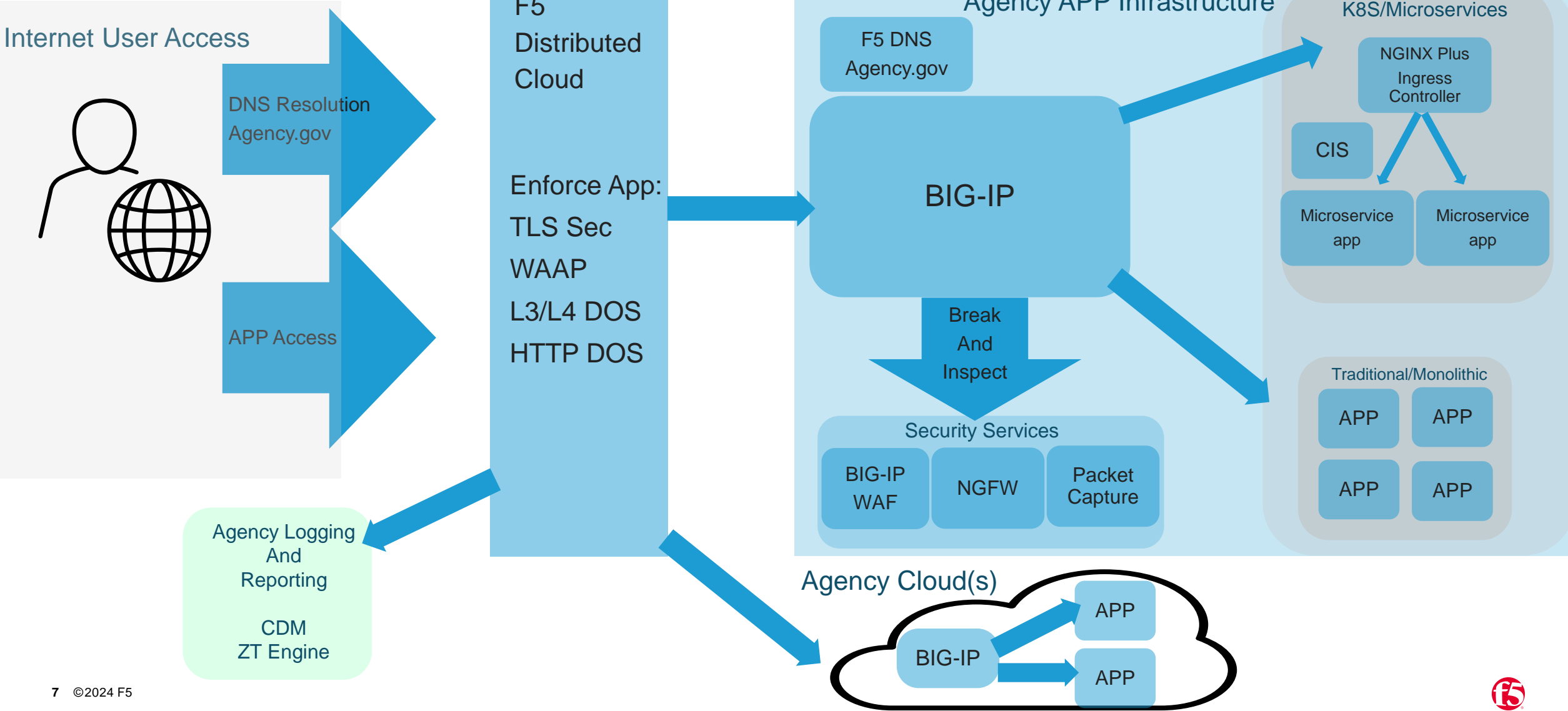
Inbound—ZT Loop—DevSecOps Policy

Gather intelligence across all applications—enhance application security policy at critical points



F5 Overview—We protect and deliver applications

As related to Zero Trust

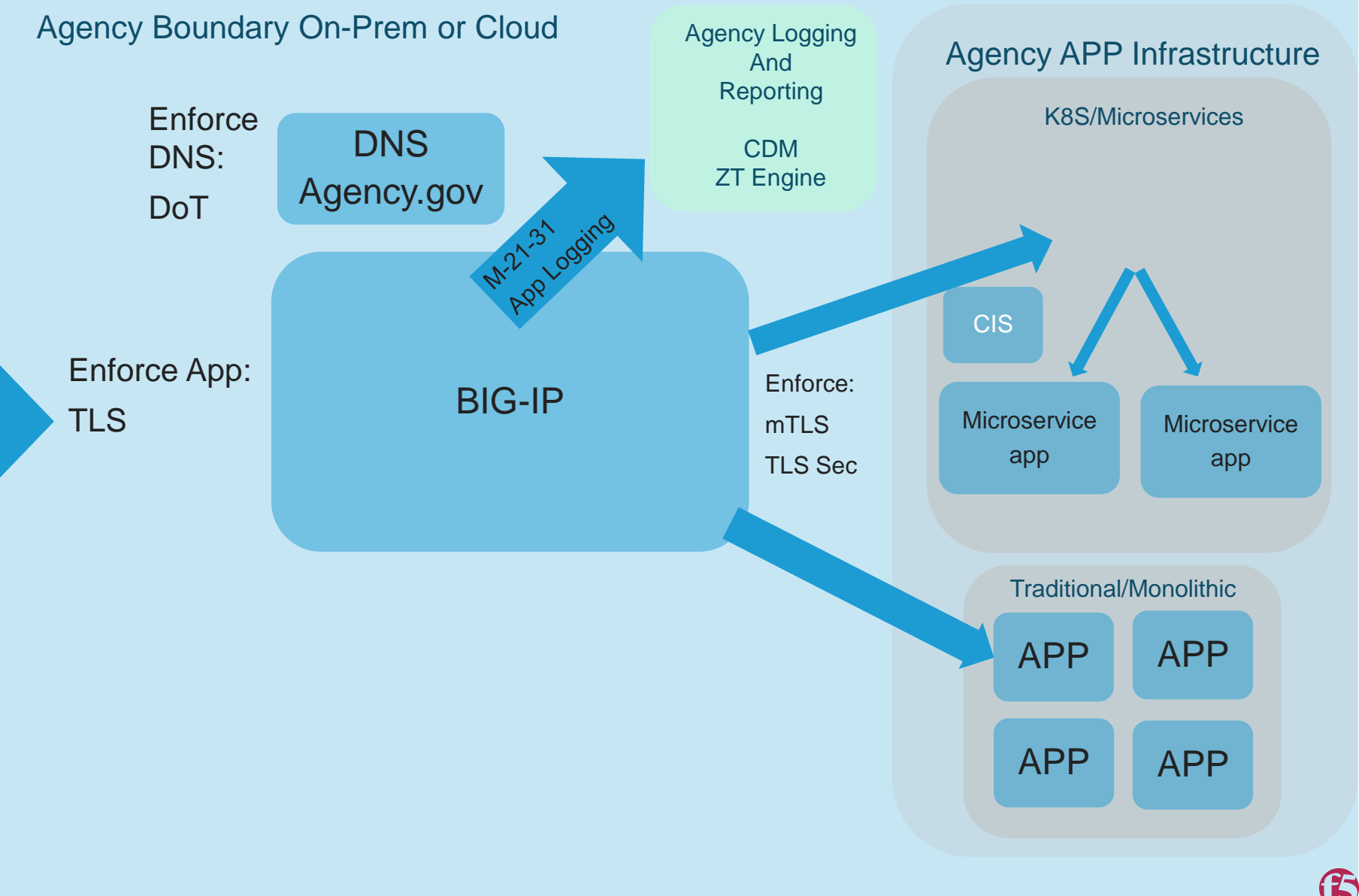


If you have F5, you have these capabilities

Internet User Access



APP Access



ZT requirements that F5 helps agencies deliver

M-22-09

	Traditional App	Modern App
Enforce User MFA across applications	✓	✓
Enforce recent encryption standards	✓	✓
Encrypt all traffic across all boundaries	✓	✓
Enforce device level signal alongside identity	✓	✓
Automated deployments	✓	✓
Every request will be validated	✓	✓
Enforce DNS DoT/DoH	✓	✓

M-21-31

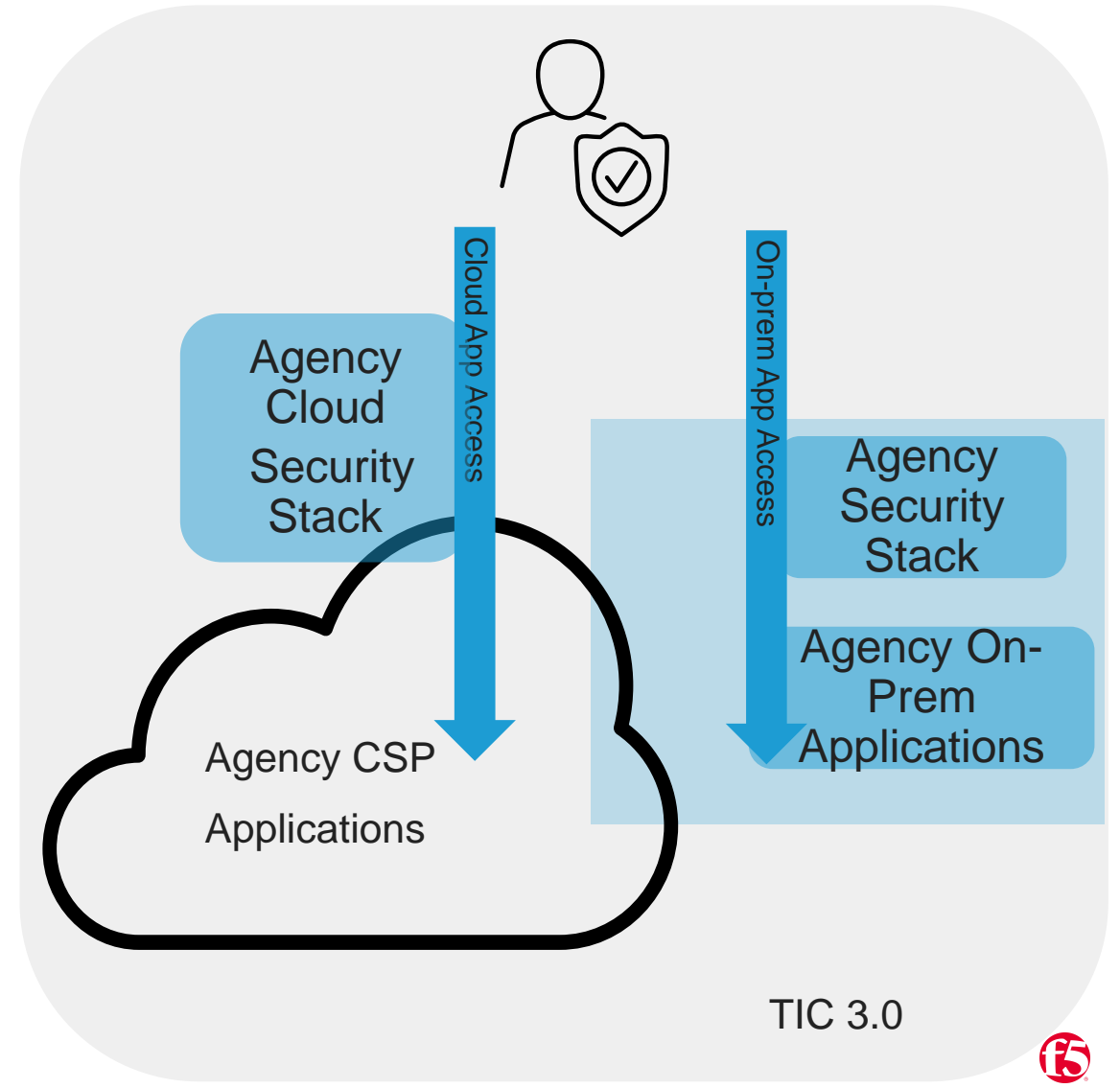
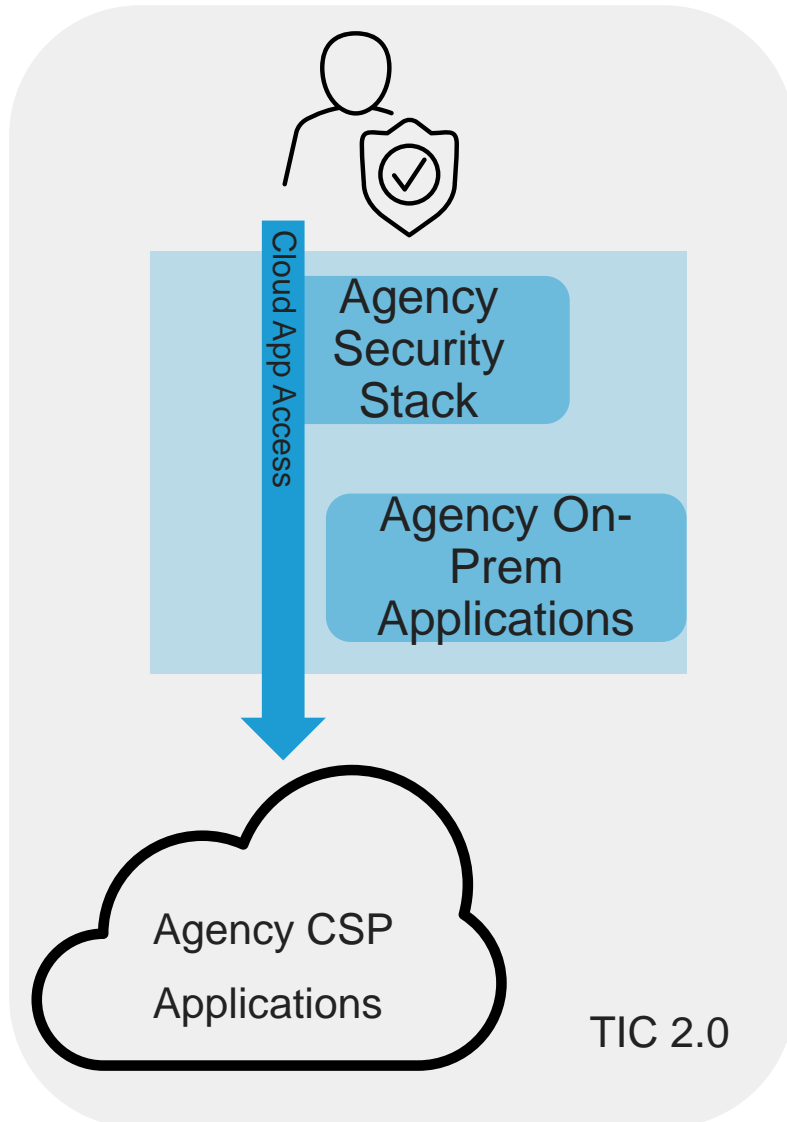
- F5 provides all M-21-31 application logging requirements for traditional and modern apps
- F5 provides all M-21-31 DNS logging requirements
- F5 products are fully automatable allowing for SOAR integration
- User behavioral monitoring
- F5 provides the ability to decrypt traffic for inspection and logging for F5 products as well as third-party security products
- F5 provides MFA CAC/PIV for Traditional and Modern Apps

Enforce MFA across applications

F5 can enforce user MFA to applications in traditional application environments and microservice/containerized environments

TIC 2.0 vs. TIC 3.0

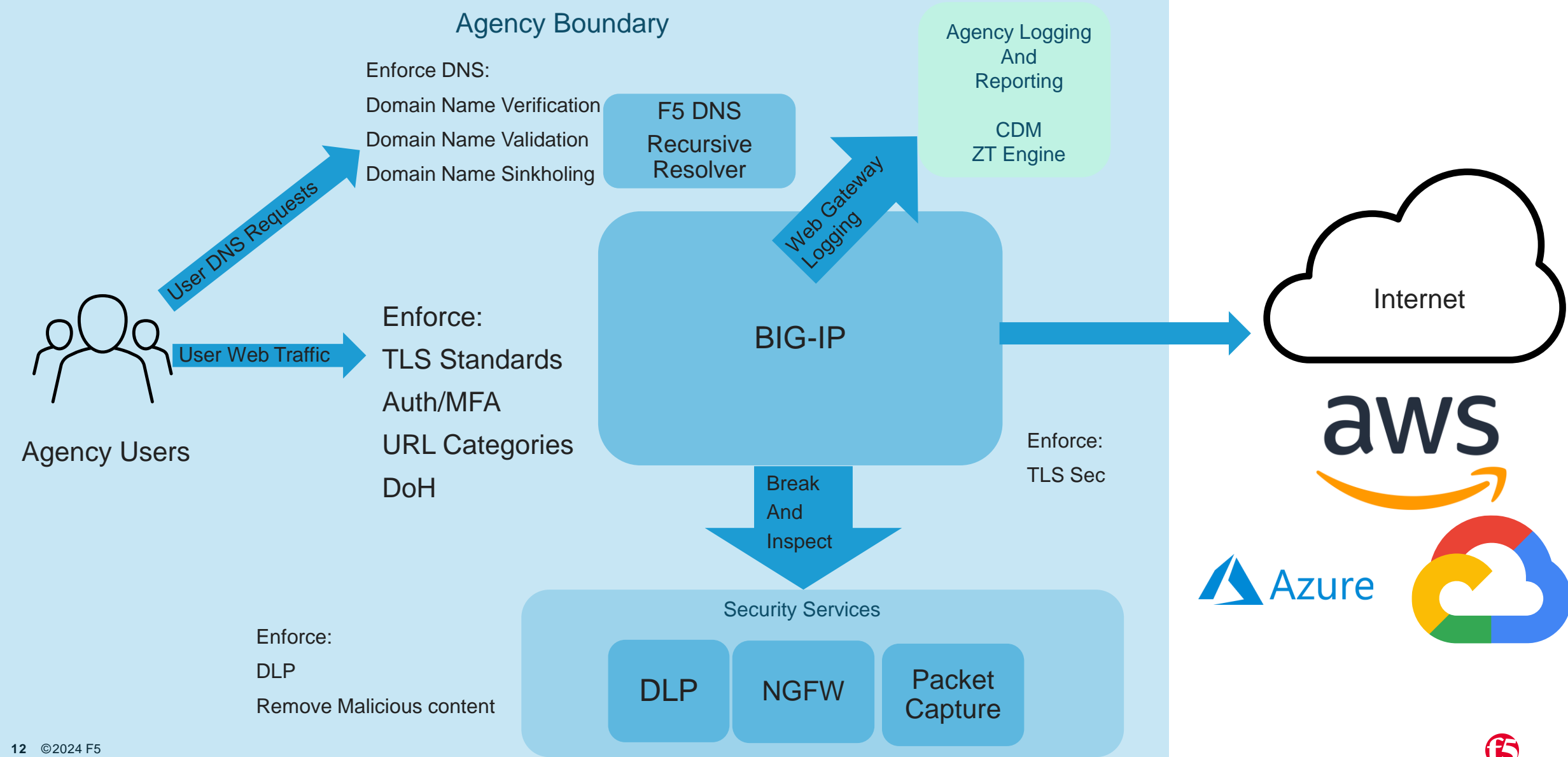
TIC 3.0 relaxes the security placement



Cybersecurity Executive Order bullets relevant to F5

- “The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks”
- “employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them”
- “including applying practices of least privilege, network segmentation, and proper configuration”
- “The Federal Government shall employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks.”
- “Information from network and system logs on Federal Information Systems is invaluable for both investigation and remediation purposes. It is essential that agencies and their IT service providers collect and maintain such data and when necessary to address a cyber incident”
- “The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.”
- “This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how”

Outbound TLS decrypt and secure web gateway by TIC 3.0 PEP



Other F5 Zero Trust material

- F5 Zero Trust Paper (upon request—ask your account team)
- Benefits of Zero Trust Adoption Through the Lens of MITRE ATT&CK and D3FEND Frameworks
 - <https://www.f5.com/resources/reports/office-of-the-cto-zero-trust-and-the-mitre-frameworks>
- M-22-09 "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" mapping to F5 products
 - <https://community.f5.com/t5/technical-articles/action-items-in-omb-memorandum-m-22-09-moving-the-u-s-government/ta-p/293847>
- Three-part Webinar Series: Adopting Zero Trust Security (On-demand)
 - <https://www.f5.com/company/events/webinars/3-part-webinar-series-adopting-zero-trust-security>
- What does the future hold for Zero Trust
 - <https://www.f5.com/company/blog/what-does-the-future-hold-for-zero-trust>
- Consideration of Techniques and Technologies for Adoption of Zero Trust
 - <https://www.f5.com/resources/reports/office-of-the-cto-techniques-and-technologies-for-zero-trust-adoption>

Inbound—App protection by F5 Zero Trust capability

