White Paper

Advancing Defense and Intelligence Security with Layer7® API Security

TABLE OF CONTENTS

Executive Summary

New applications communicating across sensitive security domains often require high-assurance guards to serve as security boundaries. Their restrictive nature requires a lengthy and costly recertification for each new protocol, data format, or change, to comply with strict certification rules. This requirement greatly increases time-to-mission and administrative overhead, reducing efficiency and increasing risk to national security.

The Layer7® API Security solution eliminates the need to recertify the high-assurance guard for new applications, and networking or protocol changes within them. It acts as a universal translator, transforming an application's native protocols into the specific format the high-assurance guard is already certified to accept. Placing a Layer7 API Gateway on both sides of the high-assurance guard allows government organizations to rapidly deploy new web-centric and legacy applications with a low-risk, Common Criteria Certified solution.

The Layer7® Cross-Domain Deployment Model

The Layer7 API Gateway removes the high-assurance guard's recertification constraint, because of its robust policy-based protocol and data transformation capabilities:

- **Protocol translation:** HTTPS, Kafka, SFTP, JMS, XMPP, TCP/UDP, FTPs, and so on, into the specific format for the high-assurance guard.
- **Data transformation:** XML to JSON, JSON to XML, unstructured to structured data, the specific format for the high-assurance guard.
- **Layer7 API Gateway deployment model:**
  - On the low side, a Layer7 API Gateway receives data from the application in its native protocol, applies powerful and flexible security policies, and applies the appropriate transformations and translations.
  - The high-assurance guard performs the required security checks.
  - On the high side, a second Layer7 API Gateway receives the data stream from high-assurance guard and transforms it back to the original, or any other format.

This model meets the high-assurance guard's security requirements and is transparent to the applications communicating across the boundary. This feature is especially useful for legacy applications that cannot be changed but still need to participate in a modern, Zero Trust environment.

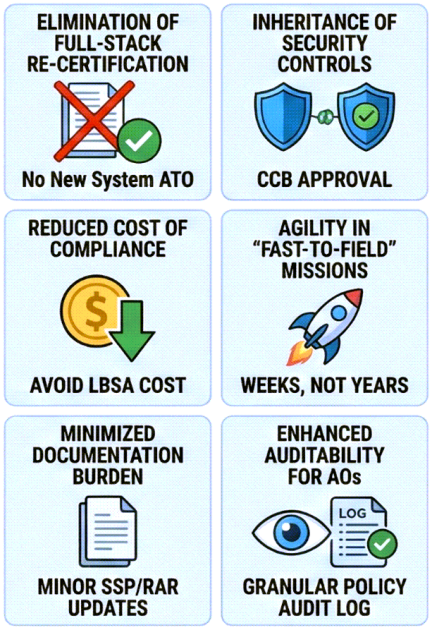
Key Features

- Eliminates lengthy high-assurance guard recertification to rapidly accelerate time to mission.
- Translates diverse military protocols to seamlessly integrate legacy applications.
- Provides a Common Criteria Certified, STIG-hardened, and FIPS-compliant boundary.
- Protects combat-support and AI applications using advanced rate limiting and DoS prevention.
- Enforces fine-grained, context-aware access control to support modern Zero Trust environments.

Federal Security Standards

- Common Criteria Certification
- FIPS 140-2 compliant
- FIPS 140-3 with hardware security module
- STIG hardened

Layer 7 Accelerating ATO and Reducing Time to Mission



Advanced Security Enforcement

In addition to transformation, the Layer7 API Gateway provides context-aware message introspection. As a policy enforcement point, this enhances security by inspecting every message according to the established security policy.

- **Cyberattack prevention:** The Layer7 API Gateway enforces protocol compliance with published standards and supports the use of post-quantum ciphers to mitigate common vulnerabilities and future-proof security.
- **Rate limiting:** Intelligently throttling API traffic protects critical infrastructure from Denial-of-Service (DoS) attacks and misconfigurations, ensuring high availability for combat-support and intelligence applications.
- **Metering:** Allows shared defense environments to track and audit data consumption across agencies, enabling observable resource distribution and precise chargeback models.
- **LLM defense:** Layer7 API Gateway rate limiting prevents prompt flooding and DoS attacks that could exhaust processing capabilities and degrade AI performance during time-sensitive missions.
- **Protocol coverage:** Enforces security policies across a wide range of net-centric and legacy technologies:
  - REST, SOAP, WSDL, and Web Services Security
  - XML Encryption (XML-Enc) and XML Digital Signature
  - OAuth 2.0, JSON Web Encryption, JSON Web Signature, JSON Web Tokens, and so on
  - Military protocols like Tactical Digital Information Links
- **Fine-grained access control:** The Layer7 API Gateway implements advanced access control models such as policy-based access control and attribute-based access control. Security enforcement decisions are user-defined and can incorporate a combination of identity, authentication protocol, time-of-day, IP address, message count, message content, and routing parameters.
- **Context-aware policy enforcement:** Adds the capability for behavior-based security policy, in cases where an API call might have valid credentials but is acting outside its normal parameters. Context-aware policy enforcement is similar to receiving a fraud alert when using a credit card in a different country.

Conclusion

The Layer7 API Gateway is a crucial component for certified high-assurance guards. It effectively bridges the gap between a high-assurance guard's static, certified protocol or data set, and the dynamic needs of modern applications to greatly reduce the time to mission. By transforming data and protocols and enforcing advanced, fine-grained security policies, the Layer7 API Gateway enables government organizations to rapidly and securely integrate new web-centric and legacy programs across security domain boundaries. This integration solves a critical limitation, allowing for the adoption of new programs with a high degree of confidence and security assurance.

For more information, contact us at engage.broadcom.com/ims-contact-us.

BROADCOM

For more information, visit our website at: www.broadcom.com

LSG-CDDT-WP100 March 18, 2026