radware

Securing Microservice Checklist

10 Commandments for Securing Microservices

SQL injections, cross-site scripting, access violations, remote file inclusion — running applications in a service mesh architecture doesn't eliminate the risk from data leakage or service disruptions. Emerging continuous integration and continuous delivery (CI/CD) technologies disrupt common practices and processes and create new blind spots.

Businesses require a next-generation web application firewall (WAF) that enables secure delivery of applications at the speed of the software development life cycle (SDLC), is as flexible as the dynamic environment and threat landscape and adapts to the needs of the business. Before considering any solution, make sure it meets the requirements of both development and operations (DevOps) and security teams. Here are 10 characteristics to look for when considering protection to data and applications in a service mesh architecture.

NATIVE FIT INTO CI/CD PIPELINE

1. **Kubernetes controlled elasticity** — Easily orchestrated, grows and scales application security along with Kubernetes pods, including autolearned policies and configuration settings.
2. **Automation at the speed of development** — Application programming interfaces (APIs) for integration with common tools for security provisioning of new services and applications, with a local management and reporting interface.
3. **TLS termination** — End-to-end encryption is necessary to secure data integrity and avoid eavesdropping and man-in-the-middle (MITM) attacks. A single TLS termination at the host also eliminates spreading multiple certificates across third parties.
4. **Minimal footprint** — Microservices are all about micro units; thus, the enforcement point in the data plane should be lightweight while the control plane (management, analytics and learning algorithms) is integrated into the environment independently.

QUALITY OF PROTECTION

5. **Extensive security** — Application protection today goes beyond the OWASP Top 10, so a good WAF needs to accurately detect malicious bot activity, secure APIs and mitigate denial-of-service attacks.
6. **Effective security (zero-day protection)** — Negative and positive security models are necessary to protect against known and unknown threats, thus maximizing security and minimizing false positives.
7. **Adaptive security** — Immediate detection of new and modified applications in the CI/CD pipeline isn't enough and must be followed by automatic generation and optimization of security policies.
8. **Data leakage prevention** — Make sure data that is being shared externally is protected. Credit card and Social Security numbers must be masked, cookies must be encrypted, and scrapers should be misled with fake data.

ADDITIONAL REQUIREMENTS

9. **Endorsed technology** — Multiple firms evaluate technology solutions, including ICSA, NSS, Forrester and Gartner. Don't take our word for it — check it for yourself.
10. **Comprehensive reporting and analytics** — Visibility to both development, security and operations (DevSecOps) and security teams via integration with common tools and platforms like elastic Kibana, Grafana, Prometheus, etc.

SELECT A SOLUTION THAT PROVIDES COMPLETE COVERAGE
WHILE ADAPTING TO YOUR CHANGING IT ENVIRONMENT.
LEARN MORE ABOUT RADWARE'S KUBERNETES WAF.