5 Steps to 360° Application Security

Tip #1:
This is just a sampling. The OWASP Top 10 List and other resources can provide additional information.

1. Identify common attack vectors & threats

Unsecured Personal Devices

Remote/Mobile Workers

SSL/TLS Encrypted Traffic

DoS/DDoS Attacks

Core Vulnerabilities

2. Secure the perimeter with firewall/next-gen firewall(s)

L2 ADC

FW/NGFW

L2 ADC

Tip #2:
ADCs/load balancers in a "firewall sandwich" can scale FW/NGFW throughput beyond 50 Gbps.

3. Decrypt and analyze SSL traffic; secure users' remote access

L7 ADC

Tip #3:
SSL VPNs provide end-point security, 2048-bit SSL encryption, advanced AAA and server-side security

Tip #4:
ADCs/load balancers decrypt SSL traffic, and include firewall and ACL capabilities to protect without impacting performance.

4. Add WAF and Advanced Security for additional protection

WAF

Advanced Security

Tip #5:
Web Application Firewalls, IDS/IPS, advanced persistent threat protection and other technologies typically operate "out of band" to inspect traffic without impacting throughput.

5. Don't neglect application-server security

Applications

Tip #6:
Many Web and application servers run OpenSSL, which has had multiple serious vulnerabilities. Non OpenSSL-based security as a front end can limit risk.

Source: Array Networks white paper, "360° Application Security"