TECH XCHANGE

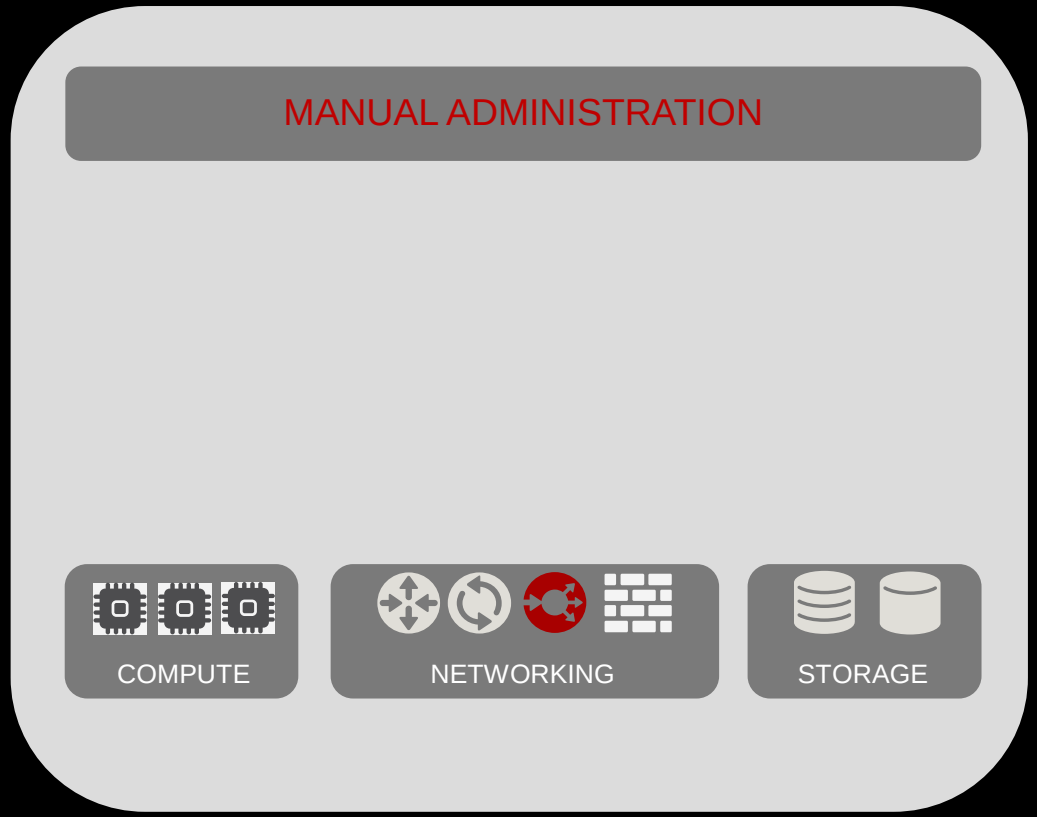
Make your App Faster, Smarter, Safer on Cisco ACI with F5

PRESENTED BY:

Wipawat Uppatumwichian

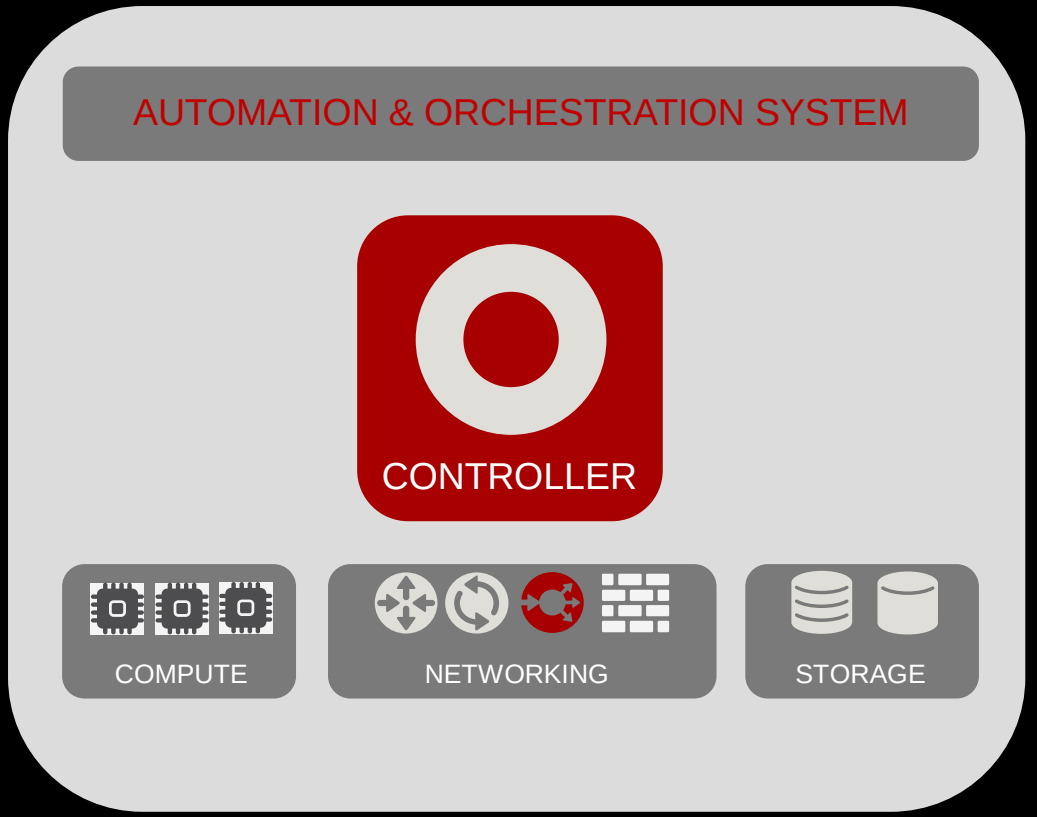
F5 Network Inc.

TRADITIONAL DATA CENTER



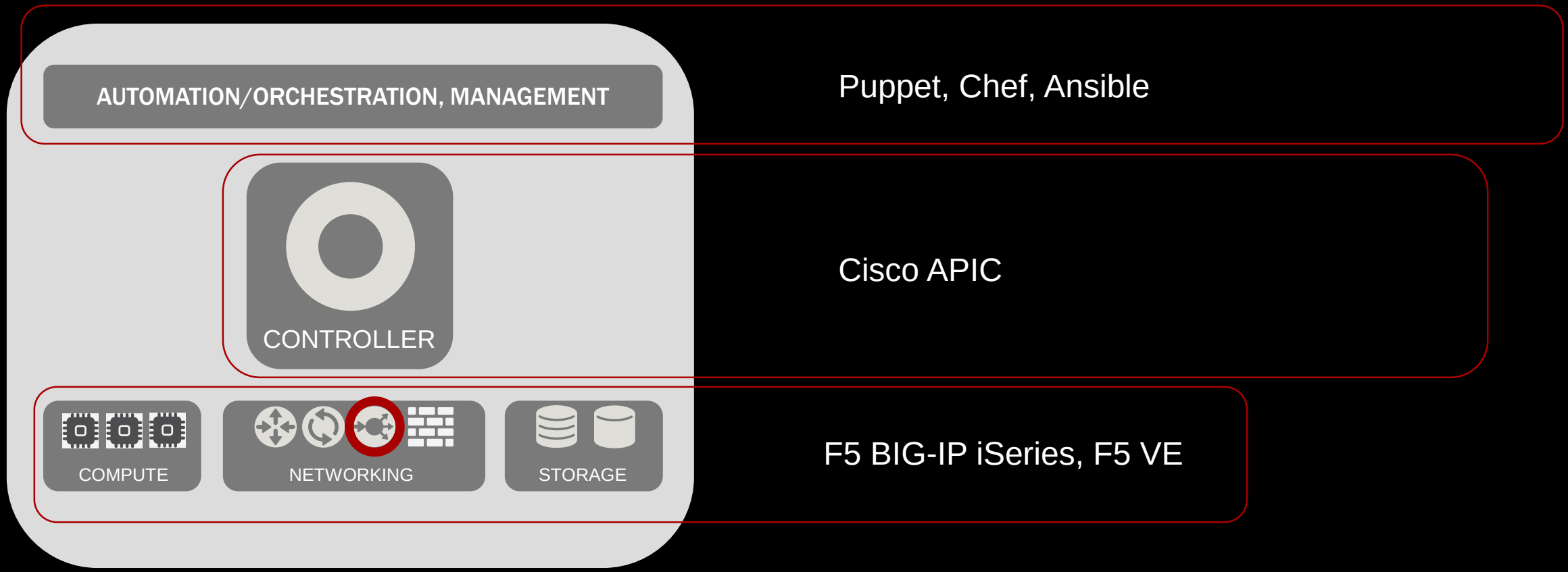
Manual administration of Compute, Networking and Storage

PRIVATE CLOUD DATA CENTER



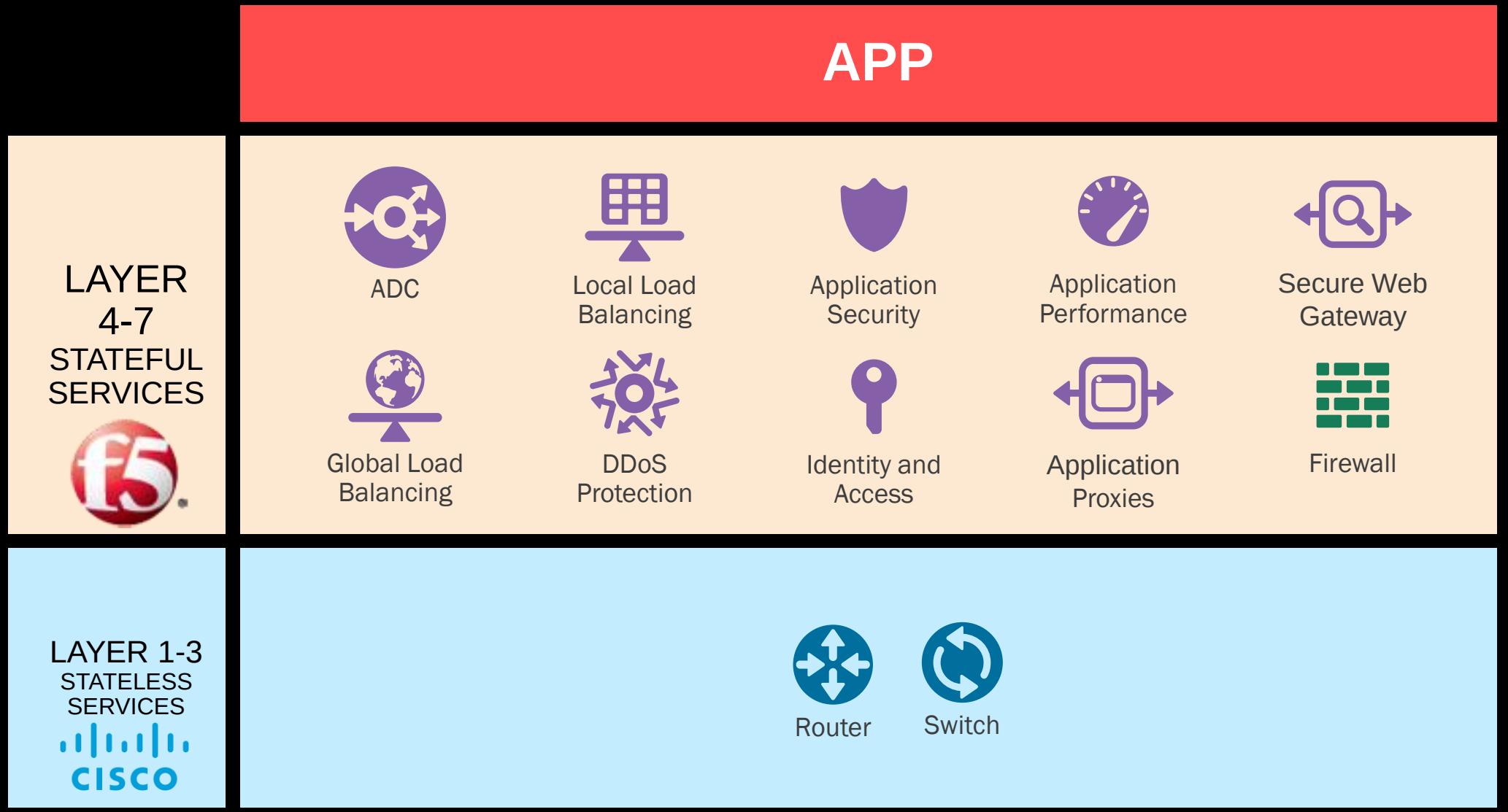
Automation and Orchestration systems driving Compute, Networking and Storage via Controllers

DATA CENTER



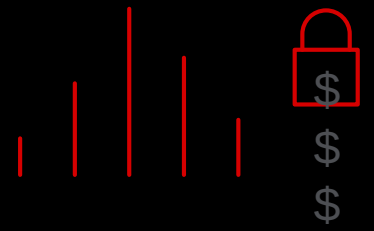
Automation and Orchestration systems driving Compute, Networking and Storage via Controllers

App stacks

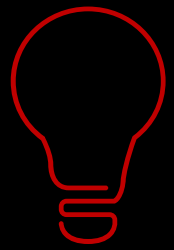


APPLICATION-CENTRIC THREATS

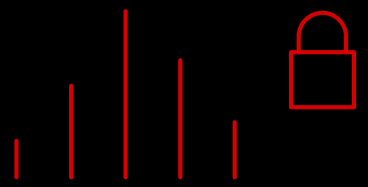
Application/Digital Currency



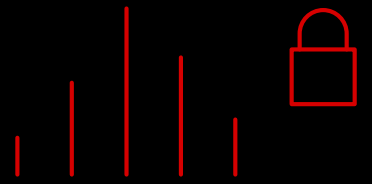
OWASP TOP 10



Application Infrastructure Components

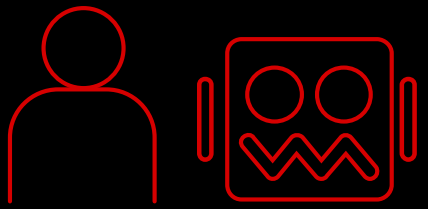


Attacks Hidden In Encrypted Traffic



Multi-Layered Attack Strategies

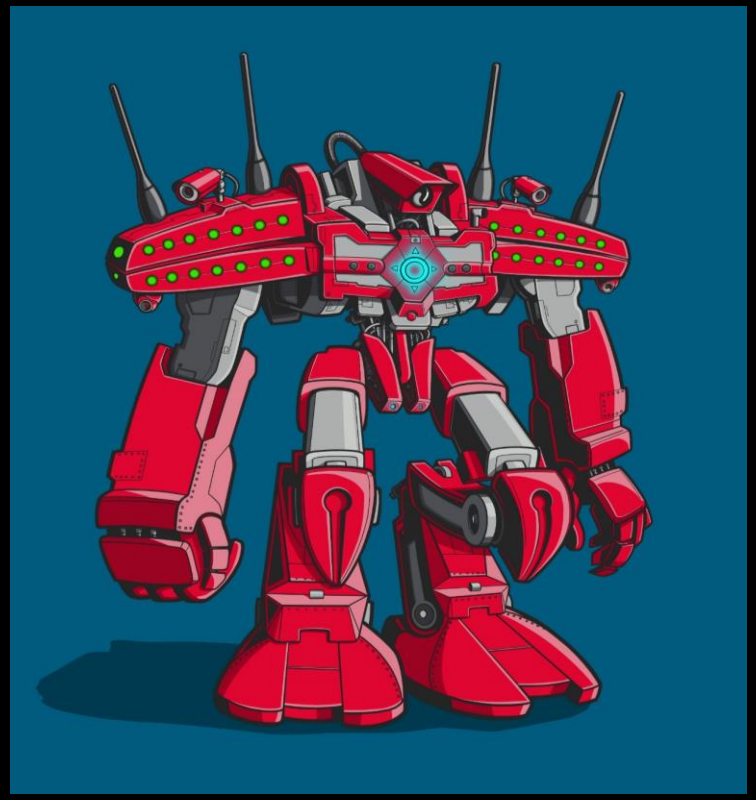
The Rise of Botnets



F5 LABS

THE HUNT FOR IoT

RISE OF THE THINGBOTS



MILLIONS
OF ATTACKS

BILLIONS
OF IoT DEVICES

PROTOCOL ADOPTION + POST QUANTUM COMPUTING

ENCRYPTION TRENDS

- HTTPS requests over 51%
- **TLS 1.2 preference high – SSL out**
- **Forward secrecy at 75%**

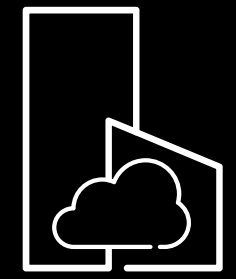
NEW ATTACK SURFACES

PUBLIC CLOUDS

CLOUD INTERCONNECT

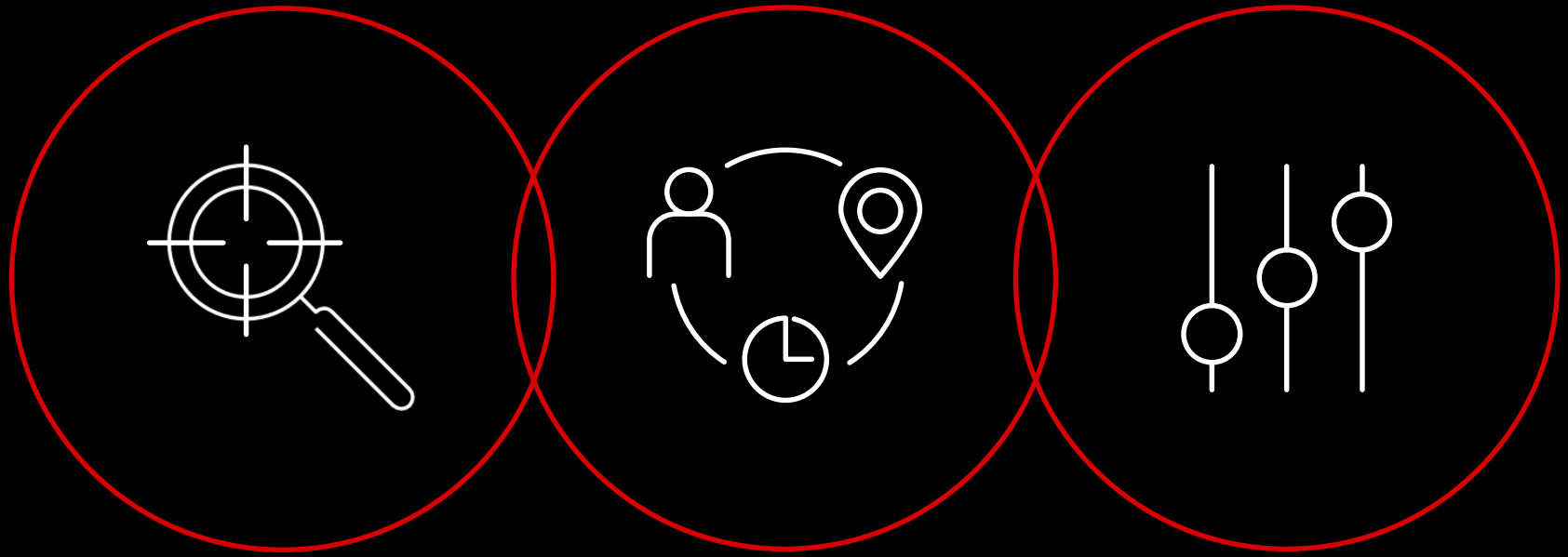
CONTAINER ENVIRONMENTS

PRIVATE CLOUDS




Our core belief:
APPLICATIONS
ARE THE GATEWAY TO DATA

The Foundation of App-Centric Protection

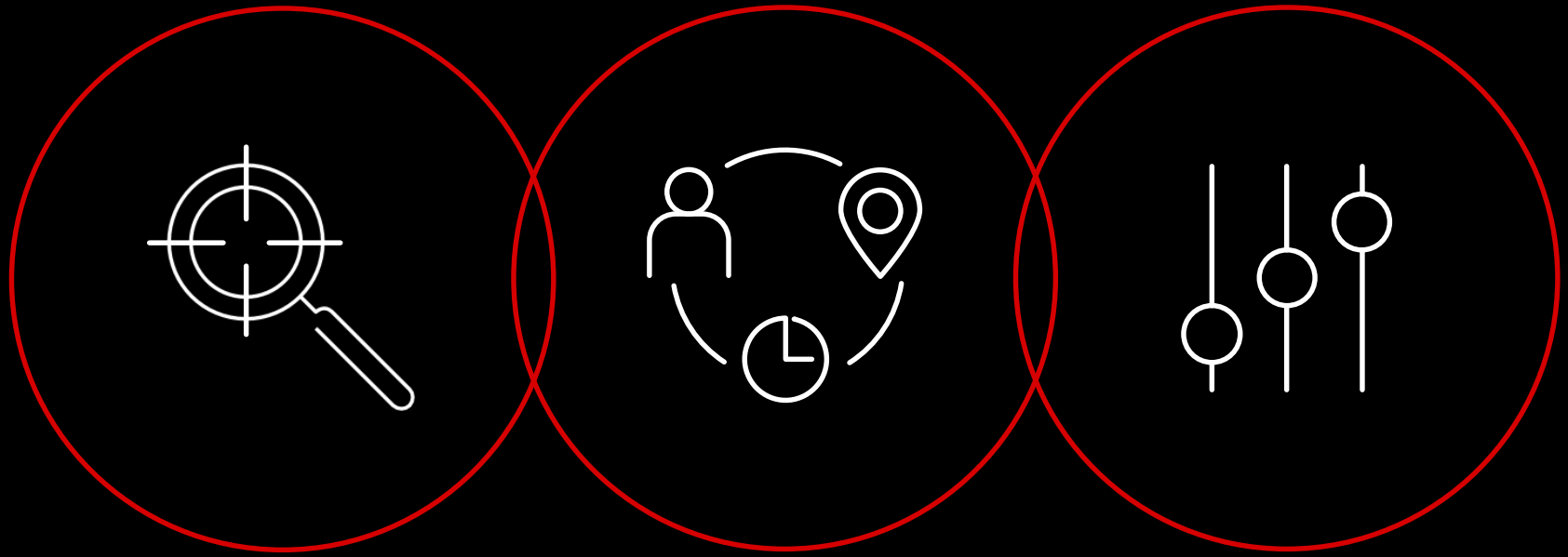


VISIBILITY

CONTEXT & BEHAVIOR

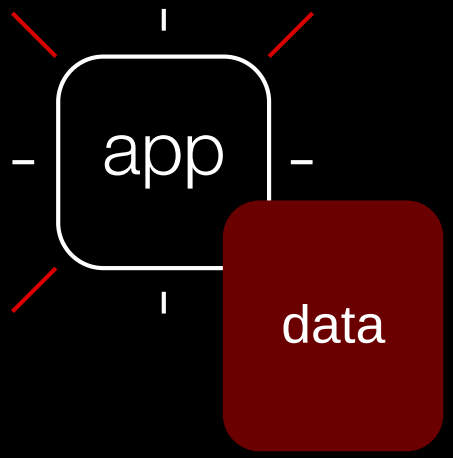
CONTROL

VISIBILITY

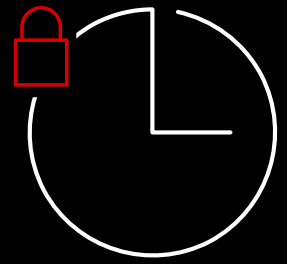


VISIBILITY

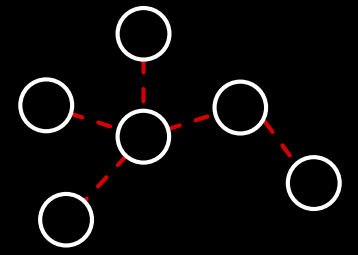
APPLICATION AWARENESS

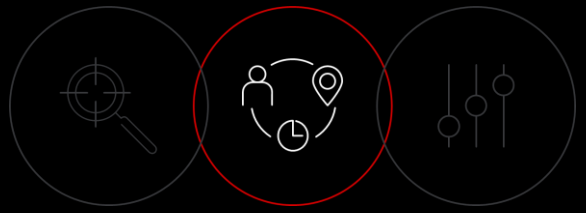


REAL-TIME ENCRYPTION



EXISTING SECURITY INVESTMENTS

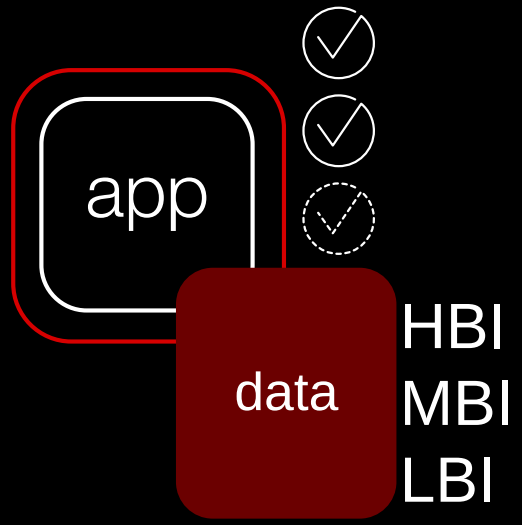




CONTEXT & BEHAVIOR

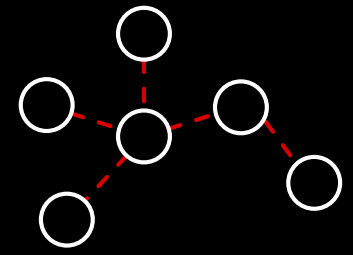
CONTEXT OF USER

CONTEXT OF APP



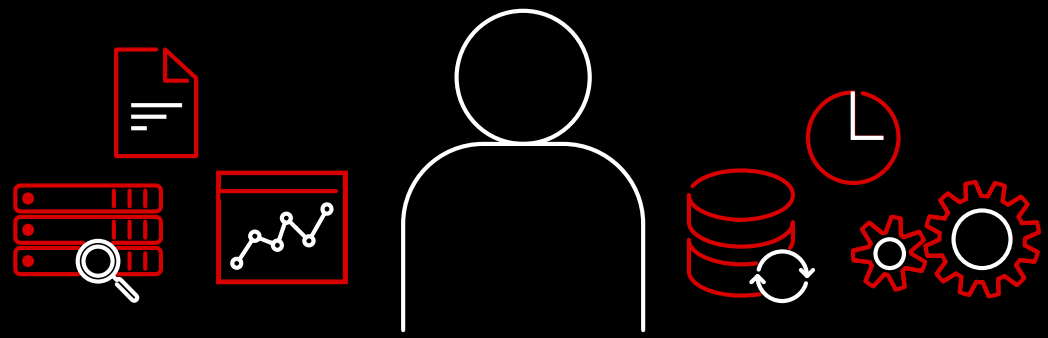
CONTEXT OF ON-PREMISE /CLOUD

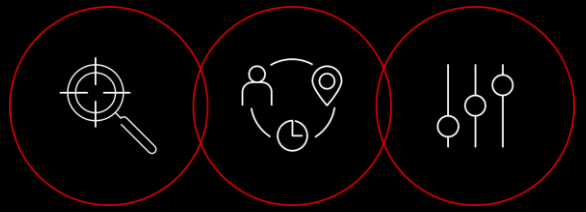
CONTEXT OF THREATS/VULNERABILITIES

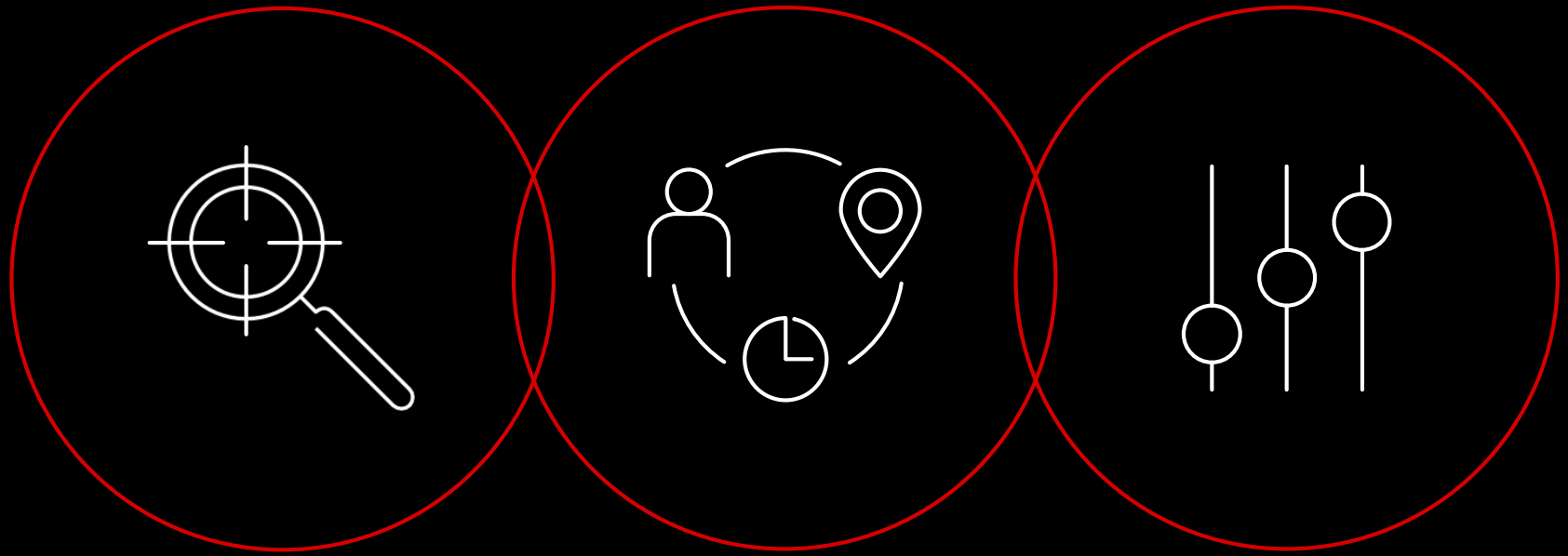


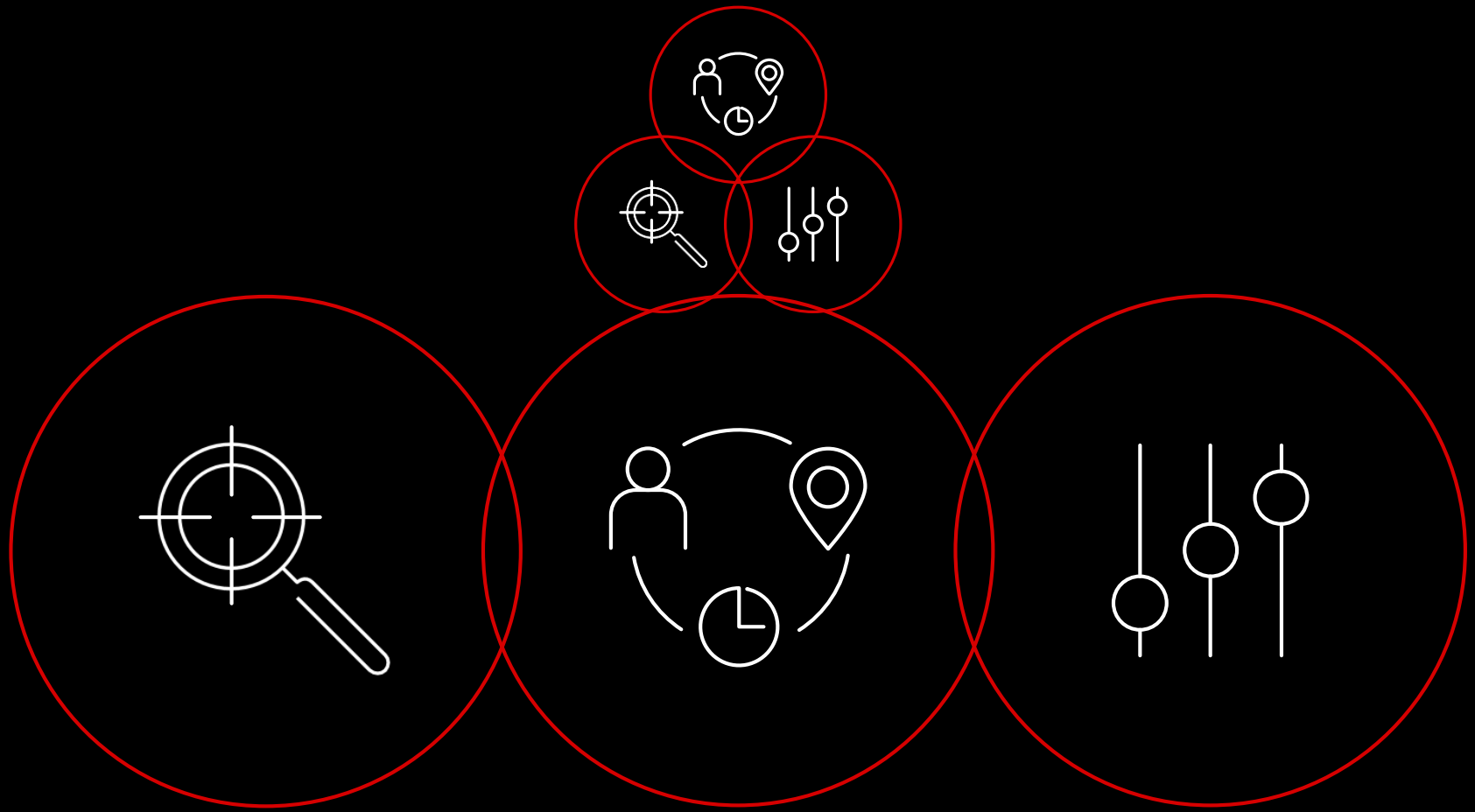
CONTROL

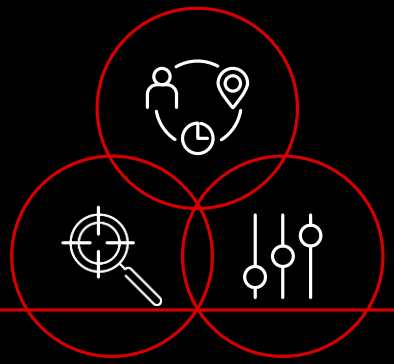
- Anti-DDoS
- Web Application Firewall
- SSL/TLS Security
- Web Fraud Protections
- DNS Security & Protection
- Identity Federation & Access









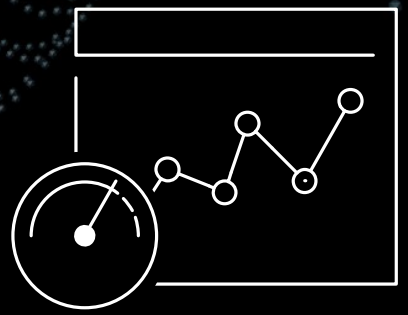


APP PROTECTION

Anti-DDoS
Application Firewall
Bot and fraud protection

CENTRALIZED SERVICES AND ANALYTICS

Full transparency
Risk and behavioral analytics
Centralized policies and management

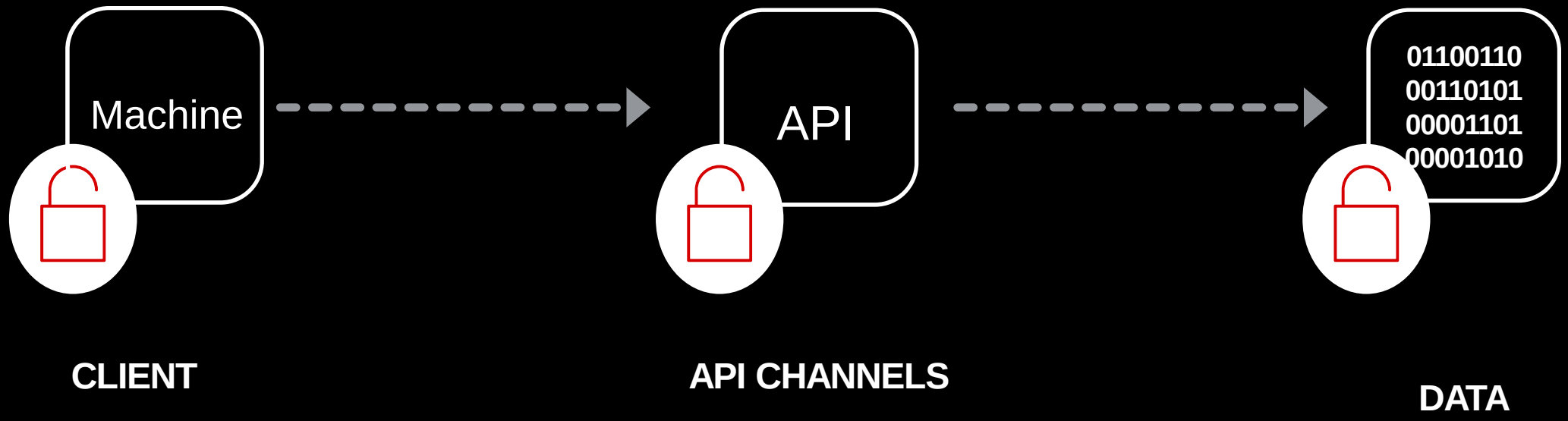


SUPPORT MULTI-CLOUD ARCHITECTURE

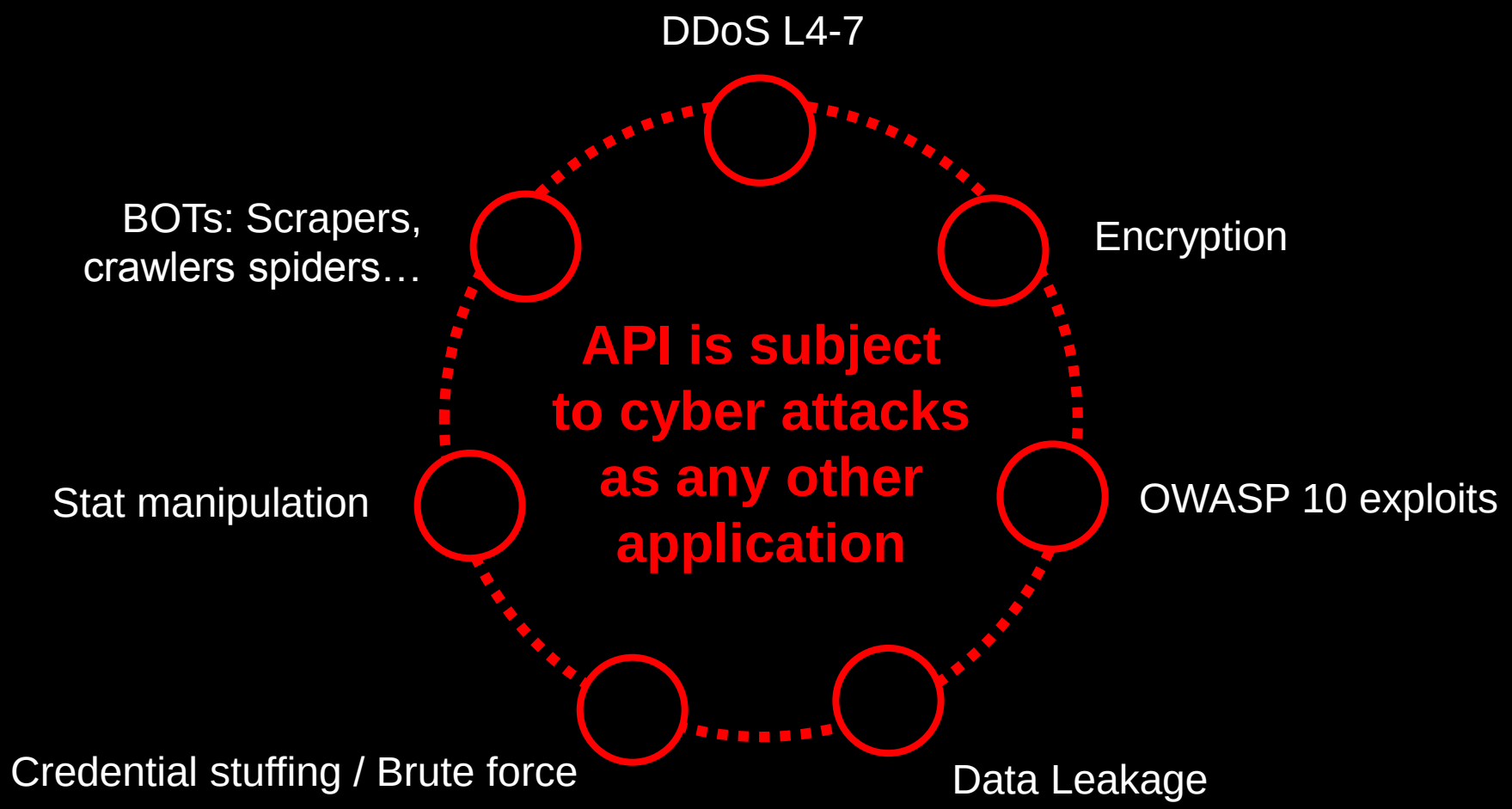
Independent from underlying technology
Security policy synchronizations
No cloud platform lock-in

API security

APIs Will Increase The Attack Surface



API Security Challenges

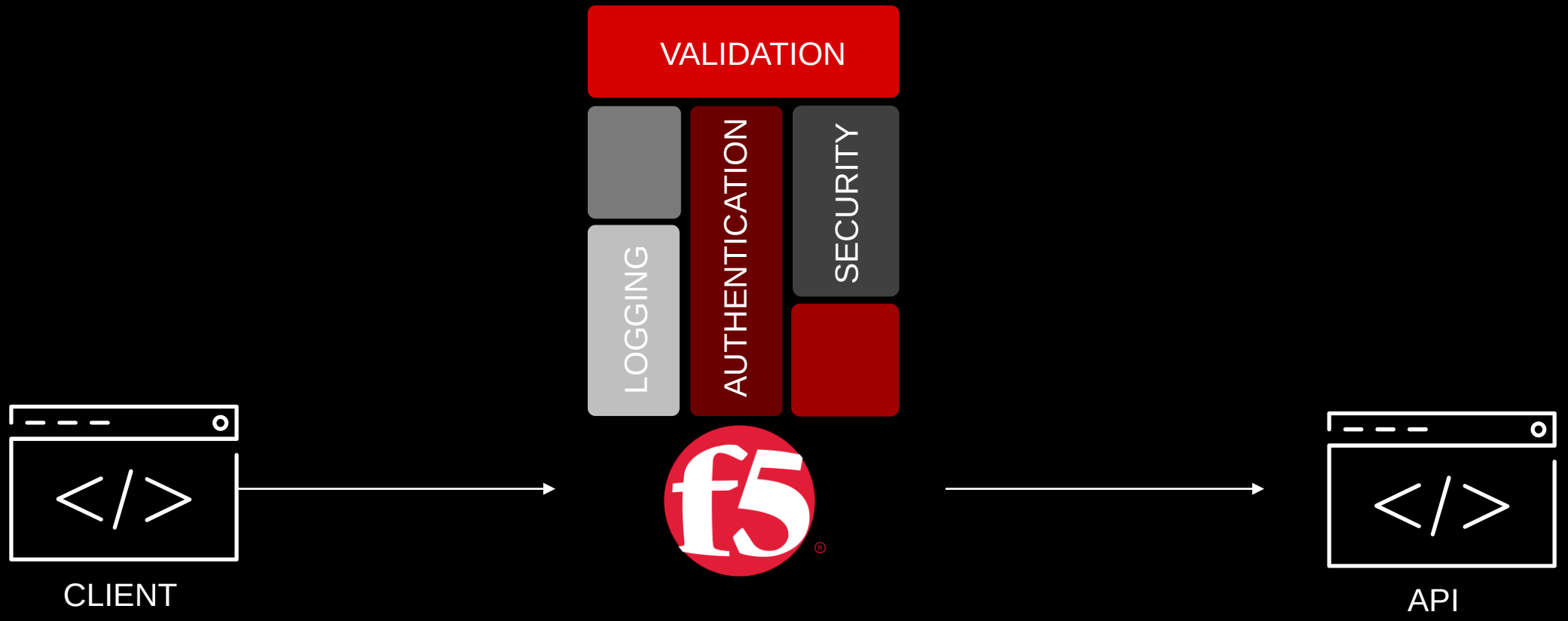


WAAP – Web Application and API Protection

Oct 2017 Gartner introduced new category for security solution

The solution can be based on a cloud-native development, or the reuse of the vendor's existing WAF appliance solutions in the back end. The core feature of a WAAP is a traffic processing engine that includes:

WAF	Bot Mitigation	DDoS Protection	API Security
This is mainly focused on injection attacks (XSS and SQL injection) and applicationlevel denial of service (DoS).	This involves detection and mitigation, if necessary, of automated connections. (It also includes user credential abuse.)	This leverages multiple points of presence and large bandwidth provisioning. (Some vendors also offer dedicated scrubbing centers.)	This is often limited to XML, REST and JSON payload processing and API usage thresholds.



WE MAKE APPS

FASTER. SMARTER. SAFER.