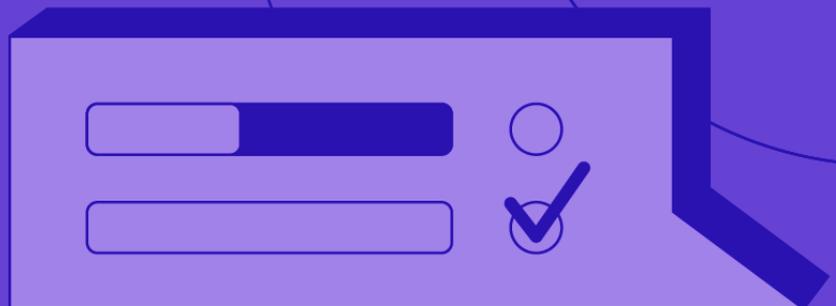Solution Brief

AttackIQ Boundary Posture Management (BPM)

AttackIQ's Boundary Posture Management (BPM) helps address the challenges of security control failure by continuously evaluating your boundary security, identifying security gaps between your assumed effectiveness and your actual security posture.

The average CISO has over 75 security controls to manage across an increasingly complex security enterprise. Yet even with the most advanced cyberdefense technologies, the best personnel, and the best processes, security controls fail constantly. To prevent security control failure, teams need to constantly test and validate their security program against multi-stage attacks using an automated breach and attack simulation platform that keeps pace with both adversary attack patterns and advanced defensive technologies.

AttackIQ's Boundary Posture Management (BPM) module addresses the challenges of security control failure by continuously evaluating your boundary security, generating analytic data about your performance, and identifying gaps between your assumed effectiveness and your actual posture. BPM runs multiple adversary emulations against your boundary security controls at scale and in production, generating real-time performance data about known threats. With the addition of BPM, AttackIQ provides the most comprehensive adversary emulation capabilities available on the market, emulating attackers with specificity and realism at the beginning, middle, and end of the kill-chain.

BENEFITS:

Provides continuous visibility into boundary security control effectiveness.

Validates boundary security effectiveness against multi-stage, comprehensive adversary attacks, leveraging packet capture (PCAP) replay between an attacking asset and target asset to assess in-line security control detection and prevention.

Executes end-to-end validation of network-deployed security controls in production and at scale.

Measures organizational detection and prevention effectiveness against advanced adversary TTPs.

Exercises and evaluates outsourced MSSP or continuous monitoring providers.

Generates technology-specific remediation guidance.

Provides analytic data to help decrease the possibility of a breach and minimize damage in the event of successful attacks.

How does Boundary Posture Management (BPM) do this?

Using already-deployed AttackIQ test points, AttackIQ's BPM evaluates the performance of network-deployed security controls with prescriptive guidance to maximize customers' investments in firewalls, web access filters, and other technologies. It does so through a combination of atomic tests, packet capture (PCAP) replays, inbound email attacks, and outbound data exfiltration to emulate a range of adversary behaviors, to include command and control, protocol enforcement, and DLP monitoring. It then provides clear mitigation recommendations with analytic data so that customers can improve their security posture.

FEATURES:

Tests Firewalls through Packet Capture (PCAP) Replays

- Command and Control
- Network Inspection
- Malware Transfer
- Protocol Enforcement
- Exploit Protection
- SSL Inspection Supported

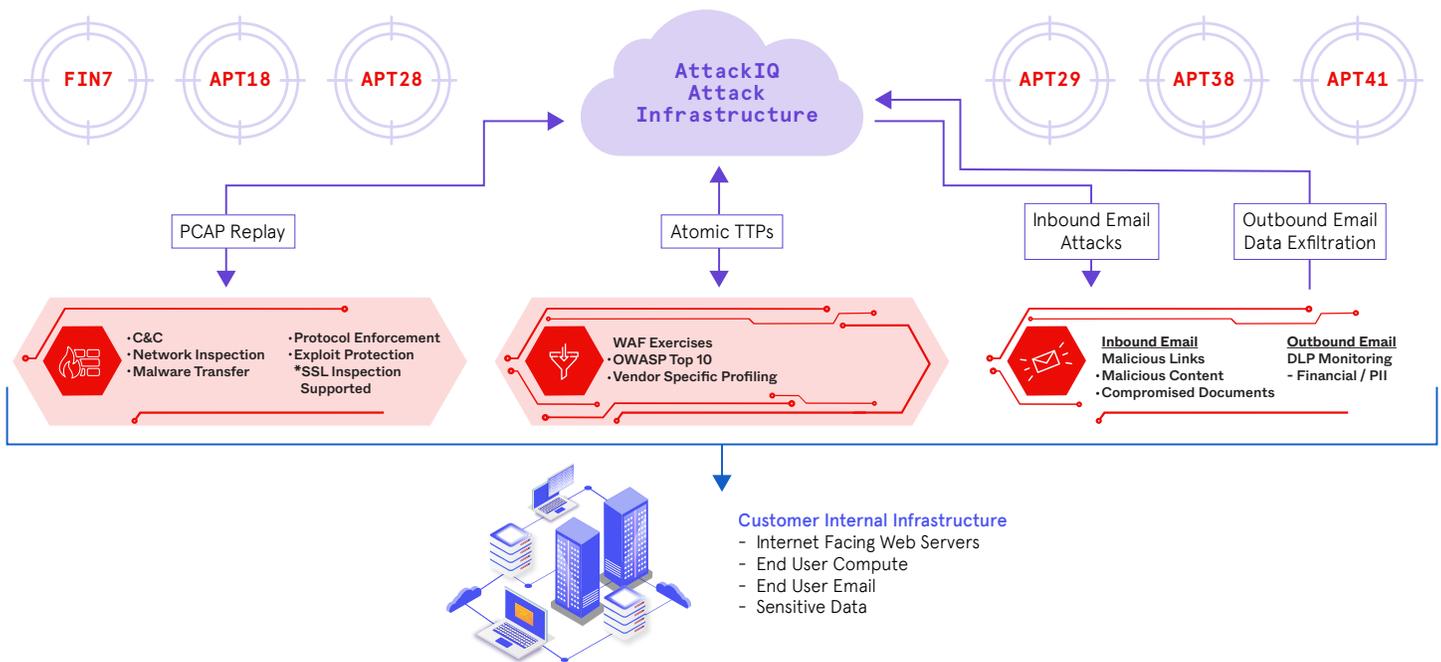### Tests Web Access Filter (WAF) through Atomic Tests

- Web Application Firewall (WAF) Exercises
- Open Web Application Security Project (OWASP) Top 10
- Vendor Specific Profiling

FEATURES: *(cont.)*

Tests Inbound and Outbound Emails:

- Inbound Email
- Malicious Links
- Malicious Content
- Compromised Documents
- Outbound Email
- DLP Monitoring
- Financial / PII

BPM Capability

Diagram nodes: FIN7, APT18, APT28 → AttackIQ Attack Infrastructure ← APT29, APT38, APT41

PCAP Replay
- C&C
- Network Inspection
- Malware Transfer
- Protocol Enforcement
- Exploit Protection
- *SSL Inspection Supported

Atomic TTPs
- WAF Exercises
- OWASP Top 10
- Vendor Specific Profiling

Inbound Email Attacks
Inbound Email
- Malicious Links
- Malicious Content
- Compromised Documents

Outbound Email Data Exfiltration
Outbound Email
DLP Monitoring
- Financial / PII

Customer Internal Infrastructure
- Internet Facing Web Servers
- End User Compute
- End User Email
- Sensitive Data