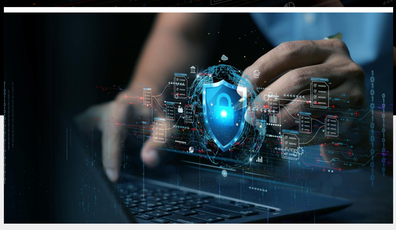
Validate Your Defenses
Against Real Attacks Specific to Your Environment



The New Reality

You can spend months building a strong cybersecurity stack: firewalls, endpoint tools, cloud controls, SIEM, and identity protections. But there's always one uncomfortable question:

Will it work as planned when the situation goes beyond "normal"?

A control can work in 10 scenarios and fail in the 11th due to a change, misconfiguration, missed integration, or workload shift. That's why modern security is built on one principle: trust, but verify, and verify continuously.

> You can build a strong cybersecurity stack, but the real test is whether it works beyond normal conditions. That's why modern security is built on one rule: trust, but continuously verify.

The Stakes Are High

Even well-funded environments can develop gaps without anyone noticing until it's too late. That's also why leadership asks a direct question:
Are we getting adequate ROI from our cybersecurity infrastructure, and is it working as efficiently as we expect?

AttackIQ highlights measurable outcomes such as

44% Reduction
in costs from breaches

47% Efficiency
gains in security ops

Up to $800K
in savings from tool consolidation

*Results vary by environment and scope.

Why Point-in-Time Assurance Breaks

Most organizations validate security in bursts: audits, periodic checks, occasional pentests, or reactive fixes after an incident. That leaves long windows where controls drift, detections fall behind, and assumptions go untested.

What teams need is a way to test continuously and safely, against realistic attack paths in their own environment, not just in theory.

Your Advanced Defense: Paramount + AttackIQ

AttackIQ runs controlled simulated attacks to validate whether security controls and detections behave the way you think they do, across endpoint, network, identity, email, and cloud vectors. It produces evidence you can use (for example, attack success rates and dwell time) so teams can measure improvement over time.

Paramount brings the delivery layer: deep security expertise, technical know-how, managed services support, and regional understanding. Validation doesn't stop at findings; it becomes fixes, tuning, and measurable improvement.

Validates controls across key attack vectors: endpoint, network, email, identity & access, and cloud (mapped to real attacker techniques).

Runs safe simulations for high-impact scenarios, including ransomware behavior and advanced persistent threat (APT) emulation.

Improves incident-response readiness by continuously pressure-testing detections, controls, and response workflows, not just once-off audits.

Produces quantifiable metrics (e.g., attack success rates, dwell time) that leadership can use to justify budgets and support compliance discussions.

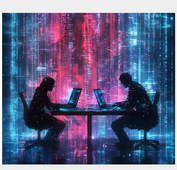
Supports third-party risk assessment (M&A, fintech/integrated partners, managed service partners) by testing integrated environments and surfacing weaknesses before a real breach.

The Joint Offering

A managed Security Validation-as-a-Service program designed to enhance SOC and MSSP outcomes by continuously validating controls and strengthening detection coverage.

Security Validation-as-a-Service (powered by AttackIQ, delivered by Paramount)

- Continuous control assurance
- Gaps identified across deployed controls and SIEM use cases
- Proactive verification that customer tools perform as expected
- Coverage mapping aligned to MITRE ATT&CK
- Evidence-based assurance reporting



Why This Matters

Every organization has a different mix of workloads, cloud usage, identity patterns, and tooling. That means adversaries don't exploit "generic security", they exploit your gaps.

Your cybersecurity is unique

You need to constantly evaluate it against threats relevant to your organization, not just "the latest threats."

Why Choose Paramount as Your Partner

Paramount stands as a regional leader in cybersecurity, trusted by organizations that cannot afford uncertainty when it comes to protecting critical information assets and infrastructure. In a world where security controls can silently drift and threats continuously evolve, we don't just deploy solutions – we ensure they perform when it matters most.

- A baseline validation run against priority controls
- Flexible testing with custom scenarios designed for your environment
- A prioritized findings report plus recommended fixes
- Optional tuning guidance for better detection and response outcomes

Connect with us today: Ask us for an assessment