How To Comprehensively Validate Your Endpoint Security Capabilities

ATTACKIQ + CYLANCE

BENEFITS

The AttackIQ and Cylance partnership and technical integration enables organizations to validate that both CylancePROTECT® and CylanceOPTICS™ are deployed correctly and configured optimally, ensuring protection for your endpoints against the latest threats.

1. Assess your current capabilities
2. Prove the benefits of using Cylance
3. Continuously demonstrate that Cylance is protecting your organization as intended

Highlighted Capability		AttackIQ + MITRE ATT&CK Validation Tactics
CylancePROTECT	CylanceOPTICS	
AI-driven malware prevention	Context-driven threat detection	Initial Access, Execution, Persistence, Defense Evasion, Credential Access, Lateral Movement
Memory exploitation prevention	On-demand root cause analysis	Initial Access, Execution, Privilege Escalation
Script management	Automated playbook driven response	Execution, Persistence, Defense Evasion
Application control for fixed-function devices	Remote investigation and remediation	Execution, Persistence, Defense Evasion

About Cylance

Cylance uses artificial intelligence to deliver prevention-first security solutions and specialized services that change the way organizations approach endpoint security. Cylance security solutions combine AI-driven predictive prevention with dynamic threat detection and response to deliver full spectrum threat prevention and threat visibility across the enterprise.

Visit **www.cylance.com** for more information.

About AttackIQ

AttackIQ is the leader in continuous security validation and has built the first platform that enables organizations to measure and validate the effectiveness of their security program. Leveraging the MITRE ATT&CK framework, AttackIQ provides organizations with evidence to prove current capabilities and also determine the highest probability risk exposures and gaps in their defensive strategy. Empowered by data, organizations can now make data-driven decisions to minimize the risk to their business.

Visit **www.attackiq.com** for more information.

FAQs

- **How does AttackIQ test the defensive capabilities of a security program?**
  AttackIQ's platform continuously exercises the full breadth and depth of your entire security program. We go on the offense to identify security control failures before the attacker does to proactively identify gaps and prioritize remediation. Our platform creates controlled adversarial behavior relevant to your environment and simultaneously measures and validates your detection and prevention capabilities.

- **Are AttackIQ's scenarios safe to run?**
  AttackIQ's scenarios are 100% safe to run and will do no harm to your production devices or network. We test real adversarial behavior by recreating known attacker patterns. All of our scenarios are certified to do no harm.

- **Are you testing real attacks or simulated attacks?**
  AttackIQ's scenarios recreate real attacker behavior. Our dedicated research team dissects both real malware and attacker behavior from "living off the land" and creates do-no-harm scenarios that produce the same behavior but are safe to run on production systems and networks.

- **What resources are required to do the testing?**
  The only requirement is to install one test-point agent on your network. From there, simply run a security assessment that will recreate attacker behavior on the control.

Not only will AttackIQ identify weak spots or flaws in existing defenses, but it will also find areas where misconfigurations or installation mistakes are preventing good cybersecurity tools from operating properly.

- CSO From IDG Product Review, January 8, 2019

"Before investing in yet another cybersecurity tool, organizations wanting to strengthen their security posture should prioritize investing the few minutes necessary to evaluate AttackIQ, a tool that can continuously validate the effectiveness of their existing cybersecurity toolchains, identify gaps, and help remediate issues."

- ESG Product Lab Evaluation, January 2019

SCHEDULE A DEMO