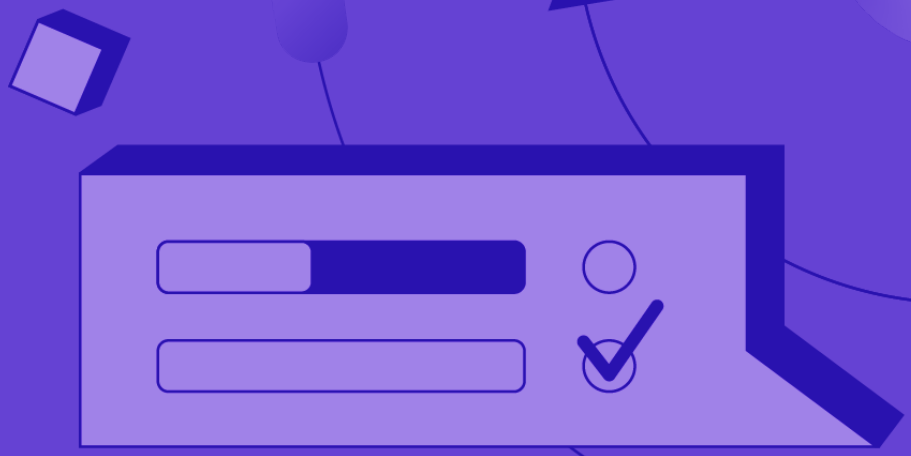
ATTACKIQ®

cisco SECURE Partner

Solution Brief

AttackIQ® Integration With Cisco Secure Endpoint Turns Assessment of Endpoint Controls Into a Routine Part of Day-to-Day Operations



AttackIQ® Integration With Cisco Secure Endpoint Turns Assessment of Endpoint Controls Into a Routine Part of Day-to-Day Operations

Every endpoint detection and response (EDR) solution promises to secure endpoints companywide. Marketing materials claim the products provide visibility into all attacks the endpoints deflect, as well as accelerating remediation anytime a threat approaches.

There's no doubt that corporate networks require effective EDR. But how can a cybersecurity team know that the endpoint security solutions they've deployed are living up to the marketing claims? The key is to emulate attacks and evaluate the efficacy of the response by staff and the security infrastructure.

To improve the efficiency of such evaluations, Cisco partnered with security optimization provider AttackIQ to integrate Cisco Secure Endpoint with the AttackIQ Security Optimization Platform.

Cisco Secure Endpoint Offers Comprehensive Protection

Cisco Secure Endpoint is a single-agent solution that provides comprehensive protection, detection, response, and user access coverage to defend against threats to an organization's endpoints. The SecureX™ platform is built into Secure Endpoint, as are extended detection and response (XDR) capabilities.

The combination of EDR, XDR, and SecureX threat-hunting capabilities, with integrated risk-based vulnerability management, helps organizations quickly detect threats. That streamlines investigations and facilitates faster response in the case of an attack. The cloud-native solution reduces remediation times by as much as 85 percent.

AttackIQ Streamlines Control Assessments

AttackIQ is the independent leader in automated security control validation. AttackIQ operates under the "assume breach" mindset, recognizing that no defenses are completely impenetrable. At some point, an intruder will break past any organization's perimeter defense and into the interior.

The AttackIQ Security Optimization Platform automates security control validation using the industry's leading breach and attack simulation capabilities. It leverages the MITRE ATT&CK® framework to help security teams understand adversaries' tactics, techniques, and procedures (TTPs). Then it runs assessments and attack graphs — end-to-end simulations that string together multiple techniques in a chain — to fully emulate the adversary at the beginning, middle, and end of the kill-chain.

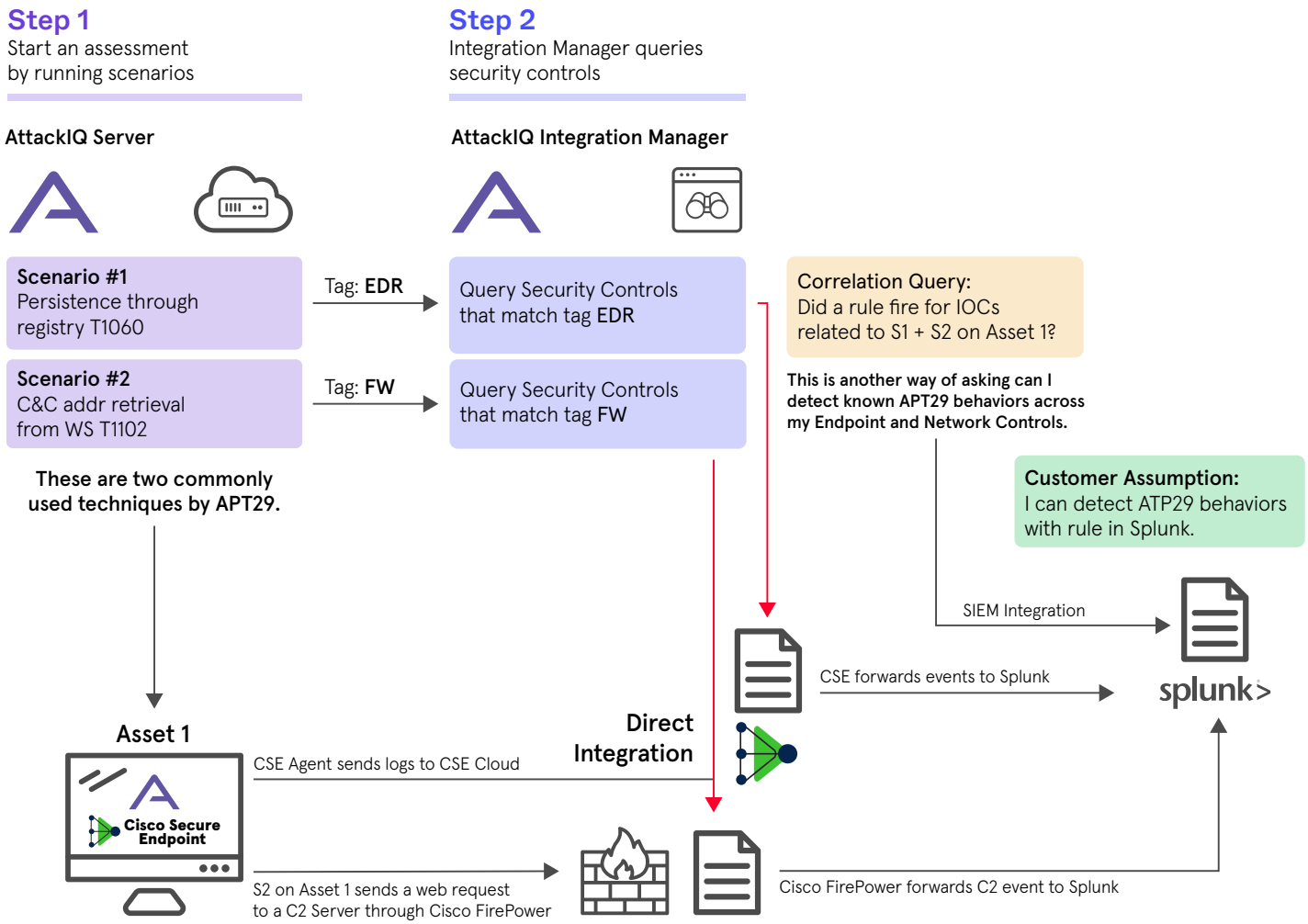
By automating security control assessments, the AttackIQ Security Optimization Platform significantly reduces the human effort required to validate security controls against real-world threats. This efficiency, in turn, enables an organization to much more frequently assess whether its controls are performing as expected.

Integration Improves AttackIQ Efficiency in Assessing Cisco Secure Endpoint

Cisco and AttackIQ engineers collaborated to develop a tight integration between the two solutions. The AttackIQ Security Optimization Platform can now query Cisco Secure Endpoint log files to efficiently assess whether the endpoint protection solution recognized specific simulated events and how well it responded to them.

For example, AttackIQ Security Optimization Platform might attempt to perform a command-and-control (C&C) address retrieval on a customer's network to contact a server outside the network (the red-teaming portion of the testing). In an actual attack, the goal would be to exfiltrate customer data. In the case of AttackIQ, the goal is to trigger an appropriate response from the customer's endpoint security solution.

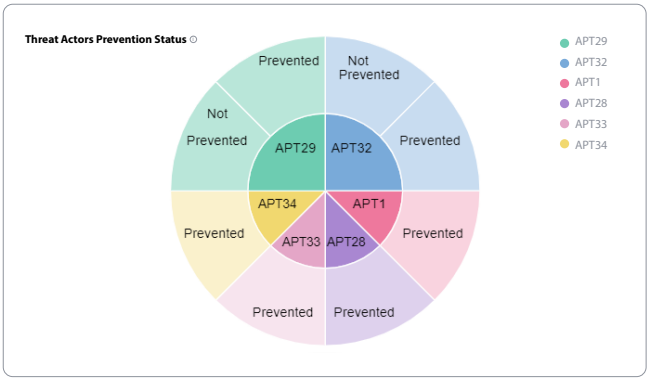
This is illustrated in step #2 in Figure 1. The AttackIQ Security Optimization Platform runs a scenario emulating a C&C attack. Cisco Secure Endpoint should discover and log the emulated security event. After initiating the event, the AttackIQ Security Optimization Platform queries Cisco Secure Endpoint log files to determine whether the EDR solution detected the simulated attack and responded appropriately.

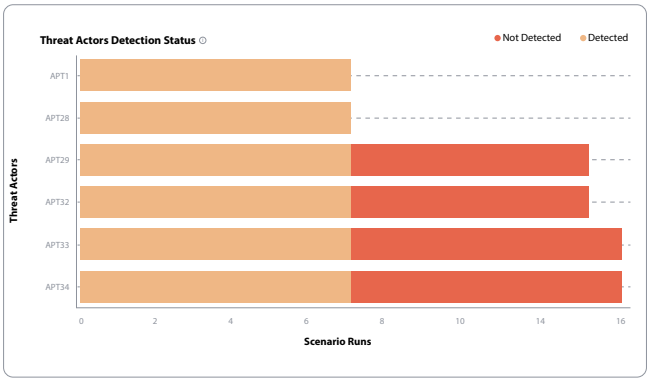


Prove Controls Effectiveness

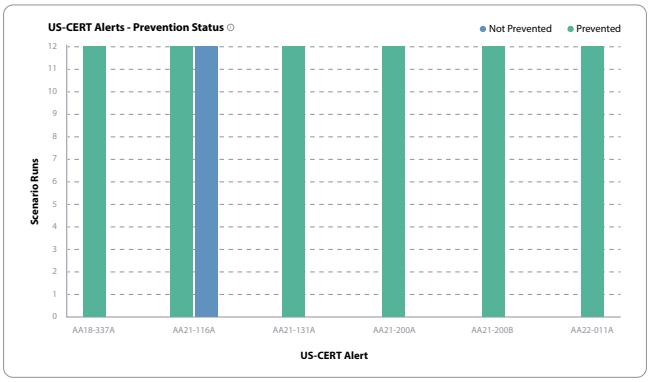
This integration enables Cisco Secure Endpoint customers to continuously emulate realistic attacks that are likely to threaten their endpoints. When the EDR solution successfully thwarts an assessment or attack graph, the customer's security team gains confidence that Secure Endpoint is configured properly and performing to expectations. The below figures show detection and prevention success rates by threat actors, US-CERT alerts, and top MITRE ATT&CK techniques (as curated by the Center for Threat-Informed Defense).

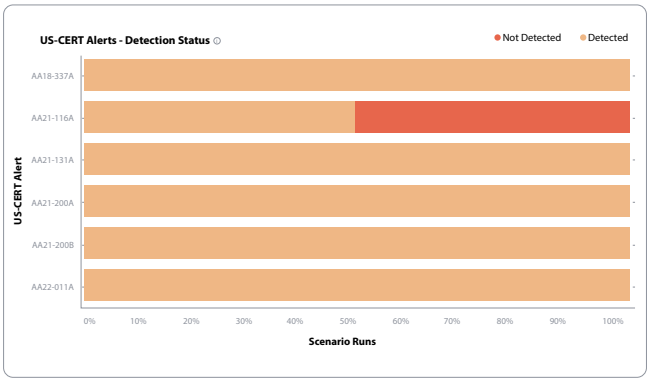
Threat Actors





US-CERT Alerts

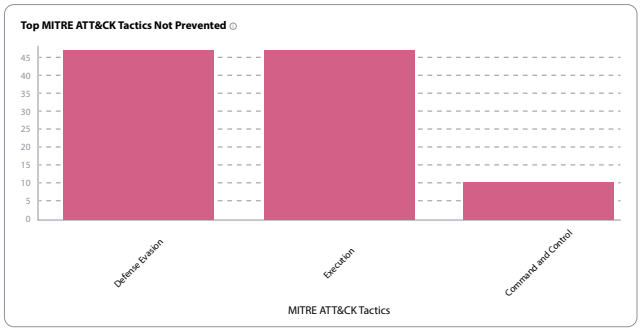


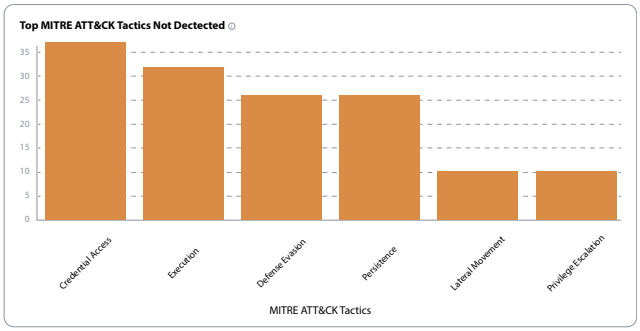


continues on next page.

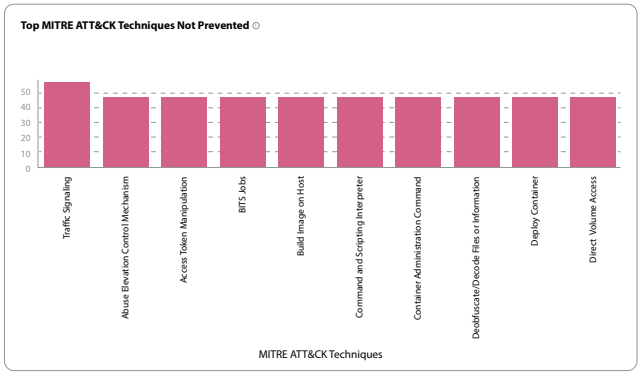
Prove Controls Effectiveness (cont.)

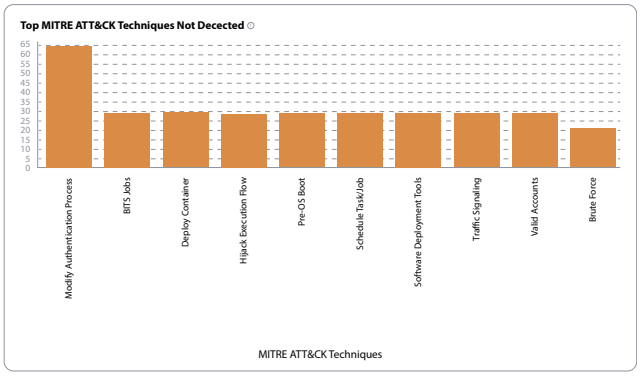
Top MITRE ATT&CK Tactics





Top MITRE ATT&CK Techniques





From a business outcome standpoint, if an emulation is successful, the security team will find gaps in their security coverage before the adversary can. The practical information provided by the Cisco and AttackIQ integration helps teams prioritize security investments to optimize their threat-informed defense.

The only way for an organization to be sure its endpoints are secure is to assess their EDR solutions' detection of and response to real-world attacks. The efficiencies built by integrating Cisco Secure Endpoint with the AttackIQ Security Optimization Platform enable security teams to make endpoint control assessments a routine component of their day-to-day operations.

ATTACKIQ
U.S. Headquarters
171 Main Street, Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with the MITRE Engenuity's Center for Threat Informed Defense

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.