

ForgeRock OpenAM and FireEye TAP Integration

Speeding Threat Detection and Remediation

SOLUTION BRIEF

SECURITY
REIMAGINED

INTEGRATED SOLUTION HIGHLIGHTS

- Leverages the strategic partnership between threat intelligence and identity security leaders.
- Pairs dynamic identity data with high-quality threat indicators.
- Delivers a unified dashboard to help security teams identify attacks based on compromised credentials.
- Provides a more comprehensive picture of when and how advanced attackers are targeting an organization.
- Prioritizes actionable intelligence to reduce the alert response burden on security teams.
- Integrates across security layers for in depth coverage.

OVERVIEW

Modern customer-facing identity solutions need to employ a light touch when dealing with users, all while providing the highest possible security. They need to deliver a great, easy to use service that empowers the user wherever possible, such as, easy self-registration or password reset. Otherwise, the users will seek other avenues of access.

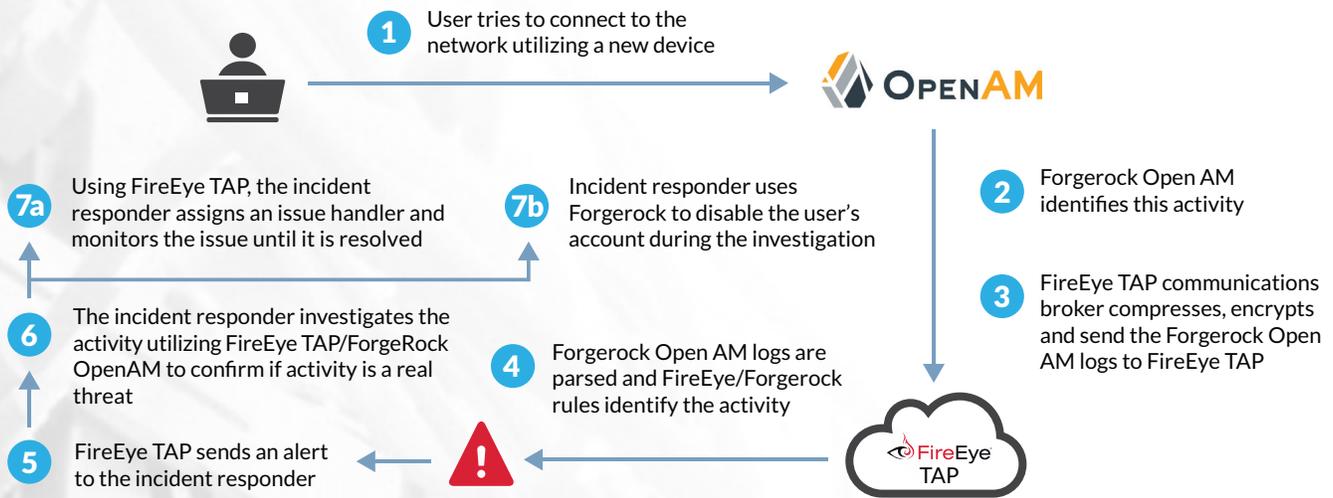
As the volume of threats increases on a global basis, it's increasingly imperative that threat detection systems handle real-time discovery of an attack. These systems need to also communicate with identity and access management platforms to lock down access when an attack is underway.

In most enterprises, the IT teams that handle security at the perimeter and the teams that handle network security are separate and rarely communicate. Unsurprisingly, the technologies they deploy do not communicate either. This fragmented approach to cyber security leaves inherent gaps and weaknesses that are ripe for a malicious attack. The ForgeRock and FireEye partnership closes this gap with our joint solution integration.

THE CHALLENGE

IT security team challenges come from a variety of directions. But can be summarized as follows:

- Threat actors have an in-depth understanding of user access practices of organizations and are adept at compromising security provisions.
- The current approach of deploying point security solutions inhibits effective communications and collaboration among these multi-vendor applications.
- Separation of network security responsibilities between perimeter security and internal network security teams leaves a gap that threat actors can exploit.
- As threat detection improves, the sheer volume of alerts overwhelms security teams with an inadequate capability to prioritize the threats that demand immediate attention.
- Stolen credentials facilitate an increasing number of breaches.
- Security teams must create a balance between convenient user access and effective in-depth security.



THE INTEGRATED SOLUTION



FIREEYE VERSION
12.01 and newer

FORGEROCK VERSION
11.0 and 12.0

When the FireEye TAP, a cloud-based security incident detection and response management platform, combines with ForgeRock's real-time intelligence on end-users, the integrated solution allows organizations to make timely security decisions based on location, IP address, time of day, known device, and other context clues. It also provides a more comprehensive picture of when and how advanced attackers are targeting an organization. Actionable intelligence is prioritized according to risk, enabling organizations to detect advanced attacks and insider threats quickly. As a result, the joint solution stops incidents before they become widespread.

THE VALUE OF THIS PARTNERSHIP

Digital identities are at the center of every online interaction and essential to achieving a 360-degree, closed-looped security model. The FireEye-ForgeRock cybersecurity coalition partnership provides mutual customers with real-time, dynamic identity data paired with high-quality threat indicators to better protect their networks from malicious attacks. The integrated solution provides a unique way to gather security intelligence quickly and provide it to customer organizations so that they can speed threat detection and remediation.

This integration allows near real-time identity context from ForgeRock paired with FireEye's expanding database of threat indicators and event and log information from across the enterprise. This provides more visibility into these threats, allowing FireEye to alert security teams of suspicious activity and help protect enterprises against attacks.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise – reinforced with an aggressive incident response team – helps eliminate the impact of breaches. The FireEye Global Defense Community includes 3,400 customers across 67 countries, including over 250 of the Fortune 500.

ABOUT FORGEROCK

ForgeRock, the fastest growing identity relationship management vendor in the world, is building secure customer relationships across the modern web. Focused on using digital identities to grow revenue, extend reach, and launch new business models, ForgeRock's Open Identity Stack powers solutions for many of the world's largest companies and government organizations.

For more information contact CSC@fireeye.com.