FireEye

Subscription Datasheet

Oculus Continuous Monitoring

Real-time threat monitoring for advanced awareness of the most dangerous APT attacks

Highlights

- Provides around the clock, around the world continuous monitoring
- Delivers advanced warning of APT and zero-day attacks utilizing the superior threat intelligence derived from millions of MVX engines deployed globally
- Reduces alert noise so you can focus on what matters
- Provides monthly reports and FireEye Cybercon™ incident alerts about threats specific to the industries you care about

Your team is busy, and your adversaries know that. In today's threat landscape, advanced persistent threat (APT) attacks are often lost in the noise of everyday alerts. FireEye® delivers advanced warning of APT and zero-day attacks to help reduce the noise so you can focus on what really matters; protecting against the attacks that have successfully penetrated your traditional defenses.

Extending the FireEye Threat Prevention Platform, Oculus Continuous Monitoring provides real-time threat monitoring that leverages superior threat intelligence, global services, and bleeding edge threat research. The FireEye Oculus team, which includes some of the industry's top cyber analysts, constantly monitors subscribed systems for advanced attacks—not just in your organization but other organizations in your industry or geography.

Service Details

Oculus Continuous Monitoring subscriptions comprise of these core components:

Proactive APT Alerts—When FireEye detects an APT and/or a zero-day attack, subscribers will receive a proactive notification to ensure they can follow-up on this attack as soon as possible. This includes proactive notifications when FireEye detects the existence of cybercrime tools used by advanced threat actors.

FireEye provides an overview of the threat upon notification and organizations can use their private, secure FireEye collaboration workspace to access the APT Encyclopedia, an online reference tool for information on a specific APT. The FireEye Oculus team will provide more APT threat details when available and/or as requested. The collaboration workspace is also the channel to securely share details about the APT with the FireEye Oculus team.

For organizations that need additional assistance, FireEye and trusted partners provide on-demand access to malware analysts and incident responders.

FireEye Cybercon Reports—Customers receive monthly reports and FireEye Cybercon incident alerts about emerging industry-specific threats. A clear, actionable FireEye Cybercon rating indicates the severity of risk and lets subscribers know when threat risks increase in their industry or region. FireEye will notify customers as soon as the FireEye Oculus team determines there is an attack underway and of any updates to the FireEye Cybercon level. All subscribing Oculus Continuous Monitoring customers will receive a detailed version of the industry FireEye Cybercon reports.

System Health Monitoring—Proactive notification of potential issues with subscribed systems that pose health or detection-efficacy risks. Organizations also receive a monthly system health report in their private collaboration space.

Methodology

FireEye taps into global, real-time threat intelligence that is continuously generated by thousands of FireEye deployments running millions of FireEye Multi-Vector Virtual Execution (MVX) engines. This threat intelligence is made actionable by the FireEye Oculus team through in-depth analysis of real-world outbreaks and advanced, bleeding-edge research.

FireEye provides a unique value proposition by diving deeper into potential threats to identify the adversaries that have a vested interest in customers' information assets and to assess the adversaries' intent and capabilities to carry out the threat.

With MVX technology, FireEye platforms generate a rich data set of threat intelligence to provide customers early warnings of advanced attacks. Customers that participate in bi-directional sharing with the FireEye Dynamic Threat Intelligence (DTI) cloud provide threat metadata about malicious activities that can be analyzed and aggregated to show trends in attacks targeting a specific set of customers based on geography, industry, or other common factors. This allows FireEye to identify patterns, and thus predict other victims, often before those organizations even realize they are being targeted and, sometimes, even before zero-day vulnerabilities have been publicized.

By identifying advanced cyber attacks as soon as possible and providing customers with proactive alerts and threat intelligence reports, customers can secure their business against would-be threat actors seeking to harm infrastructure, steal sensitive information and valuable data.

FireEye Dynamic Threat Intelligence provides global, real-time visibility into advanced threats