FIREEYE™

SOLUTION BRIEF

The Bridge Between Security, Development and Operations

The Efficiency-Security Balance
Every CIO and CISO has a responsibility to move the business forward, securely. In a perfect world, the CIO would accelerate business operations using the latest technology and the brightest of minds, while the CISO would align security operations in lockstep with advancements throughout the organization. In reality, more efficient operations are rarely realized in parallel with more secure operations.

Moving quickly while keeping costs low is especially challenging where security is concerned. More security requirements make development more difficult and when developers make security decisions without oversight, they can create complications for CIOs and CISOs.

The ultimate challenge, then, is to find opportunities for synergy across teams with different sets of incentives, skills and tools—to strike a appropriate balance between efficiency and security.

The Players
There is not always a clear separation between developer and operations professionals. Developers make security decisions through their automation of infrastructure as code, while security practitioners depend on development workflows to operate at the pace and scale of cloud deployments.

However, development and security teams still rely on different sets of people; with different incentives, processes and tools. **Insecure cloud deployments result from a lack of communication** between such teams.

Organizations try to make DevOps more secure (SecDevOps) and to develop new tools to make SecOps more efficient (DevSecOps). Both approaches involve significant challenges. It is never easy to automate security decisions at the pace of cloud innovation and DevOps, and security budgets are not built for large development teams.

Elevated Enterprise Risk
Simple mistakes are magnified in cloud environments. The networked nature of the cloud, the automated actions via APIs, the dynamic deployments driven by distributed decision making–they all expand the impact of cloud security incidents. When everything is automated, everywhere, then all of your mistakes are automated, everywhere.

Threat actors are poised to take advantage of such opportunities with malidious bots and advanced persistent threats. Enterprises currently face an unprecedented level of risk.

Typical Security Challenges

Security and development teams each struggle to encapsulate and translate their knowledge in a way that is directly useful to the other. Cloud and DevOps technologies make it possible to encapsulate (and share) deployment logic as an infrastructure as code software repository, which can enable fast, consistent deployment.

However, infrastructure-as-code automation allows development decisions—even flawed ones—to follow the code to new environments (for example, from Dev to QA to Prod). Because simple mistakes are magnified in cloud environments, security teams must catch misconfigurations as quickly as possible (fail fast, fail early) to catch (local) bugs before they become (global) incidents. Although some developers may consider the code self documenting, the language of infrastructure-as-code is not immediately useful for security practitioners. Without a tool that can translate between security policies and development code–to minimize or prevent the impact of misconfigurations–security teams may try to pull back control over deployments they do not understand. As a result, deployment velocity (efficiency) decreases as security requirements limit development options.

The Options

Enterprises often face a tough choice. They must choose to push technology forward for the sake of business efficiency, or pull technology back for the sake of business protection. They can attract talent through innovation or drive talent away through bureaucracy. The choice seems to be, "Please the CIO or the CISO… but not both."

Better options involve a hybrid form of the development and security mindsets.

The development mindset may say: "Bring good development processes to the SecOps tech" (DevSecOps). The security mindset may say: "Bring good security processes to the DevOps tech" (SecDevOps).

Unfortunately, developers and security professionals follow different processes that align with their incentives and tools. What works for one group may not work for the other.

The Solution

It is better to facilitate communications between the two groups rather than to try to have one adopt the processes or technologies of another. Better communication enables:

The knowledge of the security team to be used in development by the development team

The actions of development teams to be verified by their security counterparts before changes are made

The automation of interactions between teams which can allow each team to move at its own pace, following its own processes and use its own tools.

FireEye Cloudvisory facilitates better communications between development, deployment and security teams. Pre-deployment teams can keep their existing processes while leveraging knowledge from the security team, importing rules for scanning infrastructure as code and integrating development outputs with Cloudvisory's common pipeline for harvesting security events. Deployment teams can use Cloudvisory to track risks introduced into different types of environments (such as pre-deployment, quality assurance, production) and automate the time-consuming process of harvesting data and removing the security guesswork from gated CI/CD pipelines. Security teams can use Cloudvisory as a force multiplier and universal translator, allowing a small (central) group of security professionals to scale their influence by pushing their knowledge to the edge of the enterprise in a useful way: to translate security policy into the languages of developers and machines.

To learn more about Cloudvisory, visit **www.fireeye.com/products/cloudvisory.html**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.