Trellix

SOLUTION BRIEF

Trellix Cloudvisory

The bridge between security, development, and operations

The efficiency-security balance

CIOs and CISOs have a responsibility to move their organizations forward securely. In a perfect world, the CIO would accelerate business operations using the latest technology and the brightest minds, while the CISO would align security operations in lockstep with advancements throughout the organization. In reality, more efficient and more secure operations are rarely realized in parallel.

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 is to find opportunities for synergy across teams with different sets of incentives, skills, and tools to strike an appropriate balance between efficiency and security.

The players

There isn't always a clear separation between developers 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's never easy to automate security decisions at the pace of cloud innovation and DevOps, and security budgets aren't built for large development teams.

Elevated enterprise risk

Simple mistakes can easily become magnified in cloud environments. The networked nature of the cloud, the automated actions via APIs, and the dynamic deployments driven by distributed decision-making can expand the impact of cloud security incidents.

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

Typical security challenges

Security and development teams struggle to encapsulate and translate their knowledge in a way that's 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, it can carry over from development to quality assurance to production.

Security teams must identify cloud misconfigurations as quickly as possible 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 don't understand. As a result, deployment velocity and efficiency decrease 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.

Better options involve a hybrid of development and security mindsets. The development mindset may say, "Bring good development processes to the SecOps technology." The security mindset may say, "Bring good security processes to the DevOps technology."

Unfortunately, developers and security professionals follow different processes that don't always align. What works for one group may not work for the other.

The solution

It's better to facilitate communications between the two groups rather than try to have one adopt the processes or technologies of the other. 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, follow its own processes, and use its own tools

Trellix Cloudvisory facilitates better communication between development, deployment, and security teams.

- Predeployment teams can keep their existing processes while leveraging knowledge from security teams, 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 predeployment, quality assurance, and 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 group of security professionals to scale their influence by pushing their knowledge to the edge of the enterprise in a useful way, which helps translate security policy into the languages of developers and machines.

To learn more about Trellix, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

Trellix

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.