CLOUD SECURITY:
FIREEYE + VERODIN

Remove assumptions. Prove security.

FireEye has acquired Verodin, a security instrumentation platform that continuously measures, tests, and improves cyber security effectiveness across hybrid and multi-cloud environments.

The integration of the Verodin Security Instrumentation Platform with FireEye intelligence and expertise will enhance FireEye's ability to relentlessly protect our customers. Equipped with FireEye's leading expertise and frontline intelligence, the Verodin Security Instrumentation Platform can test your security environments against both known and newly discovered threats. This proactive, repeatable and measurable approach can enable you to identify risks in your security controls before a breach occurs and orchestrate the processes needed to optimize their defense.

WHY SECURITY INSTRUMENTATION FOR CLOUD

When people think about security instrumentation, they often think about measuring, managing, communicating and improving traditional network, endpoint and email security controls. But **most security issues—cloud and otherwise—happen because organizations do not continuously validate that security controls, segmentation, and other functions are operating as we assume they are.**

Cloud security instrumentation allows you to continuously monitor environmental drift and ensure that firewalls, web application firewalls (WAFs), intrusion prevention systems (IPS), data loss prevention (DLP), endpoint and related security controls are working as expected in all directions. Security instrumentation also evaluates network segmentation to continuously measure connectivity, directionality and other variables that often lead to compromises in flat, virtual cloud environments.

FIREEYE + VERODIN FOR AWS

The Verodin Security Instrumentation Platform is architected with a Director and Actors. The Director is a security effectiveness brain that allows you to operate the Actors and integrates with your security management stack including SIEMs, firewall manages, IPS managers, DLP managers, and endpoint security managers to deliver evidence-based reporting on how exactly your security tools respond to behavioral tests.

It also provides perspective analytics on how to better configure your security tools (rules, signatures, etc.), and gives you with a mechanism to automate the security tool validation process. The actors perform tests on the IT production environment to validate and assess control effectiveness.

In the case of cloud security, Actors are engineered to be deployed inside and outside of the AWS Cloud, enabling bidirectional communication for test behaviors.

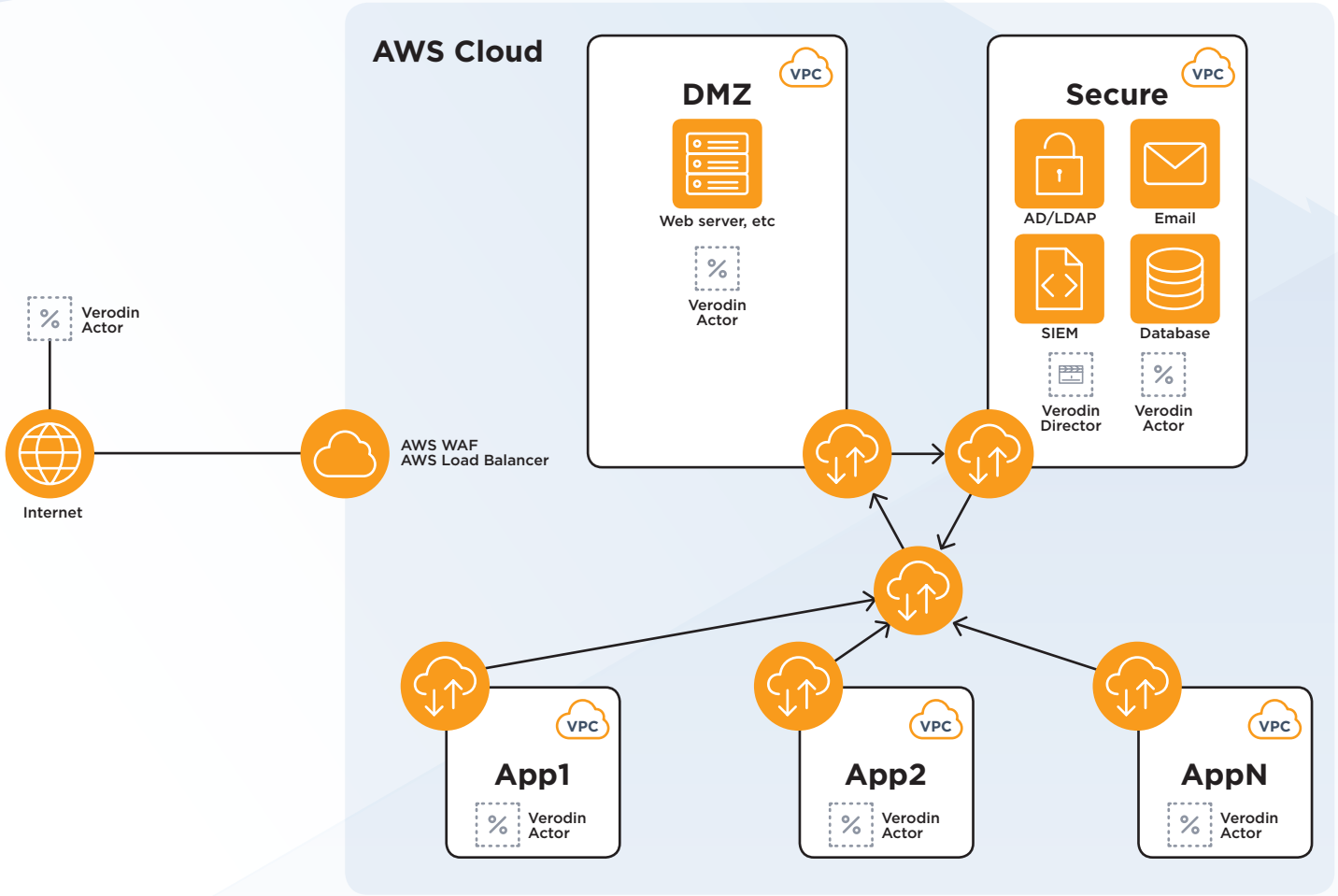
THE TEST BEHAVIORS HELP TO VALIDATE:

- North-south and east-west traffic around your cybersecurity tools
- Network segmentation
- Endpoint security
- Security effectiveness in the face of inbound attacks, data leakage, privilege escalation and other threats

Actors only communicate with each other, ensuring a safe approach to validating security tools that can operate within your production AWS environment.

The key to improving security in the cloud is continuous environmental drift validation—continuous validation that changes in any of the cloud network layers and/or security controls don't have any unforeseen and negative impacts on security.

By applying continuous environmental drift validation, you can validate the traffic paths, ensure that inspection and policy enforcement is happening, confirm that public and private layers stay separate and ensure your data is protected.



To learn more about our cloud security solutions, visit: **www.FireEye.com**