SOLUTION BRIEF

Threat Simulator

A Component of Keysight's Breach Defense Solution

Get Ahead of Attacks and Continuously Optimize Your Cybersecurity

Enterprise IT staff face a constant barrage of threats, both intentional and accidental. But simply buying and plugging in a new security device doesn't make problems magically disappear. The reality is, IT security is a process, not a destination—maintaining optimum security takes a constant investment in time and resources to get the most out of the technology and deployed products.

You can't manage what you can't measure, and security effectiveness is notoriously difficult to measure. How do you know if your network is safe? If your security products are configured correctly? If you're making the right investments? How do you justify the need for a new device?

50% of companies were breached because their cybersecurity solution was not working as expected.[1]

Be a Hero, Not a Headline

To measure and improve your security effectiveness, Keysight now applies its real-world cybersecurity experience to production networks. The new Threat Simulator is an element of the Breach Defense product family that automatically scans your perimeter defenses, web application firewall (WAF), and web policy engines to identify any vulnerabilities. Using a patented Recommendation Engine, detailed instructions on how to better configure your products to close those gaps are given in clear, easy-to-follow instructions.

Red Helix

KEYSIGHT TECHNOLOGIES

For simplified deployment and cost-effectiveness, Threat Simulator is a pure software solution with software-as-a-service (SaaS) management. An intuitive dashboard shows vulnerabilities, audit status, and security measurement over time. Run assessments on a fixed schedule or automatically when a change is detected (security policy, new malware release, etc.). You'll see which attacks you're vulnerable to and how to address them, and what steps to take if your existing solutions can't block them.

Alarmingly, 65% of companies do not verify that their security solutions are defending correctly.[1]

How It Works

Your network is completely safe. Threat Simulator never interacts with your production servers or endpoints. Instead, it uses isolated software endpoints across your network to safely exercise your live security defenses. Keysight's Dark Cloud, our malware and attack simulator, connects to these endpoints to test your security infrastructure by emulating the entire cyberattack kill chain—phishing, user behavior, malware transmission, infection, command & control, and lateral movement. In addition, Threat Simulator can validate protection of your AWS-deployed services. It also performs policy testing for different types of networks (gambling, shopping, and so forth).

Threat Simulator analyzes the detection and blocking capabilities of your entire security array, quantifies your exposure to specific threat vectors, and shows attacks that got through and how to fix the problems based on your particular firewall.

1. Keysight Security Scrimmage Survey, November, 2019

Learn more at: www.redhelix.co.uk

For more information on Keysight Technologies' products, applications or services, please contact **Red Helix**

Red Helix

KEYSIGHT TECHNOLOGIES