Breach Defense: Keysight SecOps Tools
Breach and Attack Simulation | Threat Intelligence Gateway

Your Best Defense is a Good Offense

Enterprise networks are under constant threat. New technologies, evolving attack vectors, compliance requirements, alert fatigue, vendor updates, and security skills shortages are key impediments. Security is never static, and constant change demands continuous validation. However, nearly two in three companies are concerned about their defenses. Sixty-three percent are not confident their security tools are properly configured.¹

Experiencing a breach is no longer a question of “if” — it’s a question of “when.” You need to test your production network’s readiness against the latest threats, but that has often involved considerable risk — until now.

 Fight Back Against Attackers with Keysight SecOps Tools

Don’t wait for attackers to exploit your network — meet them head-on with a virtual red team that continuously verifies, validates, and fortifies your network’s security. With Breach Defense, you can:

• Probe for vulnerabilities in your production network.
• Emulate real-world attacks without compromising your applications.

¹ Keysight Security Survey, February 2020

Nearly two in three companies are concerned about their defenses. Sixty-three percent are not confident their security tools are properly configured.
• Remediate gaps quickly with easy, step-by-step instructions.
• Measure your security effectiveness, assess whether you need additional tools, and identify potential redundancy and overspend.
• Stay ahead of attackers with a continuously-updated threat intelligence feed.
• Reduce SecOps alert fatigue and your network’s attack surface by blocking up to 80% of malicious traffic at the source.

**Threat Simulator: Validate Your Tools with Breach and Attack Simulation**

Simply buying and plugging in a new security device is not going to resolve your cybersecurity challenges instantly. Attackers are cunning, misconfigurations are rampant, and new threats continue to emerge. You don’t need another defensive tool — you need to know how effective the tools you already have actually are.

Building on more than 20 years of leadership in network security testing, Keysight Threat Simulator enables you to continuously measure and validate your security posture by simulating thousands of real-world attacks on your production network.

A series of isolated software endpoints and an intuitive GUI enables you to conduct automated assessments with maximum confidence and minimal risk. By emulating the entire cyberattack kill chain — phishing, user behavior, malware transmission, infection, command and control, and lateral movement — you can continuously measure the effectiveness of your security tools.

Knowledge is power, and with Threat Simulator, you will always be a step ahead of threats. With the ability to run continuous, automated assessments, you will be aware of potential vulnerabilities. When you identify gaps, our patented recommendation engine enables rapid remediation — giving you product-specific, step-by-step instructions to optimize your tools and fortify your network’s defenses.
ThreatARMOR: Reduce Your Attack Surface With a Threat Intelligence Gateway

Typical enterprise networks consist of a cadre of security tools, including firewalls, IPSs, antivirus, DLPs, and SIEM platforms. Hackers may be tenacious, but they are not perfect. Attacks are preventable — yet breaches remain as prevalent as ever.

So why are breaches so commonplace? The answer is simple: alert fatigue. SecOps teams work tirelessly to prevent attacks, but the sheer volume of alerts is an immense undertaking. In the face of a constant barrage of alarms, even the most vigilant security teams cannot keep up.

With bad actors frequently setting up and tearing down new IP addresses, you need a viable method to block attackers from ever entering your network. That’s why so many SecOps teams rely on Keysight ThreatARMOR to reduce their attack surface. While attackers will always find new ways to get around filters, ThreatARMOR blocks them based on their location — not their behavior.

By automatically applying our real-time threat intelligence feed to your network, ThreatARMOR enables you to reduce up to 80% of malicious and invalid traffic. Purpose-designed to eliminate traffic to and from known-bad sites without compromising performance, you can dramatically curtail SIEM alerts — keeping your SecOps team focused on what matters.
Threat Intelligence: Continuously Updated — 24/7/365

The world leader in application and security testing, Keysight’s Application and Threat Intelligence (ATI) Research Center, keeps your Breach Defense tools continuously updated with a robust database of the latest threats and exploits. With our threat intelligence feed, you can trust your team is always a step ahead. Whether that means emulating the newest attack with Threat Simulator or updating your ThreatARMOR appliance every five minutes with the latest batch of malicious IP addresses, you will always have visibility into the latest threats.

Curtailing threats means knowing your attacker. So, when you need to dive a little deeper, you can drill down on specific attacks to learn even more. From attack signatures to evidence of malicious activity, our database gives you a constant stream of actionable intelligence — 24/7/365.

Why You Win with Breach Defense

If you aren’t testing your defenses, attackers are. That’s why organizations trust Keysight, the world leader in network application and security testing, to accelerate their defenses with dynamic network intelligence.

Take control of your security and meet attackers head-on. Discover how you can validate, verify, and fortify your network with our family of Breach Defense products.

Learn more at: www.ixiacom.com/breachdefense.

Learn more at: www.keysight.com

For more information on Keysight Technologies’ products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus