Threat Simulator — Breach and Attack Simulation

Validate your tools, fix vulnerabilities, and prove your network is protected. Part of Keysight's security operations suite.

Problem: Security is Hard, Misconfigurations are Common, and Breaches are Rampant

With a multitude of emerging threats from inside and outside your network, the risk of a security breach has never been higher. All those risk factors are combined with a big human element that assumes everything has been setup and configured properly to get the best outcomes from each security tool. Organizations typically respond to this problem by throwing more money at the problem — acquiring additional security controls while increasing management complexity and complicating visibility for teams such as SecOps that are pressed to provide results and ROI.

But, the real problem behind all those things is that it has been extremely difficult to effectively measure your security posture. And when you can't measure security, it becomes harder to manage and improve it.

The result is that you can't quantify the risks to your business, or the return on your security investment, or understand how to optimize it.

KEYSIGHT

Highlights

- Part of Keysight's Security Operations Suite of enterprise security tools.
- Safe and cost-effective way to measure and validate the effectiveness of your production security tools.
- Patented recommendation engine provides clear, actionable insights on how to
- remediate identified gaps.
- Enables you to perform automated breach and attack simulations on a regular basis.
- Eliminates the assumptions that security controls are deployed and configured
- correctly.
- Identify environmental drifts from historical visualized results.
- Active validation of all phases of the Attack Life Cycle.
- Reduces compliance audit time with data- driven evidence.
- Prove security attacks are properly identified and reported.
- Justify current and future IT spending.
- Always up to date.

Solution: proactive, continuous security validation

To ensure a strong defense, organizations need to embrace an offensive approach that employ up-to-date threat intelligence to continuously verify their enterprise-wide security controls are working as expected and are optimized for maximum protection.

With Keysight's Threat Simulator, enterprises can measure their security posture, gain insights into the effectiveness of their security tools and obtain actionable remediation steps to improve it.

With this data, you can start optimizing the existing security solutions so that you can improve your security without adding another expensive security solution.

Keysight Threat Simulator™ builds on 20+ years of leadership in network security testing to reveal your security exposure across public, private, and hybrid networks. The ongoing research of our Application and Threat Intelligence team ensures regular updates so you have access to the latest breach scenarios and threat simulations.

Key features

- Multi-tenancy access control and segmentation
- Flexible, cloud-based breach and attack simulation platform that scales as your network grows.
- Actionable remediation recommendations help you improve and optimize your security controls.
- Light, container-based, infrastructure-agnostic software agents enable operations on-premises, on private and public clouds, and on remote user laptops.
- Fast insights on your security posture.
- Fully managed “Dark Cloud” infrastructure, simulating external adversaries, malicious nodes, and C&C servers in the public domain.
- Modern, web-based interface that’s easy to use.
- Built-in integration with top network security controls and SIEM tools.
- A diversified library of MITRE ATT&CK techniques and threat vectors to validate network, endpoint and email security controls.
- Out-of-the-box attack library enables you to simulate the full Cyber Kill Chain® for popular breaches, relevant software threats, and Advanced Persistent Threats (APTs).
- Scheduler enables continuous security assessments across your enterprise-wide network.
- SIEM-proxy agent facilitates communication with SIEM tools.
- Built in packet capture support.
- Visual ladder diagrams complement predefined security assessments.
- Agent tagging supporting user-provided metadata, making it easier to mange individual agents.
- Agent grouping creates abstraction layers, allowing simple and rapid validations of multiple network segments at once.

Product capabilities

When it comes to network security, your best defense is a good offense. Keysight Threat Simulator™ is a breach and attack simulation platform that provides enterprise security teams with insights into the effectiveness of their security posture and actionable intelligence to improve it.

A cloud-native, serverless design

Keysight Threat Simulator is a completely cloud-based platform, delivered as a SaaS. At its core, it is an implicit microservices architecture orchestrated via APIs. This serverless design enables Threat Simulator to auto-scale on demand — eliminating the need for complex and costly data backhauls.

Delivered as a SaaS solution, Threat Simulator eliminates common anxieties with

deployment, especially where network architectures are more complex. It offers a modern, simplified web user interface with great “out-of-the-box” experience.

Keysight Threat Simulator comprises three core components:

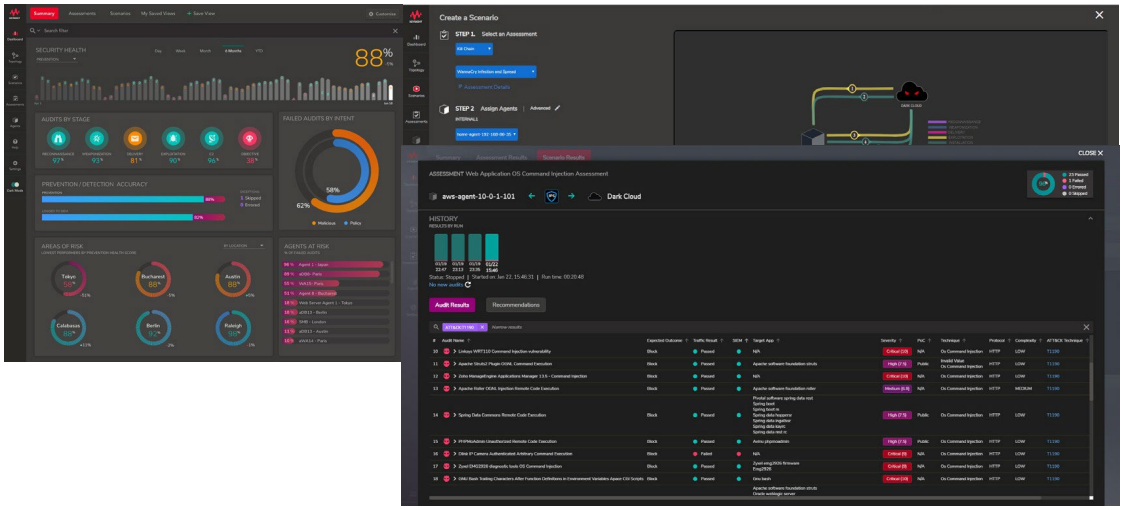
- A user-friendly web-based interface makes it easy to configure and run security assessment scenarios, identify drifts in your security posture and retrieve actionable remediations.
- A “dark cloud” entity that spins up agents on demand to simulate threat actors in the public domain (e.g.: malicious websites, external hackers, C&C).
- Agents that are deployed on your Enterprise network; available in Docker-container format, they act as simulator “targets” or “attackers” inside your network, enabling safe, yet realistic, attack and breach simulation scenarios (inside-to-outside, outside- to-inside and lateral movement).

On-prem edition

Effective data management including aspects such as data-sovereignty and data-residency has been a challenge for many organizations that may be bound by organizational or industry requirements. To satisfy these requirements, Threat Simulator offers an on-prem edition that can be hosted on supported hypervisors regardless of location or access to the internet. The on-prem edition allows the infrastructure component along with a custom on-prem version of the Dark Cloud, which can be deployed on a hypervisor running on operating systems such as VMware ESXi™ or Linux KVM. Moreover, the on-prem edition offers TACACS+ protocol support allowing seamless integration with enterprise technologies such as Microsoft Windows™ Active Directory.

Network security and enterprise tools ecosystem

Threat Simulator offers turnkey integrations with a large ecosystem of network security controls, making it easy to get specific, actionable recommendations to improve and manage your cybersecurity effectiveness. Integration with leading SIEM vendors enable end to end validation on how the prevention/detection works and identifies security sensors that may go dark. Bidirectional communication with SIEM tools provides SOC teams with push events that notify them during attack and breach simulations, enabling them to quickly distinguish simulated attacks from non-simulated ones.



Thread Simulator – Web User Interface (Dashboard, Scenario Builder, Detailed Results)

Network, Endpoint and email security assessments, powered by Threat Simulator: validate security posture, identify vulnerabilities, and prioritize fixes

Are you looking to improve security operations, but lacking the personnel to do so? We get that. When your team is constantly fighting fires, it can be hard to make time for anything else.

That's why we can offer network, endpoint and email security assessments, powered by Threat Simulator. Whether you're looking for recurring monthly assessments or a one-time engagement, our trained professionals can give you a detailed analysis of your security posture without the hassle and complexity of adding another tool to your stack. We can safely simulate attacks on your production network, reveal vulnerable misconfigurations, and give you specific, step-by-step instructions to remediate and prioritize fixes.

Our standard assessment covers the entirety of your defensive deployment, and covers network, endpoint, and email security controls. However, you can also choose from a variety of tailored audits to drill down on specific focus areas, such as the following:

- branch security
- email security
- endpoint security
- MITRE ATT&CK groups
- APT campaigns
- WAF security

No matter what you choose, our assessments are quick and cost-effective — complete with personalized reports and remediation guidelines. With our team’s detailed analysis, you gain actionable insight into the flaws a malicious actor is likely to exploit, enabling you to immediately implement fixes to protect your network, users, and applications.

Specifications

Feature category	Feature
General features	• SaaS-based validation platform using safe attack and breach modeling that scales as your network grow • On-prem edition supported on VMWare ESXi™ and Linux KVM hypervisors • Modern, easy to use, web-based user interface • Actionable remediation recommendations help you improve and optimize your security controls • Prevention health score with historical trending to identify drift • Detection/Alerting health score with historical trending to identify drift • Distributed architecture with light software agents • Minutes to the first security insight • Built-in packet capture support • Topology viewer • Dashboards (Summary, Assessment, Scenario, Agents)
Attack and Breach Simulation	• Active validation of all phases of the Attack Life Cycle • Diversified and realistic library of techniques, threat vectors and kill chain modeling • Always safe – simulated attacks and breaches are only between Threat Simulator agents • Option to run attacks over encrypted or clear text • New security audits added every 2 weeks • Security assessment for network security controls WAF, IDS/IPS, DLP, URL Filtering, Gateway Antivirus and Malware Sandbox • Endpoint security assessments covering MITRE ATT&CK techniques and MITRE ATT&CK Groups • Email security assessments for Microsoft Office 365, IMAP, and SMTP. • Active validation of both datacenter and perimeter-based security controls • IPv4 support
Threat Simulator Agent	• Light, container-based software agents require 1 vCPU, 1 GB RAM and 8 GB disk • Available as docker-container for Linux distributions (e.g: RedHat, CentOS, Ubuntu) to run network-based and email security assessments • Available as a Windows and MacOS native applications to run endpoint, network, and email security assessments • Infrastructure agnostic allowing operations on-premise, private and public clouds • Runs on 32-bit or 64-bit x86 architectures • Flexibility to use a single interface for management/test traffic or dedicated test interfaces • Downloads and installs in < 2 min • IPv4 support
SIEM Connector Agent	• Light, container-based software requires 1 vCPU, 1 GB RAM, and 8 GB disk space. • Runs on 32-bit or 64-bit x86 architectures

Feature category	Feature
	• Downloads and installs in minutes • Acts as a proxy between the Threat Simulator SaaS backend and the SIEM tool • IPv4 connectivity
SIEM Integrations	• IBM QRadar (Network assessments) • Splunk (Network and Endpoint assessments) • LogZ.io (Network assessments)
Endpoint Integrations	• CrowdStrike Falcon EDR events • SentinelOne Singularity threats • Trellix ePolicy Orchestrator (On-prem edition) • Generic vendor support

Ordering info (SaaS edition)

Part number	Description
983-2010	Threat Simulator BASE bundle (5 agents, 1-year subscription) All-inclusive networking security assessment bundle includes: • Access to the Threat Simulator SaaS web console • Up to 5 software agents deployed on customer's network perimeter • Dark Cloud simulation hosted on Keysight's managed infrastructure • All network-based security assessments Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).
983-2011	Threat Simulator BASIC bundle (10 agents, 1-year subscription) • All-inclusive networking security assessment bundle includes: • Access to the Threat Simulator SaaS web console • Up to 10 software agents deployed on customer's network perimeter • Dark Cloud simulation hosted on Keysight's managed infrastructure • All network-based security assessments Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).
983-2012	Threat Simulator STANDARD bundle (25 agents, 1-year subscription) All-inclusive networking security assessment bundle includes: • Access to the Threat Simulator SaaS web console • Up to 25 software agents deployed on customer's network perimeter • Dark Cloud simulation hosted on Keysight's managed infrastructure • All network-based security assessments Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year)."

Part number	Description
983-2013	Threat Simulator PLUS bundle (50 agents, 1-year subscription) All-inclusive networking security assessment bundle includes: • Access to the Threat Simulator SaaS web console • Up to 50 software agents deployed on customer's network perimeter • Dark Cloud simulation hosted on Keysight's managed infrastructure • All network-based security assessments Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).
983-2014	Threat Simulator PREMIUM bundle (100 agents, 1-year subscription) All-inclusive networking security assessment bundle includes: • Access to the Threat Simulator SaaS web console • Up to 100 software agents deployed on customer's network perimeter • Dark Cloud simulation hosted on Keysight's managed infrastructure • All network-based security assessments Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).
983-2019	Simulator Optional Endpoint Security add-on (1-year subscription, SaaS) The endpoint security assessment add-on provides access to all endpoint security assessments for the active duration of the subscription. Requires previous purchase of a Threat Simulator agent bundle (983-2010, 983-2011, 983-2012, 983-2013, 983-2014 or 983-2015). Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).
983-2020	Threat Simulator Optional Email Security add-on (1-year subscription, SaaS) The email security assessment add-on enables all-inclusive access to all email security assessments for the active duration of the subscription. Requires previous purchase of a Threat Simulator agent bundle (983-2010, 983-2011, 983-2012, 983-2013, 983-2014 or 983-2015). Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).

Ordering info (On-prem edition)

Part number	Description
983-2110	Threat Simulator On-Premise (5 agents, 1-year subscription) All-inclusive security assessment bundle includes: • Access to the Threat Simulator and Dark Cloud OVA images • Up to 5 software agents deployed on customer's network perimeter • Dark Cloud simulation available as a virtual machine image • All network, endpoint, and email-based security assessments Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).
983-2111	Threat Simulator On-Premise (10 agents, 1-year subscription) All-inclusive security assessment bundle includes: • Access to the Threat Simulator and Dark Cloud OVA images • Up to 10 software agents deployed on customer's network perimeter • Dark Cloud simulation available as a virtual machine image • All network, endpoint, and email-based security assessments Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).

Part number	Description
983-2112	Threat Simulator On-Premise (25 agents, 1-year subscription) All-inclusive security assessment bundle includes: • Access to the Threat Simulator and Dark Cloud OVA images • Up to 25 software agents deployed on customer's network perimeter • Dark Cloud simulation available as a virtual machine image • All network, endpoint, and email-based security assessments Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).
983-2113	Threat Simulator On-Premise (50 agents, 1-year subscription) All-inclusive security assessment bundle includes: • Access to the Threat Simulator and Dark Cloud OVA images • Up to 50 software agents deployed on customer's network perimeter • Dark Cloud simulation available as a virtual machine image • All network, endpoint, and email-based security assessments Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).
983-2114	Threat Simulator On-Premise (100 agents, 1-year subscription) All-inclusive security assessment bundle includes: • Access to the Threat Simulator and Dark Cloud OVA images • Up to 100 software agents deployed on customer's network perimeter • Dark Cloud simulation available as a virtual machine image • All network, endpoint, and email-based security assessments Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).
983-2115	Threat Simulator On-Premise (1 agent, 1-year subscription) All-inclusive security assessment bundle includes: • Access to the Threat Simulator and Dark Cloud OVA images • Up to 1 software agent deployed on customer's network perimeter • Dark Cloud simulation available as a virtual machine image • All network, endpoint, and email-based security assessments Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).

Part number	Description
983-2131	Threat Simulator On-Premise MSSP Single-Agent License (1 agent, 1-year subscription) All-inclusive security assessment bundle includes: • Access to the Threat Simulator and Dark Cloud OVA images • Up to 1 software agent deployed on customer's network perimeter • Dark Cloud simulation available as a virtual machine image • All network, endpoint, and email-based security assessments Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).
983-2133	Threat Simulator On-Premise MSSP Single-Agent License w/Enterprise 24x7 support (1 agent, 1-year subscription) All-inclusive security assessment bundle includes: • Access to the Threat Simulator and Dark Cloud OVA images • Up to 1 software agent deployed on customer's network perimeter • Dark Cloud simulation available as a virtual machine image • All network, endpoint, and email-based security assessments • Enterprise 24x7 support Requires license term to be specified (must be purchased in multiples of years, the list price is per unit per year).