TRAPX SECURITY

Data Sheet

DeceptionGrid™ 7.1

The threat landscape has permanently changed. The New Normal, with a large remote workforce and distributed assets, has pushed security teams into a new reality of surface area expansion, blind spots and risk exposure. Concerns about lateral movement visibility and the disparity between attack and response velocity remain a serious concern. Traditional monitoring and controls simply do not fit in this paradigm as they leave more devices, systems and processes exposed, and more risk unaddressed.

Recent attacks have achieved a next-level of stealth, executing in a way that is invisible to the most robust conventional security technology. What worked before no longer works. It is time for a new approach in Cybersecurity. It is time to deploy Active Defense — strategy, tactics and countermeasures to counter attacks and get ahead of the adversary.

TrapX DeceptionGrid 7.1 is the industry's first software platform that activates Active Defense to enable security teams to proactively plan, deploy, test and refine Deception deployments against attack scenarios outlined in MITRE ATT&CK.

- Patented emulation technology delivers both comprehensive protection and full visibility at scale. Hundreds of authentic traps, which can be deployed in just minutes, hide real assets and dramatically decrease risk.
- New lures and traps enable Endpoint Fitness audit capabilities that assess the state of remote worker endpoints. Patch levels, protection and connections are all visualized through an intuitive summary dashboard and heatmap.
- High-fidelity alerts supply MITRE ATT&CK context to facilitate Active Defense planning and incident response.
- TrapX Active Defense Scorecard (ADS) provides real-time intelligence and visualization of defense coverage to fine-tune tactics for continuous, adaptable protection.

Active Defense is the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy. Backed by more than 10 years of adversary engagement experience MITRE introduced Shield, a knowledgebase of tactics and techniques that help you to counter current attacks while you learn about your adversary to prepare for the future.

USE CASES

- Ransomware
- Man-in-the-Middle Attacks
- Credential Theft
- AD Reconnaissance Attacks
- Lateral Movement
- IT/OT/IoT Security
- Insider Threats

A Unified Platform for Active Defense Flexibility

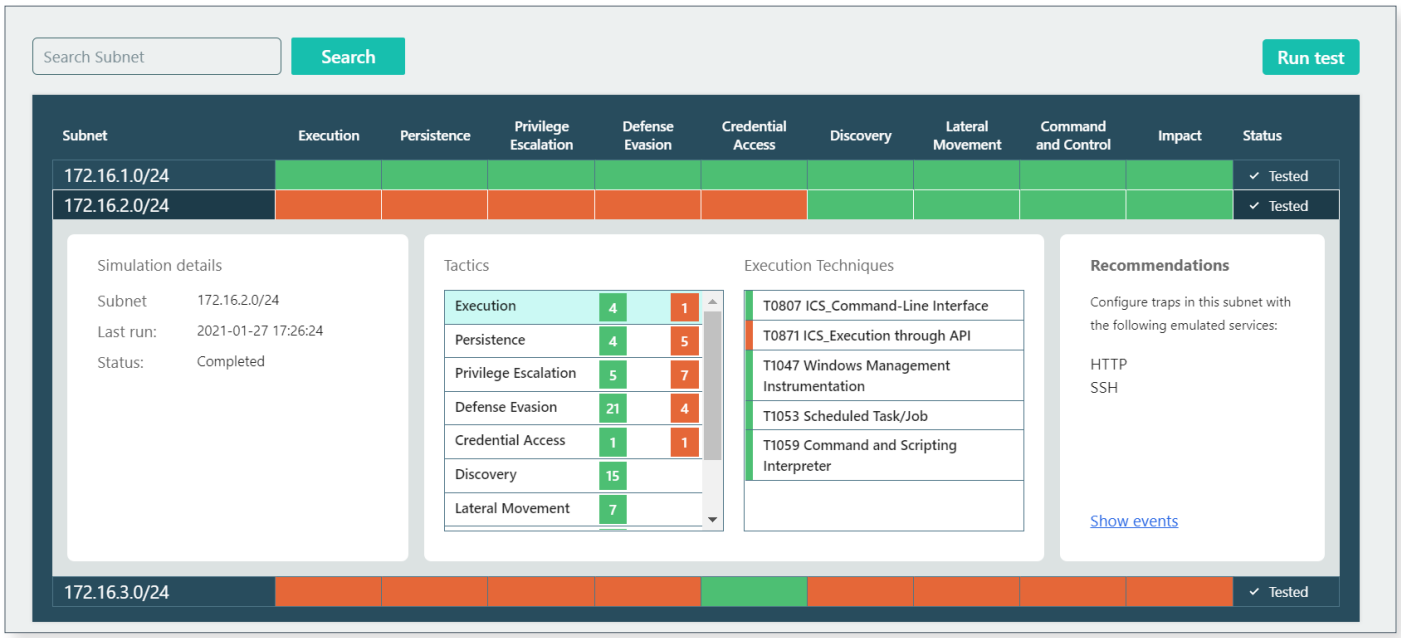
TrapX DeceptionGrid™ 7.1 fills a vital gap in layered cybersecurity. It is a light, fast and transparent solution that covers the entire surface area and disrupts attacks in the network, independent of the state or nature of the endpoint. DeceptionGrid hides real assets in a crowd of imposters that interact with attackers and misinform them in exchange for insight into their TTPs, allowing for rapid response and containment. In just minutes, TrapX's patented emulation technology launches hundreds of authentic traps that engage attackers and malware and generate high-fidelity alerts for rapid response. With coverage of nearly 100 MITRE Techniques, the ability to test trap efficacy against these techniques in real time, as well as the capability to map alerts to MITRE ATT&CK to aid in investigation, TrapX DeceptionGrid 7.1 provides the power to deploy Active Defense.

Our emulated traps can be enriched with high interaction traps and lures to provide an end-to-end solution from a single platform for complete Active Defense flexibility. You might lead by scattering traps that cover and protect critical assets. Then lure attackers toward traps. Then strategically use high interaction traps to gather intelligence on the attacker. All while testing and visualizing your defense coverage and adjusting as needed, in real-time.

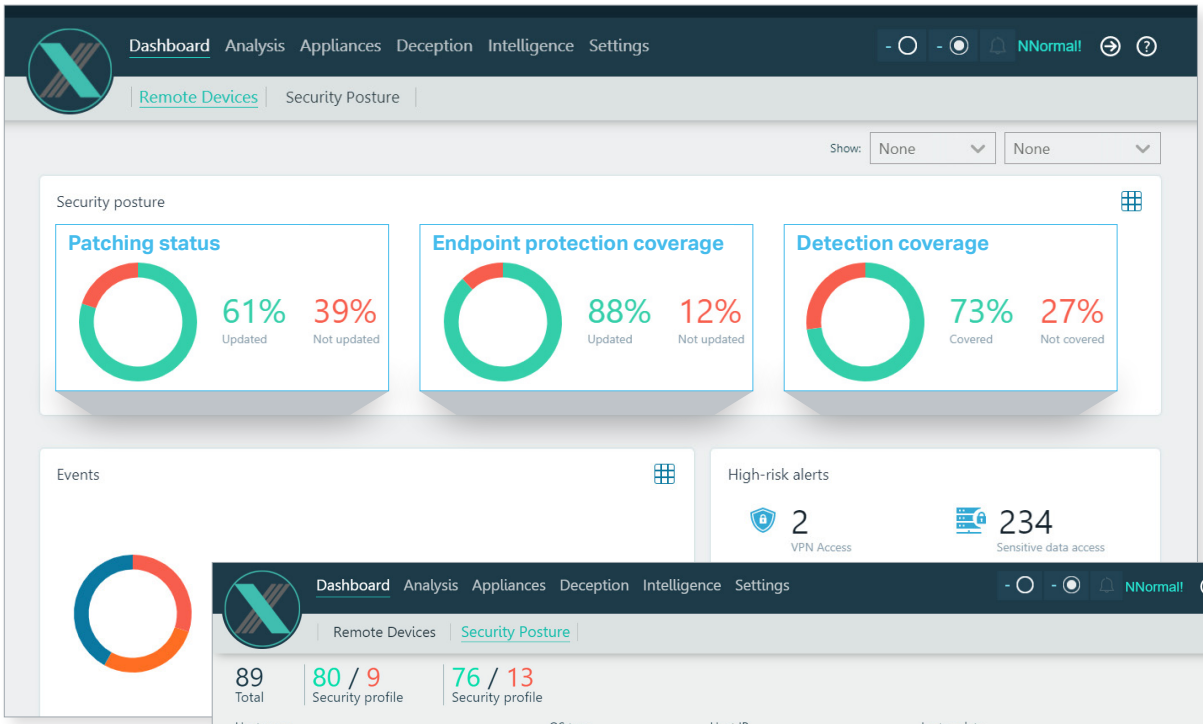
Unlike anything else on the market, our lightweight, touch-less technology offers non-disruptive support for a broad array of systems and devices, including IT, OT, IoT, SCADA, ICS, and SWIFT.

TRAPX DECEPTIONGRID 7.1 ACTIVE DEFENSE	
Endpoint Fitness	Fast, lightweight audit that assesses the state of Deception landscape, including remote worker endpoints. Patch levels, protection and connections are all visualized through an intuitive summary dashboard and heatmap.
Agentless Endpoint Lures	A rich variety of deceptive data, including credentials, files, browser history and more, coax the attacker away from real assets and into emulated traps.
Cloud, Network and Corporate Traps	Lures direct attacker to emulated network system and device traps. Attackers waste their time exchanging insight into their TTPs in exchange for fake information.
On-Prem or Hosted Security Console (TSOC)	Central management of Deception environment: scan, deploy and adapt in minutes. Attack Visualization displays alert signals and attack intelligence, giving Security Operations valuable visibility into malicious activity.
TrapX Active Defense Scorecard (ADS)	Non-disruptive Deception environment testing against ATT&CK Techniques and Sub-techniques enabling visualization of trap coverage through a real-time heatmap. Coupled with TrapX scanning and rapid deployment, ADS provides the unique ability to discover assets, deploy, test, and redeploy traps with minimal disruption.

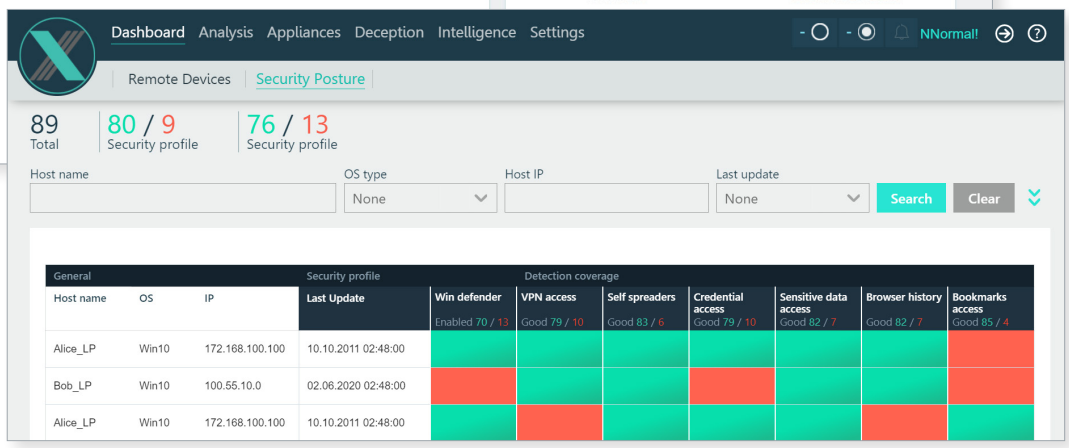
TrapX Console Dashboard



Active Defense Scorecard



Endpoint Fitness



The DeceptionGrid 7.1 Advantage for Active Defense

End-to-End Protection & Visibility

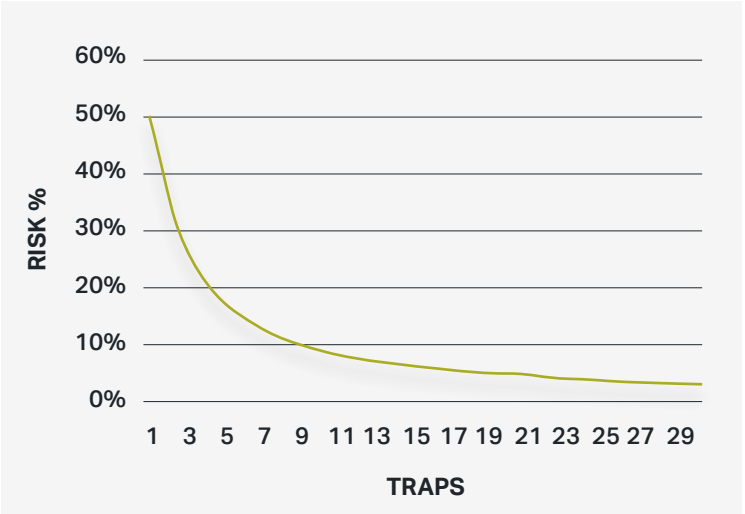
DeceptionGrid 7.1 provides Security Operations teams end-to-end visibility of distributed devices and networks.

- Diverts attacks from critical assets
- End-to-end visibility — from endpoint and network to Cloud and/or on-prem environments
- Test and validate against MITRE ATT&CK techniques
- Protects corporate assets from the risk of unmanaged devices or networks

Deception in Depth: More Traps = Less Risk

TrapX populates the attack surface with traps, hiding real assets and forcing attacker into a guessing game. Easy to deploy traps dramatically reduce risk.

- One critical asset joined by one trap reduces exposure by 50%; two traps by 66%; three by 75%, and so on
- Lightweight traps do not consume resources, touch assets, or collect data
- Fast activation of traps is much faster than remediation



MITRE ATT&CK Integration

TrapX provide MITRE ATT&CK context to high-fidelity alerts. Traps expose Techniques and Sub-techniques active within network. Lateral movement insight can be traced back to attack groups for an aligned Active Defense strategy.

- Coverage of nearly 100 MITRE Techniques
- Ability to test trap efficacy against MITRE techniques in real time
- Capability to map alerts to MITRE ATT&CK to aid in investigation

TrapX Security, Inc.
303 Wyman Street
Suite 300
Waltham, MA 02451

+1–855–249–4453
www.trapx.com

sales@trapx.com
partners@trapx.com
support@trapx.com

About TrapX Security

TrapX has created a new generation of Deception technology that provides real-time breach detection and prevention. Our proven solution immerses real IT assets in a virtual minefield of traps that misinform and misdirect would-be attackers, alerting SOC teams to malicious activity with actionable intelligence immediately. Our solutions enable our customers to rapidly isolate, fingerprint and disable new Zero Day attacks and APTs in real-time. TrapX Security has thousands of government and Global 2000 users around the world, servicing customers in manufacturing, defense, healthcare, finance, energy, consumer products and other key industries. For more information, visit **www.trapx.com**.