TRAPX SECURITY | Check Point SOFTWARE TECHNOLOGIES LTD.

Solution Brief

TrapX DeceptionGrid™ + Check Point®

Deception Technology Finds Sophisticated Attackers That May Already Be Inside Your Network

Insights

TrapX Security and CheckPoint have joined forces to provide real-time visibility, threat detection, and rapid threat containment for both internal networks and cloud deployments. The DeceptionGrid and CheckPoint joint solution enables early detection of targeted attacks and sophisticated threat actors operating inside networks, including networks with a broad diversity of devices to include Internet of Things (IoT) devices and embedded processors. Together we provide the agility needed to isolate compromised assets and stop attackers in near real-time.

Joint Solution

TrapX Security and CheckPoint have integrated TrapX's powerful DeceptionGrid technology into CheckPoint's firewall.

DeceptionGrid is based on the TrapX architecture, which combines wide-ranging Deception capabilities to bait, engage, and trap attackers. DeceptionGrid's multi-tier architecture presents Deception attack surfaces that match attacker activity adaptively, creating a tempting environment for attackers within the network.

Once an attacker is identified by DeceptionGrid, CheckPoint processes this enhanced threat intelligence and instantly applies this security insight to trigger an automated response to drop the connection. This response action is confidently triggered by high-fidelity DeceptionGrid alerts.

Unlike conventional security methods which generate alerts based on probabilities and known threats, DeceptionGrid alerts are binary — attackers either attempt to engage a trap or they don't. If they do, we know with nearly 100 percent confidence that it's an attack.

In large enterprises, building a motivated security operations center (SOC) team is essential. Yet security operations team morale is worn down by constant alert fatigue due to the thousands and, in some cases, millions of alerts daily. This raises triage costs, reduces team effectiveness, and makes it difficult to retain and build a motivated team. The sheer volume of alerts also makes it extremely difficult to identify real attackers.

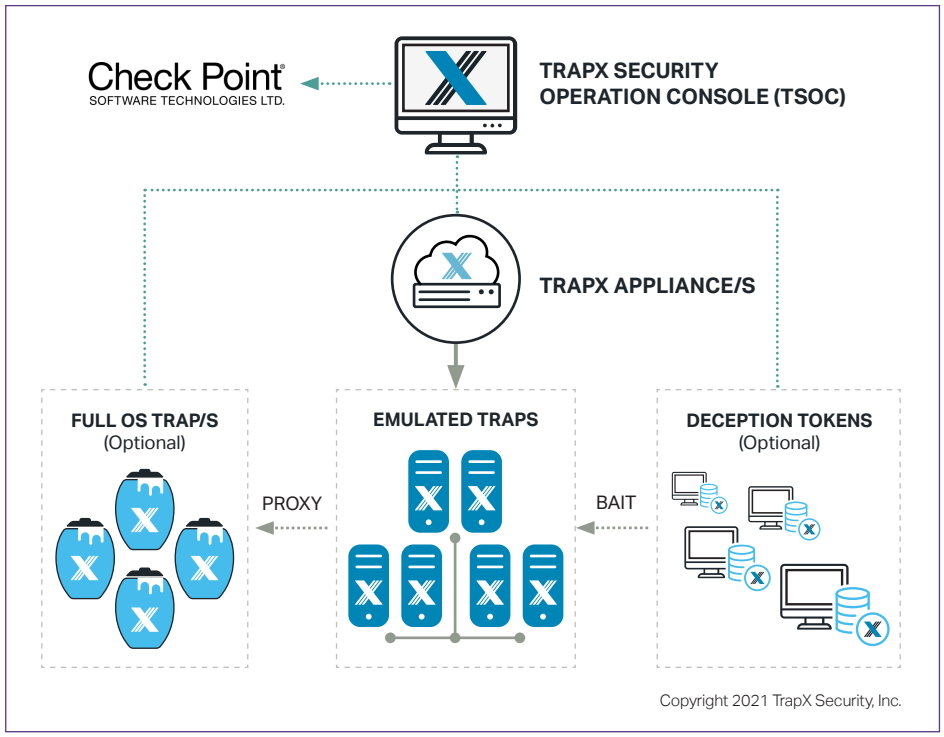
Product Benefits

- Detects the new breed of cyber attackers
- Reduced time-to-breach detection
- Reduces or eliminates economic losses
- Improves compliance
- Lowest cost of implementation
- Compatible with existing investments

Product Features

- Powerful situational awareness
- High fidelity alerts
- Deep visibility
- Actionable intelligence
- Deception tokens (lures)
- Emulated traps

TrapX DeceptionGrid™



DeceptionGrid baits attackers by deploying automated, camouflaged Deception tokens (lures) and medium- and high-interaction traps (decoys) among authentic IT assets. The traps appear identical in every way to authentic IT assets and connected Internet of Things (IoT) devices. The attacker may see an array of camouflaged traps which appear as tempting medical devices, servers, automated teller machines, retail point of sale workstations, switches, industrial control system components, and many other devices. DeceptionGrid even maintains a facade of convincing network traffic among the traps, thereby enhancing the illusion of authenticity and further engaging sophisticated attackers.

Once an attacker has penetrated a network in which DeceptionGrid has been deployed, they're faced with immediate identification at every turn. Just one touch of a DeceptionGrid trap sets off a high-confidence alert. DeceptionGrid integrates with CheckPoint® to contain the attack and enable a return to normal operations.

DeceptionGrid Differentiation

No more alert-fatigue. A TrapX alert is more than 99% accurate and immediately actionable.

Complete automated forensic analysis of captured malware and attacker tools.

Smart Auto-Pilot automates deployment of thousands of DeceptionGrid traps for the largest enterprise.

Powerful emulation technology deploys traps camouflaged as industry-specific devices, including medical devices, ATMs, point-of-sale terminals, Internet of things (IoT) devices, and much more.

DeceptionGrid architecture integrates the benefits of tokens, emulated traps, FullOS traps, and our Active Networks feature in one integrated architecture for more rapid detection, deep attacker engagement, and comprehensive threat containment.

Comprehensive partner integrations create end-to-end workflows from detection to remediation and increase value from existing ecosystem investments.

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 Security is a pioneer and global leader in cyber Deception technology TrapX DeceptionGrid rapidly detects, deceives, and defeats advanced real-time cyber-attacks and human attackers in real-time. The DeceptionGrid provides automated, highly accurate insight into malicious activity unseen by other forms of cybersecurity. By deploying DeceptionGrid, users can create proactive security to fundamentally halt the progression of an attack. This strategy shifts the economics of cyberattacks to cost the attacker instead of the victim. TrapX Research Labs clients include several Forbes Fortune 500 commercial and government customers worldwide. Sectors include defense, healthcare, finance, energy, consumer products, and other key industries. Learn more about this cybersecurity solution at **www.trapx.com**.