CHECK POINT + TRAPX
DECEPTIONGRID

Deception Technology

Finds sophisticated attackers that may already be inside your network.

Product Benefits

- Detects the new breed of cyberattackers.
- 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

INSIGHTS

TrapX Security and Check Point® have joined forces to provide real-time visibility, threat detection, and rapid threat containment for both internal networks and cloud deployments. The TrapX DeceptionGrid and Check Point 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

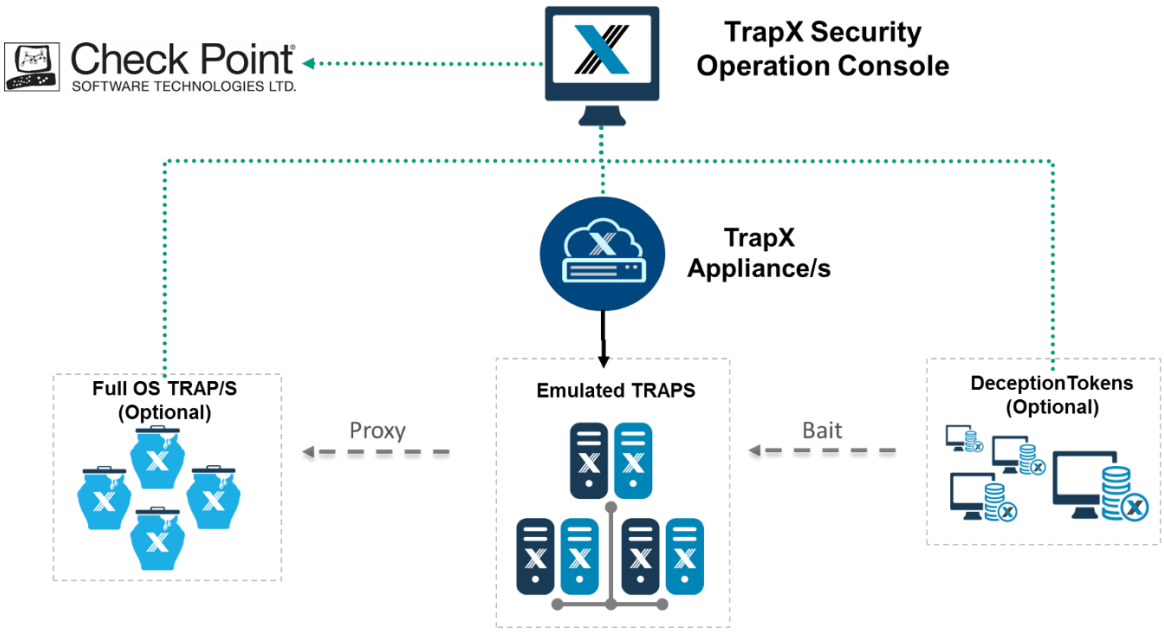
DeceptionGrid is based on TrapX architecture, which combines wide-ranging deception capabilities to bait, engage, and trap attackers. DeceptionGrid's multi-tier architecture presents deception attack surfaces that match attacker activity adaptively, creating a tempting environment for attackers within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

Once an attacker is identified by DeceptionGrid, its IP address information is sent to Check Point Security Gateways 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 team is essential. Yet security operations team morale is worn down by constant alert fatigue due to the thousands and, in some cases, even 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 find attackers.

TRAPX DECEPTIONGRID



DeceptionGrid baits attackers by deploying automated, camouflaged deception Tokens (lures) and medium- and high-interaction Traps (decoys) among authentic IT resources. 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 the DeceptionGrid 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 capture malware and attacker tools.

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

» Provides everything needed for security operations centers to act rapidly in response to a threat.

» Powerful emulation technology enables camouflaging traps 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.