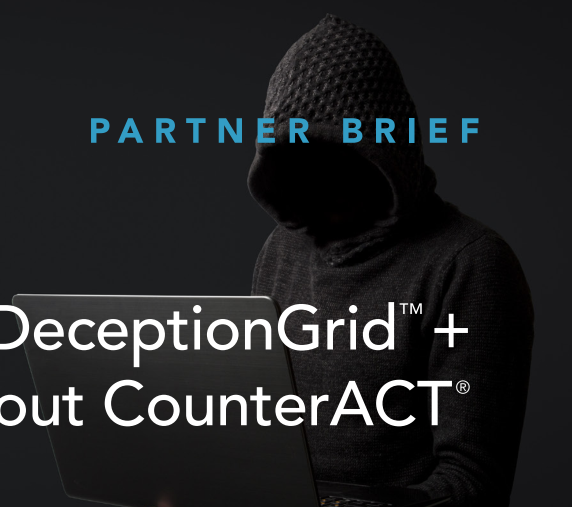
PARTNER BRIEF



ACTIVE DEFENSE

TrapX DeceptionGrid™ + ForeScout CounterACT®

TrapX Security and ForeScout® Technologies have joined forces to provide real-time visibility and threat detection, improved incident response, and rapid threat containment leveraging the capabilities of ForeScout solutions. The TrapX DeceptionGrid and ForeScout CounterACT joint solution enables early detection of targeted attacks and sophisticated threat actors operating inside networks, along with the agility needed to isolate compromised assets and stop attackers in near real-time.

The Challenge

Advanced threat actors employ sophisticated techniques to penetrate even the most robust network defenses. The question isn't whether attackers will penetrate your networks, but when and how often. Attackers can operate undetected for many months, which can ultimately spell disaster for the targeted network.

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. All of this raises triage costs, reduces team effectiveness and makes it difficult to retain and build a successful team. The sheer volume of alerts also makes it extremely difficult to find attackers. Which alert is the important one? Which alert did we miss? Unfortunately, just one successful penetration can compromise an entire network unless the attacker is rapidly identified, quarantined, and stopped.

Joint Solution

TrapX Security and ForeScout have integrated TrapX's powerful DeceptionGrid technology into ForeScout CounterACT, an agentless visibility and control appliance that dynamically identifies and evaluates network endpoints and applications the instant they connect to your network. 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.

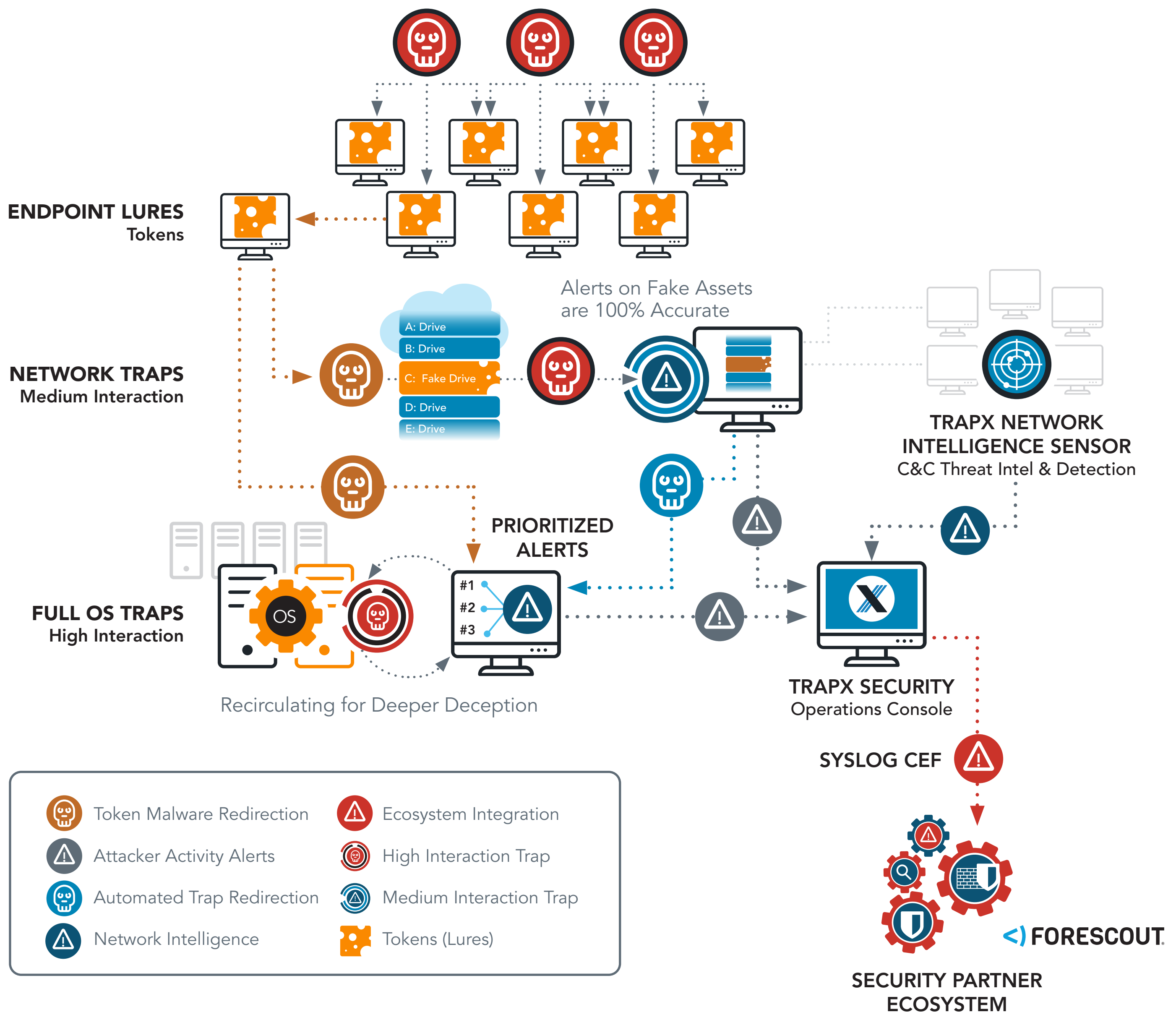
If they do, you'll know with nearly 100 percent confidence that it's an attack. Once an attacker is identified by DeceptionGrid, CounterACT processes this enhanced threat intelligence and instantly applies this security insight to trigger an automated response and enforce its broad range of policy-based controls, such as isolating the device and remediating the endpoint to eliminate threats. This response action can be initiated by a SOC analyst directly, or can be implemented via policy-based automation triggered by DeceptionGrid's high-fidelity alerts.

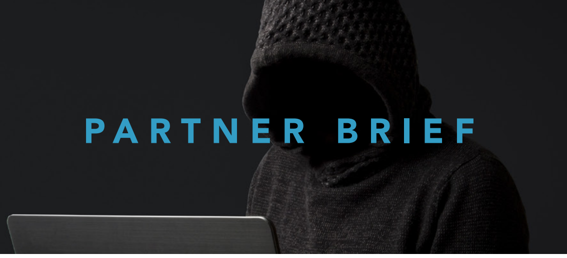
How will you know if an attacker has penetrated your network?

How quickly will you know that your current security protections have failed?

How quickly can you isolate and shut down the attack and return to normal operations?

TRAPXSECURITY DECEPTIONGRID™ ARCHITECTURE





TrapX DeceptionGrid

DeceptionGrid is based on TrapX's Deception-in-Depth 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.

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 your authentic IT assets and connected Internet of Things (IoT) devices. The attacker sees 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 more. DeceptionGrid even maintains a facade of convincing network traffic among the traps, thereby enhancing the illusion of authenticity and further engaging sophisticated attackers.

DeceptionGrid Architecture

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 by the attacker sets off a high-confidence alert. Then DeceptionGrid integrates with key elements of the network and CounterACT to contain the attack and enable a rapid return to normal operations.

Benefits

- **Reduced time-to-breach detection**—DeceptionGrid detects malware and human threat actor movements inside the perimeter immediately.
- **Powerful situational awareness**—DeceptionGrid detects lateral movements that are often missed by other types of cyber tools and defenses.
- **Highest-fidelity alerts**—DeceptionGrid generates a very low volume of highly accurate alerts.
- **Deception-in-Depth integrated product platform**—Deception-in-Depth brings the industry's most powerful and comprehensive suite of Deception techniques together in one multi-tier architecture to bait, engage, and trap attackers.
- **Ease-of-deployment**—DeceptionGrid deployment is simple and fast, using our proprietary emulations and powerful automation.
- **Actionable intelligence**—Information flows across our integrated network to leverage discovery and uncover hidden threats that target critical assets in both IT and OT infrastructures.
- **Deep visibility into internal networks**—The DeceptionGrid/CounterACT joint solution provides augmented and actionable real-time visibility into lateral movements from attackers, targeting special turnkey systems such as IoT, SCADA, ICS, POS, and medical devices.
- **ForeScout integration**—DeceptionGrid integrates seamlessly into CounterACT for fast deployment, trouble-free administration, and automated rapid threat containment. TrapX provides MSSP partners that bring the expertise and skills needed to supplement constrained in-house teams. DeceptionGrid can also retrieve asset inventory from ForeScout CounterACT and use it for automatic trap configuration and coverage analysis, ensuring the Deception deployment mimics the organizational asset inventory.

Use Case #1

QUARANTINE SUSPECTED ENDPOINTS

Once DeceptionGrid identifies a suspicious endpoint (IP), it instructs CounterACT to isolate that endpoint from the network. This halts the attack immediately and gives your security team time to investigate the incident without risking further infection/compromise to the network.

This quarantine can be initiated by a security operations center analyst directly, or can be implemented by policy-based automation triggered by high-fidelity DeceptionGrid alerts.

Use Case #3

PROACTIVE MITIGATION

TrapX identifies indicators of compromise (IOC) based upon interaction with our emulated decoys (including IoT, SCADA, medical, ATM, and POS devices and systems). DeceptionGrid shares these IOCs (e.g., detect malware binary file hash) with CounterACT. CounterACT isolates the infected endpoint based on your policy. It leverages its IOC repository to scan other endpoints that are attempting to connect or are already connected on the network for new IOCs and initiates remediation actions.

Use Case #2

DIVERSION

Once a suspicious endpoint (IP) is identified by DeceptionGrid or any other integrated third-party solution, the information is communicated to CounterACT, which moves the endpoint to a special predefined segment (e.g., DeceptionGrid VLAN) of the network, which includes decoys.

At this point, any attempt by malware or a human attacker to move laterally from that suspicious endpoint to the decoys immediately reveals their tactics, techniques, and procedures to DeceptionGrid, which enables the security operations team to better understand and contain the threat. This enables more rapid conviction of suspect entities moving with the network before they can cause further damage and theft.

TRAPX SECURITY

TrapX Security is the pioneer and global leader in cyber deception technology. Their DeceptionGrid solution rapidly detects, deceives, and defeats advanced cyber attacks and human attackers in real-time. DeceptionGrid also provides automated, highly accurate insight into malicious activity unseen by other types of cyber defenses. By deploying DeceptionGrid, you can create a proactive security posture, fundamentally halting the progression of an attack while changing the economics of cyber attacks by shifting the cost to the attacker. The TrapX Security customer-base includes Forbes Global 2000 commercial and government customers worldwide in sectors that include defense, healthcare, finance, energy, consumer products, and other key industries. Learn more at www.trapx.com.

FORESCOUT

Forescout Technologies, Inc. (NASDAQ: FSCT) actively defends the Enterprise of Things by identifying, segmenting and enforcing compliance of every connected thing. Fortune 1000 companies trust Forescout as it provides the most widely deployed, enterprise-class platform at scale across IT, IoT, and OT managed and unmanaged devices. Forescout arms customers with more device intelligence than any other company in the world, allowing organizations across every industry to accurately classify risk, detect anomalies and quickly remediate cyberthreats without disruption of critical business assets.
Don't just see it. Secure it.

The Enterprise of Things – Secured.
Learn more at www.forescout.com.

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 you to any 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 defense, health care, finance, energy, consumer products and other key industries.