Solution Brief

TrapX™ DeceptionGrid™ + Cisco® Security: Adaptive Cyber Threat Defense

Advanced Defense for the Sophisticated Attacker

TrapX's DeceptionGrid is now combined with Cisco Identity Services Engine (ISE) using Platform Exchange Grid (pxGrid) and Cisco Advanced Malware Protection (AMP) Threat Grid. This integration enables DeceptionGrid to provide actionable threat intelligence and initiate rapid threat containment actions or interdiction throughout Cisco's security ecosystem. The joint solution offers customers early detection capabilities for advanced targeted attacks, Zero-Day malware, and human threat actors operating inside the network, as well as the ability to assertively isolate compromised assets with agility, shutting down attackers in near real-time.

TrapX DeceptionGrid

DeceptionGrid provides adaptive Deception technology for Global 2000 enterprises where self-camouflaging traps (also known as decoys) are automatically distributed through the network. These traps are intermingled with, and appear identical to, real information technology resources within the environment including servers, workstations, switches, and specialized devices such as IoT and Supervisory Control and Data Acquisition (SCADA) devices. Agent-less tokens are deployed on real assets and act as lures to actively divert threat actors to these traps.

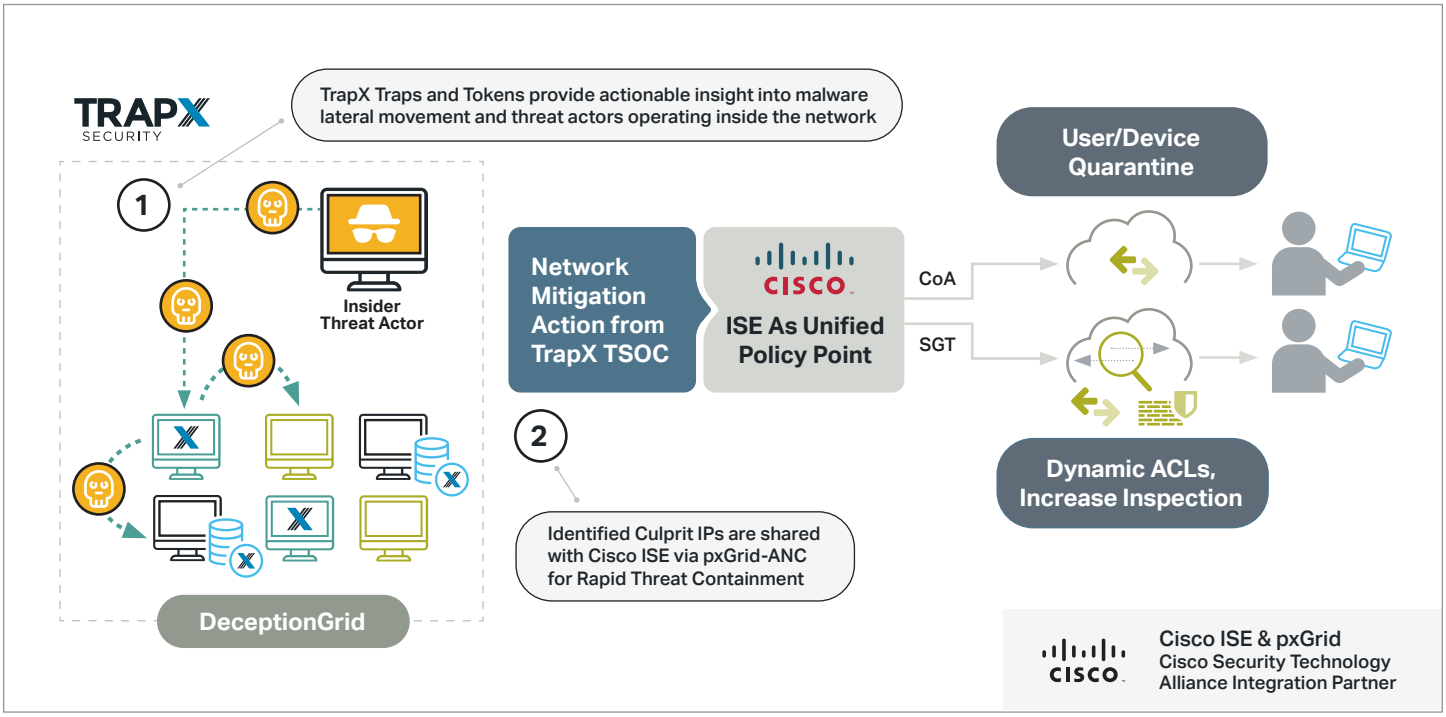
The moment a trap is touched, by malware or other activity, it sets off a high-fidelity alert. DeceptionGrid captures the malicious behavior and any suspicious binaries that have been uploaded to the traps. DeceptionGrid then performs automated forensics analysis and generates near real-time, Indications of Compromise (IOCs) against the insider threats. These IOCs can be shared with the Cisco Security ecosystem via Cisco ISE and Cisco AMP Threat Grid.

Cisco Partnership Benefits

- **Powerful Situational Awareness.** DeceptionGrid detects VLAN lateral movement unseen by other cyber defenses.
- **Reduced Time-to-Breach Detection.** DeceptionGrid detects the movement of malware almost immediately.
- **Highest Fidelity Alerting.** DeceptionGrid generates a very small number of highly accurate alerts.
- **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 uncover hidden threats targeting critical assets in both IT and OT infrastructure.
- **Combined solution provides augmented, actionable visibility.** into lateral movement caused by attackers targeting special turnkey systems like IOTs, SCADA, ICS, POS and medical devices.
- **Cisco Ecosystem Integration.** DeceptionGrid seamlessly integrates into your existing Cisco security architecture for rapid deployment, ease of management, and rapid threat containment via Cisco ISE.

Cisco Identity Services Engine (ISE) Platform Exchange Grid (pxGrid)

Cisco ISE is a next-generation secure policy management platform that automates and enforces context-aware security access to network resources. Cisco pxGrid is a messaging fabric that enables multi-vendor, cross-platform network system collaboration among parts of the IT infrastructure. DeceptionGrid leverages Cisco ISE- pxGrid to share IOCs with Cisco ISE and make it available to 3rd party vendors in Cisco's expanding security ecosystems.



Cisco Advanced Malware Protection (AMP) Threat Grid

Cisco AMP is a unified malware and threat analysis platform that provides context-driven analytics to accurately identify attacks in real-time, analyzing millions of files and correlating them against hundreds of millions of other malware artifacts to give customers a global view of threats in their security environment. Integrating DeceptionGrid with Cisco AMP Threat Grid allows for an automated detail analysis of Zero-Day binaries captured by the traps. TrapX Security Operations Console (TSOC) utilizes the detailed binary analysis report provided by Cisco AMP Threat Grid and combines it with IOCs detected through our own automated PCAP forensic analysis in order to generate high-fidelity alerts offering conviction against identified insider threats and threat actors.

How TrapX DeceptionGrid Deceives, Detects and Defeats Attackers

Detect advanced insider threats targeting IT assets, IOTs, medical devices and other special turn-key systems.

Challenge	Solution
Advanced cyber attackers use highly specialized techniques and customized Zero-Day malware to bypass traditional security controls and target high-value IT assets from inside the network. Unprotected IoT and special turn-key systems connected to internal networks greatly increase the risk of compromise by these attackers.	DeceptionGrid actively lures attackers towards fake computing resources (decoys) hosting false data. Once attackers touch these traps they are identified and a high-fidelity alert is generated. This rapidly identifies attackers within the network and reduces their access to high-value data and assets such as IoTs, ICS, PoS, and medical devices. Detected IOCs and any suspicious binaries captured by the traps are shared with the Cisco Security ecosystem via Cisco AMP Threat Grid. AMP Threat Grid performs dynamic analysis on the binaries which allows a security team full visibility as to how the malware operates and the best way to respond.
Gain Incident Response Agility	**Trigger rapid threat containment via Cisco ISE with a push of a button**
Challenge	**Solution**
Data breaches are continuing to grow in size, yet there is a continued shortage of IT security experts, and the average number of days-to-detection for advanced threats remains in the three digits. The result is a need for security intelligence acceleration, automation and threat intelligence sharing. IR and hunt teams need solutions to help prioritize incidents and automate the response process.	DeceptionGrid offers actionable insight against insider threats with high-fidelity alerts and conviction against Zero-Days, APTs, and adversaries operating within the perimeter. Detected IOCs are shared with the Cisco Security ecosystem via Cisco ISE pxGrid. When a high fidelity notification of a compromised asset is sent from DeceptionGrid to Cisco ISE it can automatically trigger a real-time quarantine policy enforcement preventing the attack from causing further damage while security teams respond to the incident.

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**.