PRODUCT BRIEF

DeceptionGrid™ 6.0

An Introduction to DeceptionGrid

In today's environment, the question isn't whether attackers will penetrate your networks, but when and how often. Attackers are using increasingly sophisticated techniques to penetrate the most robust perimeter and endpoint defenses.

How do you know if an attacker has penetrated your network? How can you identify them quickly? What are their intentions? How quickly can you stop an attack and return to normal operations?

TrapX Deception in Depth architecture addresses these important questions with powerful DeceptionGrid technology to bait, engage, and trap sophisticated attackers at every step. DeceptionGrid is a full suite of deception techniques, including the automated deception Tokens (lures) and medium and high-interaction Traps (decoys). It baits attackers by deploying camouflaged Traps and Tokens among your actual IT resources. Our Traps appear identical in every way to your real operational IT assets and your connected Internet-of-things (IoT) devices. Deception in Depth takes the illusion a step further, engaging sophisticated attackers by maintaining a facade of convincing network traffic among our Traps.

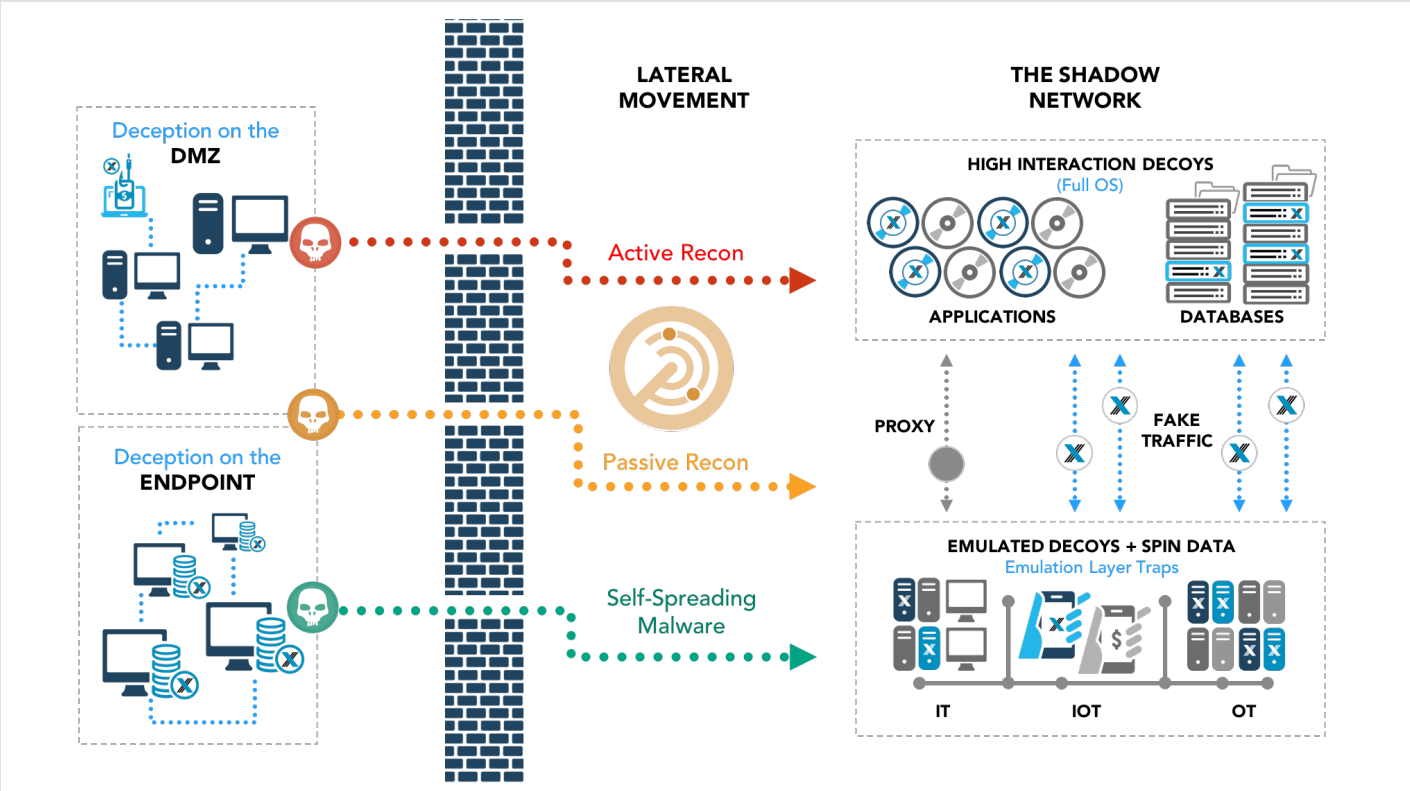
DeceptionGrid dynamically baits, engages, and traps attackers across all areas of the network.

When cyber attackers penetrate an enterprise network, they move laterally to locate high-value targets. DeceptionGrid dynamically baits, engages, and traps attackers across all areas of the network. Just one touch of the DeceptionGrid by the attacker sets off a high-confidence ALERT. DeceptionGrid integrates with key elements of the network and security ecosystem to contain attacks and enable a return to normal operations.

Deception in Depth – The Architecture of Choice

TrapX Deception in Depth combines wide-ranging deception capabilities to bait, engage, and trap attackers, presenting deception attack surfaces that best match attacker activity. This multi-tier architecture creates a tempting environment for attackers within the network. Everywhere they turn, they're faced with immediate identification. Bait such as cached credentials, data base connections, network share, and more, lure attackers to the Traps. The Traps extend transparently through our smart-deception proxy to our fullOS decoys for the deepest attacker engagement and diversion.

This multi-tier approach to engagement maximizes the deception surface to bait the attacker. It allows us to identify attackers quickly, determine their intentions, and gather detailed forensics and evidence. This deep visibility into malicious activity within your network can minimize or eliminate the risk to intellectual property, IT assets, critical infrastructure, and impact on business operations.



DeceptionGrid Architecture

High Accuracy – Minimal Alerts

In large enterprises, conventional cyber-defense technologies, such as firewalls and endpoint security, can generate thousands or even millions of alerts daily, overwhelming cyber-security operations. Unfortunately, just one successful penetration can compromise an entire network.

DeceptionGrid takes a different approach. Unlike firewalls and endpoint security methods, which generate alerts based upon probability, DeceptionGrid alerts are binary. Attackers either attempt to engage our Traps or they don't. If they do touch a Trap, we know with nearly 100 percent probability that it's an attack.

DeceptionGrid Core Components

DeceptionGrid Core Functionality – DeceptionGrid scans your existing network and provisions hundreds-to-thousands deception components. Deception Tokens, or lures, which appear as ordinary files and databases, are embedded within real IT assets. Traps—decoys that emulate servers, workstations, network switches, etc.—can be deployed rapidly, as can special decoys that emulate medical devices, ATMs, retail point-of-sale terminals, components of the SWIFT™ financial network, and more.

Full Automated Forensics – Real-time automation isolates attacker tools and malware and can forward it for advanced analysis. TrapX provides malware analysis services based on our ecosystem integration, and we also offer a cloud-based option. We combine the additional intelligence gained from our analysis with Trap activity and deliver a comprehensive assessment to your security operations center team. DeceptionGrid's Network Intelligence Sensor feature analyzes outgoing communications and, combined with its analysis of Trap activity, builds a complete picture of compromised assets and attacker activity.

AIR Module – AIR Module, designed for rapid automated forensic analysis of suspect endpoints, is a core component of DeceptionGrid and a key part of our Deception in Depth architecture. Automated analysis is triggered by indications of compromise (IOCs) identified by DeceptionGrid and often pointing to compromised endpoints. The AIR Module performs a complete, fully automated forensic analysis of any suspect endpoints, then loads the forensics artifacts from the endpoints into the AIR Module. The module then runs smart intelligence correlation against the artifacts to complete and deliver the analysis.

Integrated Event Management and Threat Intelligence – Information from the automated forensic analysis is pulled into the management system, tagged with a unique ID, and then stored within the integrated event management database. The business intelligence engine combines the information with threat intelligence data to prevent future attacks. The Network Intelligence Center monitors outbound activity on real hosts, based on information on malicious activity spotted within decoy systems.

CryptoTrap™ Module – CrytoTrap is another important core component of DeceptionGrid and a key part of our Deception in Depth architecture. CryptoTrap is designed specifically to deceive, contain, and mitigate ransomware early in the exploitation cycle, halting the attack while protecting valuable resources. Traps are created that appear as valuable network shares to ransomware. Customers can also provide their own decoy data to make the information appear even more authentic. CryptoTrap reacts to a ransomware attack immediately and holds the ransomware captive to protect real systems while concurrently disconnecting the source of the attack.

DeceptionGrid takes a different approach. Unlike firewalls and endpoint security methods, which generate alerts based upon probability, DeceptionGrid alerts are binary. Attackers either attempt to engage our Traps or they don't. If they do touch a Trap, we know with nearly 100 percent probability that it's an attack.

Deploy in the Cloud or On-Premise

DeceptionGrid is designed to deploy rapidly to support the requirements of the largest enterprise. Automation allows IT teams to complete full deployment in just a few hours in most cases. We can also deploy DeceptionGrid through a managed security service provider (MSSP). DeceptionGrid's security operations console provides support to MSSPs to monitor the status of large numbers of customers.

Automation Delivers Enterprise Scale

DeceptionGrid was developed to overcome the limitations of conventional perimeter defenses, signature-based tools and intrusion-detection methods, and honeypots. Our multi-tier Deception in Depth architecture includes powerful automation for scalability, which is essential to supporting large enterprises and government systems without the high cost of configuring individual deception nodes manually.

Partner Ecosystem

DeceptionGrid provides the advanced business analytics and smart cloud intelligence needed to correlate threats across our partner ecosystem. We empower partner organizations to make data driven security decisions, better engage customers, manage customer environments, and help them gain a distinct competitive advantage.

Comprehensive Service and Support

The TrapX Service and Support Program is designed to help you stay several steps ahead of attackers, using the TrapX solution. Our proactive services for deploying our advanced deception technology can help you identify and eliminate threats that often go unnoticed by other cybersecurity solutions, ensuring the highest level of protection for your key assets.

Differentiation

- Faster, real-time detection of cyber attacker movement anywhere in your local network and cloud environments.
- 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.
- Automated deployment of thousands of DeceptionGrid traps with minimal resources.
- 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.
- The Advanced Incident Response (AIR) Module delivers an automated memory analysis for any endpoint suspected of being compromised.
- Deception in Depth architecture integrates the benefits of Tokens, emulated Traps, FullOS Traps, and our Active Networks feature in one integrated multi-tier 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.

Key Benefits of DeceptionGrid

- **Targets the new breed of cyber attackers.** Deception technology finds sophisticated attackers that existing vendors cannot detect and that may already be inside your network.
- **Reduces or eliminates economic losses.** Accurate and rapid detection reduces the risk of economic loss due to destruction of enterprise assets, theft of data, and overall impact to business operations.
- **Reduces time to breach detection.** Advanced real-time forensics and analysis, coupled with high accuracy, uniquely empowers your security operations center to take immediate action to disrupt all attacks within the network perimeter.
- **Comprehensive visibility and coverage.** Defense in Depth provides comprehensive visibility into internal networks, revealing attacker activity and intentions, and terminating the attack.
- **Improves compliance,** to meet PCI and HIPAA data breach laws, along with other regulatory requirements in various countries.
- **Lowest cost of implementation.** Deception in Depth provides the greatest breadth and depth of deception technology at the lowest cost to your enterprise.
- **Compatible with existing investments.** Deception technology can integrate with your existing operations and defense-in-depth vendor solutions.

ABOUT US

TrapX has created a new generation of deception technology that provides real-time breach detection and prevention. Our field proven solution deceives would-be attackers with turn-key decoys (traps) that "imitate" your true assets. Hundreds or thousands of traps can be deployed with little effort, creating a virtual mine field for cyberattacks, 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. Uniquely our automation, innovative protection for your core and extreme accuracy enable us to provide complete and deep insight into malware and malicious activity unseen by other types of cyber defense. TrapX Security has many thousands of government and Global 2000 users around the world, servicing customers in defense, health care, finance, energy, consumer products and other key industries.

TrapX Security, Inc.
1875 S. Grant St.
Suite 570
San Mateo, CA 94402
+1-855-249-4453

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