DECEPTIONGRID™ 7.0

DECEPTIONGRID - A POWERFUL DEFENSE AGAINST ADVANCED THREATS

The primary reason why organizations fail to prevent cyberattacks, and attackers are so successful, is not technical; it's economical. There is an inherent economic imbalance between the defender and the attacker. Generally, attacking is quite cheap while defending remains extraordinarily expensive. Attacks rarely require sophisticated or expensive infrastructure and an active underground knowledge-exchange shares unpublished vulnerabilities. Attackers tend to exploit the weakest link of a system; from there, they may pivot to anywhere throughout an organization.

The defender, on the other hand, must remain 100% successful in order to stop an attack. The challenge is only getting more complex with the increasing adoption of cloud-based and IoT devices. Learning how an attacker carries out an attack from beginning till end is essential to cybersecurity teams. Tactics, Techniques, and Procedures, or TTP, describes an analysis of an operation and corresponding profiles of certain threats or actors.

TrapX creates a paradigm shift in cybersecurity by placing the economic responsibility on attackers rather than the victims. DeceptionGrid 7.0 is a low-friction, highly accurate threat detection and threat-response platform. A centrally managed system creates, distributes, and monitors an entire deceptive environment. Authentic decoys disguised as company assets are used to entice, detect, and engage attackers. Fake assets such as documents, users, devices, applications, services, and infrastructure fool automated hacking tools and human adversaries. A responsive alert system swiftly and decisively notifies teams of any suspicious activity. Ongoing attack intelligence relays important information to other users susceptible to attack.

Knowing your adversary is essential to the fight against malicious network attacks. An ability to detect, deceive, and defeat makes the TrapX DeceptionGrid a proactive approach to cybersecurity.
DeceptionGrid 7.0 is a universal solution for enterprises, data centers, and campuses around the world. Single appliance supports detection of all small to high network interactions throughout an entire network. Whether on-premise or cloud-based, systems of all varieties benefit from the software's ability to adjust with precision. Pain-free deployment, a minimal ongoing operational burden, and zero false positives give teams what they need to stay on top of advanced threats. Detect, deceive, and defeat; a three-pronged approach relieves woes commonly experienced by security, IT, and management alike.

The TrapX DeceptionGrid 7.0 is the only full-stack deception solution that ensures attackers get diverted to, and are occupied by, fictitious resources. Authentic decoys resemble real company assets to attract the attention of these malicious threats. Using a shadow network, the tool analyzes attacks and uses insight to adjust accordingly in real-time. Legitimate network users never engage with either traps or bait, therefore, DeceptionGrid alerts contain no false positives and allow the security team to focus on real issues instead of false alarms.

COMPREHENSIVE DEPLOYMENT

TrapX DeceptionGrid 7.0 levels the playing field by detecting previously unseen attack techniques and patterns. In support of over 500-traps per appliance, the platform requires a very limited number of resources even when deployed throughout the most expansive of networks. End-to-end integration with existing solutions automatically translates attack intelligence to the mitigation of threats. A sophisticated emulation engine simulates any attack surface across IoT/OT/Enterprise scenarios, whether on the endpoint network or data. This multi-tiered deception provides a much wider reach by funneling attackers towards trap interaction. The integration of full Linux OS features adds further compatibility to systems used within every industry.

AUTHENTIC DECOYS ALLOWING DEEP ENGAGEMENT AT SCALE

The majority of available deception tools force a tradeoff between deep deception at a low scale, via virtualized decoys, and low interaction at a large scale. TrapX revolutionizes the market by combining emulated decoys that can proxy attacker activity to high interaction decoys supporting deep deception at enterprise-grade scalability. DeceptionGrid 7.0 is a multi-tier approach offering network emulation traps alongside real OS support including Linux. A higher number of diverse contact points quickly detects threats, determines intention, prevents attack, and gathers detail forensics. An extremely low total cost of ownership makes this a practical solution for businesses of all shapes and sizes.

A centralized automated system manages and monitors decoys disguised as workstations, devices, servers, users, and more. These deceptive artifacts stay silent when undisturbed as the security team regularly rotates locations to gain further insight within IT and OT environments. Artificial users mimic normal activity to give attackers a false sense of a successful attack; in reality, they are trapped. Decoys intercept sophisticated human attackers and consume significant quantities of an attacker's time. A smart proxy diverts traffic from each of the Linux emulated Traps to the Linux FOS, giving complete control of an attacker to cybersecurity teams. This strategy offers a deep level of engagement and supports enterprise-grade scalability.
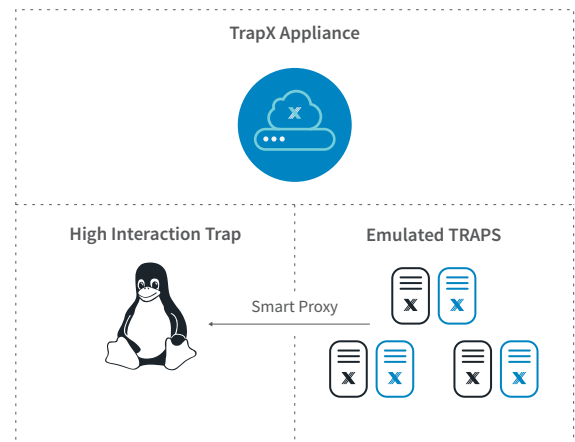
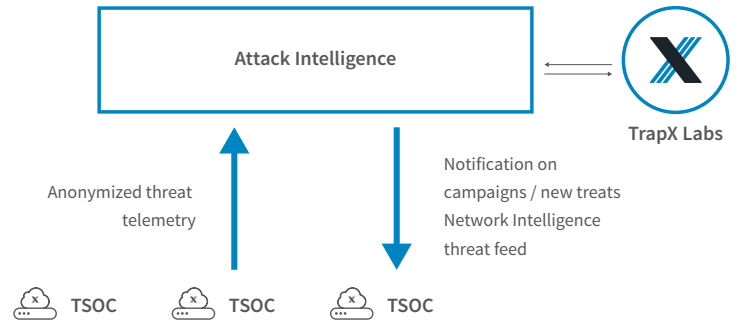# KNOW YOUR ADVERSARY'S NEXT MOVE

Just a few days, or even hours, of notice is extremely valuable to networks fighting sophisticated attacks. TrapX tracks the activity of hackers, reporting what protocols are accessed and which scripts were used. The new DeceptionGrid 7.0 Attack intelligence service allows customers to receive TTP notifications from TrapX Labs regarding malware and other campaigns affecting specific industries, geographies, or even specific vulnerabilities. Each notification provides insights into attackers' techniques, tactics, and procedures (TTP's). This attack intelligence allows timely patching of vulnerabilities and the strengthening of security controls. Each notification is based on attacker activities gathered by deployments alongside a TrapX Labs analysis and detailed recommendations. Comprehensive technological capability positions TrapX as the industry-leading provider of solutions across all deception use cases.

BUILD YOUR OWN TRAP

Build Your Own Trap (BYOT) enables the creation of fake attack surfaces tailor-made to be identical to a user's native environments. Attackers can never tell what's real and what's fake because each trap is designed to look and behave exactly like actual assets. Traps may be camouflaged as any specialized IoT and OT devices. This takes away the pain of virtualized honeypots that require users to install operating systems and provide software.

RESPONSIVE ALERT SYSTEM

Precise, informative alerts greatly reduce the time needed for remediation and resolution. Version 7.0 of the DeceptionGrid adds an extra step to the process by providing an early-warning of attacks during the post-breach phase. Threat information, as detected by decoy deployment, is collected and anonymously and sent to TrapX's Attack Intelligence server. Once data is analyzed, any trends or patterns are immediately made available to clients. Detailed forensics allows security teams to enter the mind of the attacker to better understand their intentions. This proactive process thwarts any incoming or upcoming attacks as previously identified by the TrapX.

Attack Intelligence

TrapX Labs

Anonymized threat telemetry

Notification on campaigns / new treats Network Intelligence threat feed

TSOC   TSOC   TSOC

REAL-TIME RESULTS

An advanced real-time analysis enables security teams to take immediate action against threats affecting a wide range of IT and IoT devices. DeceptionGrid 7.0 maximizes deception touchpoints to achieve a deeper engagement with decoys. The platform's Deception In-depth model gives organizations a multi-tiered defense to cyberattacks. A combination of endpoint, network, and application traps entice and engage the most sophisticated of cybercrime. Network emulated traps alongside full OS support including Linux improves overall engagement and support. Early detection minimizes financial loss due to the destruction or theft of vital corporate assets.

PROVEN RESULTS

TrapX has a positive track record with over 400 production customers. Real-time breach protection is a primary solution for commercial and governmental organizations worldwide within top industries.

DIFFERENTIATION

• Full-compatibility with other systems – An ability to work in tandem with existing operations and defense systems makes TrapX DeceptionGrid 7.0 a premium choice for sensitive environments.

• Easy to deploy and configure - Overall passivity throughout a variety of environments alleviates reluctance of leadership to adopt new technology.

• Multi-Tier Deception – A full-stack, low friction single appliance that places the economic burden on the attacker.

• Smart proxy – DeceptionGrid 7.0 detects authentic decoy interaction and allows cybersecurity to gain full control of attacks.

• Know your adversary – Real-time analysis of Tactics, Techniques, and Procedures (TTP) allows cybersecurity teams to adjust to sophisticated threats.

• Improved detection of sophisticated threats – Advanced decoys take the form of form of authentic assets to lure invaders. Traps replicating SCADA, IoT, medical, and special-use applications/devices directly targeting specific motivations.

• Build Your Own Trap (BYOT) - Gives users the ability to create their own unique attack surfaces and apps tailor-fit within your organization.

• Adaptability – The TrapX DeceptionGrid 7.0 Covers all scenarios in IT, IoT, OT, or Cloud environments by complementing or replacing SIEM, UEBA, or NTA.

• Fast detection – Overall cybersecurity efforts improve thanks to an advanced alert system with earlier and more precise threat detection

• Scalability - Single appliance support enables medium to high interaction at any scale. Innovative cybersecurity techniques define, locate, and defend against the latest and most sophisticated threats.

• Detailed forensics – TrapX DeceptionGrid 7.0 captures large volumes of data including profiles of legitimate user activity and any unusual actions associated with the profile. Information is passed on to other users to prevent future attacks.

• Reduced incident cost – Deception tools generally cost less and require fewer resources to operate than other cybersecurity measures.

• Highly interactive with Linux: smart proxies divert traffic from individual Linux-emulated traps to the Linux FOS. The FOS Trap is a jailed disposal env that can be recycled at any point.

• Used by Fortune 500 companies - TrapX is widely recognized as a leader in threat detection and response strategies via advanced deception technology.

KEY BENEFITS OF DECEPTIONGRID 7.0

• A multi-tiered approach detects, deceives, and defeats sophisticated threats

• Deception uncovers sophisticated attacks otherwise undetectable by other cybersecurity tools

• A diverse set of lures disguised as company asset lays a trail of breadcrumbs for attackers

• Emulated, proxied decoys seek the direct attention of potential attackers

• Suspicious behavior automatically triggers attention from the entire security ecosystem

• Low friction deployment with highly accurate alerts and zero false-positives

• A greater level of attack intelligence that informs customers of attacks in real-time

• Highly scalable up to the enterprise- level and interactive with Linux operating system

• Advanced real-time forensics and analytics disrupts attacks within the network's perimeter

• Profiles on attacker techniques, tactics, and procedures (TTP's) strengthen future defenses

• Track activity of hackers to identify what protocols are accessed and which scripts were running

• Users share counter-measures and traps via attack intelligence developed by fellow users

• DeceptionGrid 7.0 can integrate with any existing cybersecurity solution

• PCI and HIPAA compliance along with other regulatory requirements around the world

• The greater depth of deception technology at the lowest possible cost to your enterprise