Deception in Depth
The Architecture of Choice for Deception Technology

TrapX Research Labs
March 7, 2017
Notice

TrapX Security reports, white papers, and legal updates are made available for educational purposes only. It is our intent to provide general information only. Although the information in our reports, white papers, and updates is intended to be current and accurate, the information presented herein may not reflect the most current developments or research.

Please note that these materials may be changed, improved, or updated without notice. TrapX Security is not responsible for any errors or omissions in the content of this report or for damages arising from the use of this report under any circumstances.

Disclaimer

We have worked in strict confidence with client institutions to remediate current and future cyber-attacks. Data referenced about cyber attacks is based on government sources, our own research, and public third-party disclosures. We continue to believe that these numbers are conservative and under reported on a global basis. Our disclosed numbers represent data at a point in time during the year.
Contents

Executive Summary ........................................................................................................................................... 4
The Legacy of Defense in Depth ........................................................................................................................ 5
Pivotal Events Highlight Failure ......................................................................................................................... 7
Reducing Time to Breach - Increasing Visibility ................................................................................................. 9
Introducing Deception in Depth ......................................................................................................................... 11
  Deception in Depth - The Architecture of Choice .......................................................................................... 11
Deception in Depth: Breaking the Cyber Intrusion Chain ................................................................................. 12
  Reconnaissance .................................................................................................................................................... 12
  Lateral Movement ............................................................................................................................................... 13
  Attack High Value Target ................................................................................................................................ 14
DeceptionGrid™ .................................................................................................................................................. 16
  Low Volume - High Fidelity Alerts .................................................................................................................... 16
DeceptionGrid™ Core Components ................................................................................................................... 17
  DeceptionGrid Core Functionality .................................................................................................................. 17
  Full Automated Forensics ............................................................................................................................... 17
  Air Module .......................................................................................................................................................... 17
  Integrated Event Management and Threat Intelligence .................................................................................. 17
  CryptoTrap™ Module ....................................................................................................................................... 18
  DeceptionGrid Key Differentiation Summary ............................................................................................... 18
  DeceptionGrid Key Benefits Summary ........................................................................................................... 19
Deploy in the Cloud or On-Premise ..................................................................................................................... 19
Automation Delivers Enterprise Scale ................................................................................................................ 19
Partner Ecosystem ............................................................................................................................................... 20
Comprehensive Service and Support ................................................................................................................ 21
Executive Summary

Sophisticated human attackers use advanced tools and techniques to penetrate your perimeter and endpoint defenses. In today’s cyber security environment it is no longer a question of whether attackers will penetrate your networks, but when and how often.

The TrapX Security Deception in Depth architecture addresses these important challenges with a powerful multi-tier deception platform (DeceptionGrid) designed to match to each step of a sophisticated attack with deception. As the attack unfolds, at every stage DeceptionGrid moves to bait, trap and engage the attacker.

This paper will overview the technical capabilities of a full Deception in Depth architecture. We will share data on the important functionality of each tier of deception, the capabilities it provides and how it targets each specific phases of attacker activity.

For more information please reach out to our cyber security practice via info@trapx.com. If you are currently undergoing a suspected breach event, please reach out to support@trapx.com or call us directly via Americas: 1-855-249-4453 or EMEA & Asia Pacific: +44-208-819-9849.
The Legacy of Defense in Depth

Several years ago, the Lockheed Martin Cyber Kill Chain® was heavily popularized by the cyber defense community. The Cyber Kill Chain is heavily intrusion-centric and brings primary attention to an attacker’s efforts to penetrate the enterprise. At its very core, the Cyber Kill Chain is also focused on malware.

The Cyber Kill Chain defined seven main steps that include external reconnaissance & planning, weaponization (creation of the malicious payload), delivery, exploitation (execution of the exploit), installation, establishment of command and control to operate assets within the target network, and then action which was generally exfiltration of data targeted for theft. Consistent with the focus on the perimeter, most of the Cyber Kill Chain is focused on penetration and intrusion. Attention is targeted on the attacker activities prior to and during the intrusion event.

In concert with the stages of the attack defined by the Cyber Kill Chain, evolving strategies for cyber defense centered around the deployment of defense in depth to build and protect a strong perimeter around enterprise resources. Defense in depth follows the military principle that it is much more difficult for an enemy to defeat a multi-layered defense system than to penetrate a single barrier. In support of the defense in depth strategy, de rigueur cyber defense circa 2000, sought to build a strong and layered perimeter against attacker penetration.

The first line of defense was certainly the firewall which could restrict traffic by IP, type of protocol, port used and in many other ways. This was followed by endpoint detection systems wrapped around core technology utilizing some form of signature analysis. Similarly, an intrusion detection system also designed for signature recognition. The notion of stateful packet inspection evolved with Next Generation Firewalls (NGFW) to payload inspection, and included behavioral and heuristic detection capabilities.

These advanced intrusion detection systems often used hard coded rules but most often relied on activity overlaid by probability. If the characteristics for a positive alert tightened and demanded high probability, the number of false positives dropped. The danger, of course, was that an attacker activity would go without notice.

In contrast, if the characteristics for a positive alert loosened, then the number of false positive alerts would increase dramatically. The triage necessary to sort
through them quickly became untenable as the number of alerts soared into the thousands, tens of thousands and in some cases millions.

New software applications such as SIEMS not only consolidated alerts from disparate systems but also seek to add additional layers of threat intelligence and analysis, comparing alerts from multiple security systems, and rules had to be developed to look for activity that combined looked suspicious. This intelligence and analysis could then help reduce the large barrage of alerts to highlight only those that would truly merit attention, but the volume is often still too large to cope with.

Malware tools were still hand-written by attackers and hence were usually identified and compromised by cyber security signature analysis tools. While the availability of new attacker tools accelerated, it was still done at a pace which the countermeasures developed for signature recognition match.

Defense in depth, as arrayed around perimeter defense, worked well for several years. Defense in depth defined the architecture and approach for information security used by a large percentage of CIO’s on a global basis. It became the basis of budgeting acquisition strategies in support of cyber defense deployment.
Pivotal Events Highlight Failure

By 2008 to 2009, the situation had changed almost radically. The number of threats facing government and enterprise grew far larger than the malware predominantly addressed by the Kill Chain. The sophistication of human attackers and the tools they could use increased substantially. The cybercrime industry, growing into their new market opportunity, developed a broader supply chain. Tools emerged that enabled the remanufacturing of malware tools, encryption to better camouflage it, and additional sensors so that these tools could even detect sandboxes and change behavior. Cybercrime and nation states could evolve the threats faster than they could be mitigated by counter measure and sensor.

Cyber criminals became very successful. Most enterprise and government institutions were vulnerable to a sophisticated and persistent attack. There were far more relatively undefended potential targets than attackers. If the perimeter could be penetrated, then endless strategies appeared that could completely compromise targeted networks and systems. This perceived market opportunity drove additional funding for both nation state teams and organized crime at varying levels of scale. With rewards, so high, both entities began to invest in substantial research and development as well as expanded operations.
In many nation states, the deployment of cyber warfare team had been met with early initial success. Nation state objectives included the gathering of information, the placement of command and control “back doors” that could be used in strategic need to damage or compromise targeted infrastructure, or immediate direct damage to targeted resources.

Stuxnet, identified in 2010, showed the levels of sophistication that could be brought to bear in the development of weaponized malware. The discovery of Stuxnet was a pivotal event and a wake-up call to many nations and to the leadership in large enterprise corporate IT. The Stuxnet attack showed a major leap in innovation, sophistication and, most important, the willingness to use cyber offense as a component of national policy.

The Stuxnet intrusion, as it turned out, was relatively easy. Stuxnet was passed via malware laced memory sticks left in locations frequented by targeted personnel. Once placed within their systems, these memory sticks propagated a worm which moved through the network and distributed the destructive payload. The attack also propagated a rootkit that cleaned up all the traces of the attack. Consider the aggression associated with the attack. Stuxnet was engineered to impact the operation of nuclear centrifuges. Stuxnet programming literally commanded the centrifuges to shake themselves apart while they were in operation with highly radioactive material.

Similarly, major banks and financial institutions faced an ongoing barrage of attacks on internet based transactions, key financial application, automated teller machine (ATM) and retail point of sale systems. These attacks started to expand into healthcare and other important industries.

Cyber security leadership in the most forward thinking Government agencies, together with private industry, understood that an improved strategy was urgently required. The thesis that one could defend the perimeter, and thus successfully defend the enterprise was flawed. The efficacy of defense in depth as a deployment model, and the notion of successfully defending the perimeter, was in serious question. The damage that was likely incurred by the Stuxnet attacked centrifuges, could certainly happen to any important applications software systems, infrastructure such as power plants and generation, hospitals medical devices and databases, and more.

In a 2011 SANS publication, Prescott E. Small noted that, “Businesses and Information Technology Security Professionals have spent a tremendous amount of time, money and resources to deploy a Defense in Depth approach to Information Technology Security. Yet successful attacks against RSA, … the United States Military and many others are examples of how Defense in Depth, as practiced, is unsustainable."1

Reducing Time to Breach - Increasing Visibility

Many organizations are suffering from continual breaches of their internal networks, key application systems and data storage. Leadership understands that increasing visibility into activity within internal networks is critical. Regardless of the strength of the perimeter and endpoint defense, the broadscale barrage of focused attacks has raised the statistical probability of an attacker getting into the networks unseen to an unacceptably high rate.

The metrics associated with these breaches continue to present compelling evidence that current cyber defense infrastructure is woefully inadequate. One of the key metrics tracked today by information technology and cyber security management is the time to breach detection. Time to breach detection within global 2000 corporations at one time stood at close to approximately 416 days in 2012. Consider that during this time window of 416 days an attacker had almost complete access to targeted networks. Once the network was penetrated, the detection of the breach was usually triggered by the discover of a corporations data for sale on the dark web, the loss of financial assets, or the

gross destruction of information technology assets. Even today, as the time to breach detection metric has been reduced to 99 days, information technology leadership knows that legacy architectures and solutions still do not provide an adequate or acceptable solution for protecting the information technology. Visibility and detection remain the key issues.

---

1. How will you know if there is an attacker within your networks?
2. How can you find them rapidly?
3. What are their intentions?
4. How quickly can you contain the attack and return to normal business operations?

---

Introducing Deception in Depth

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, database connections, network share, and more, lure attackers to TrapX DeceptionGrid medium interaction Traps or full interaction traps based on attacker activity. The medium interaction traps extend transparently through our smart-deception to our high interaction traps for the deepest attacker engagement and diversion.

This multi-tier approach to engagement maximizes the deception surface to deceive 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.

Advanced automation takes the power and functionality of Deception in Depth and makes it easy to use and simple to deploy. Automation enables your security operations team rapidly deploy hundreds to thousands of Traps across your network. Automation also supports administration, notification in the event of compromise and all of the tiers within our Deception in Depth architecture.

TrapX Security DeceptionGrid™ Architecture

- Endpoint Lures Tokens
- Network Traps Medium Interaction
- Full OS Traps High Interaction
- Alerts on Fake Assets are 100% Accurate
- Prioritized Alerts
- Recirculating for Deeper Deception
- Token Malware Redirection
- Attacker Activity Alerts
- Automated Trap Redirection
- Network Intelligence
- Automated IoC Collection
- Ecosystem Integration

© 2017 TrapX Security, Inc. All Rights Reserved.
Deception in Depth: Breaking the Cyber Intrusion Chain

Reconnaissance

Once an attacker is inside your network, they start reconnaissance to acquire general information and orientation to help determine the breadth of potential assets they can target. They try to observe the network architecture and may capture network traffic to better understand the network topology. DeceptionGrid presents attackers with tokens (or lures) which are fake information technology artifacts (fake shares, credentials, data files, configuration files, etc.) that are scattered within your real endpoints and other IT assets. DeceptionGrid traps are active - they maintain a facade of ongoing network traffic among and between the deployed traps to further lure and engage sophisticated attackers.

This *1st tier of deception* presents a tempting mix of exactly the assets and intelligence desired by the attacker. Tokens are designed as bait which further lure the attacker into the traps.
Lateral Movement

Once the attacker has completed their reconnaissance, they will move laterally to map other parts of the network, and target the resources they want for theft and/or destruction. DeceptionGrid presents the attacker with traps which are fake IT assets distributed throughout the entire network.

The 2nd tier of deception assets use powerful emulation allowing traps to imitate any asset, whether it is a workstation, server, or specialized device. All of this is achieved without the need for any operating systems or applications, and offers the most diverse deception environments available. These traps draw the attacker in and trap the attacker’s malware tools. Traps utilize emulation to also provide broad scale deployment across the largest enterprise network.

Our patented emulation is very powerful - you can emulate almost any operating system and application mix. The inclusion of pre-built emulations for specialized attacker targets to include a broad mix of medical devices, automated teller machines (ATMs), the SWIFT financial systems, industrial control systems (SCADA components) and a broad mix of internet of things (IoT) devices. Further, the emulations uniquely cover components in the network, endpoint, applications and even data. You can emulate switches, routers, and many other network components. Emulation allows you to blanket and surround the real information technology resources with our Traps which rapidly identify attacker activity.
Attack High Value Target

In the final stages of the attack identified high value targets are then compromised for the theft of targeted data or damage. The attacker may also seek to penetrate application interfaces, modify transactions or perform other complex
attack procedures that require deep interaction with the traps.

As they engage more deeply with our medium interaction (emulation) traps, our **3rd tier of deception** automation continues to extend the illusion to deeper levels. Deeper interaction by the attacker will transparently extend access from the medium interaction trap to a full interaction (fullOS) trap. This smart deception proxy presents a full and convincing set of attack targets to the attacker, and does so while minimizing manual configuration, automating deployment and reducing costs. Full operating system also allows us to deploy servers which replicate actual production servers. This provides continued deep engagement for the attacker, distracting them from real IT assets, and allowing for quarantine and cessation of the attack.
DeceptionGrid™

DeceptionGrid is designed 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 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.

When cyber attackers penetrate an enterprise network, they move laterally to locate high-value targets. DeceptionGrid 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. Then DeceptionGrid integrates with key elements of the network and security ecosystem to contain attacks and enable a return to normal operations.

Low Volume - High Fidelity Alerts

Traditional cyber defense technologies, such as firewalls and endpoint security, generate many alerts. In a large enterprise the alert volume may reach thousands, hundreds of thousands or, in some cases, millions of alerts per day. Security operations personnel cannot process or investigate most of the activity. Yet it only takes one successful penetration to compromise an entire network.

DeceptionGrid takes a very different approach. DeceptionGrid ALERTS are the end result of a binary process. Any party that seeks to identify, enter, view or interact with any of our traps is immediately identified by this behavior. If you touch these traps this is clearly a violation - you should not be doing so. This is a huge advantage over heuristics and probability based approaches and the many thousands of extraneous alerts these techniques generate.
DeceptionGrid™ Core Components

DeceptionGrid Core Functionality

DeceptionGrid scans your existing network and determines the best deception architecture tailored to your specific network environment. Deception Tokens, or lures, which appear as ordinary files and databases, are embedded within real IT assets. Medium interaction traps—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 systems, and more. High interaction traps use full operating systems and support the deepest attacker engagement.

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 compromised endpoints identified by DeceptionGrid. 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 identify future attacks. The Network Intelligence Center monitors outbound activity on real hosts, based on information on malicious activity spotted within decoy systems.

© 2017 TrapX Security, Inc. All Rights Reserved.
CryptoTrap™ Module

CryptoTrap 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 Key Differentiation Summary

» 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 provides automated reputation analysis and forensic collection 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.

» Important partner integrations create end-to-end workflows from detection to remediation and increase value from existing ecosystem investments.
DeceptionGrid Key Benefits Summary

» **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.** Deception 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.

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.

Service Providers

The TrapX managed service provider program (MSP/MSSP) allows partners to take our products and services directly to market under the software-as-a-service (SaaS) business model. The program is structured to minimize operational overhead and maximize sales and profitability. TrapX Security provides our suite of software and service modules, which give you and your customers complete control and management of their security. Our commitment to supporting our service provider partners is a key part of our business, facilitating the growth of our combined customer market.

Resellers

The TrapX real-time adaptive security model provides unique advantages to our TrapX Partner Program resellers, including training programs and sales and marketing commitments.

Technology Partners

Best-of-breed technologies that work together seamlessly enhance customer value and speed of implementation, enabling existing security systems to benefit from DeceptionGrid’s detection and advanced IOCs. Through our Technology Partnership Program, we ensure that our customers can easily implement the TrapX Security Platform in conjunction with other technologies, such as intrusion detection and prevention, next-generation firewalls, and endpoint security solutions.

Our program works across various industry disciplines and business functions to test your company’s products and services with the TrapX Security Platform. Our testing process ensures that your products meet the technical requirements needed to perform well within our platform.
We offer a variety of certifications under the Technology Partner Program, some of which may require integration with our API. Complete program details are available to TrapX registered partners.

Our key partner integrations define the DeceptionGrid ecosystem. Sandbox support integration includes Cisco AMP Threat Grid, McAfee ATD, Palo Alto Networks WildFire, ThreatTrack, and Cuckoo. Sandbox integration enables TrapX to provide an additional level of actionable threat intelligence from attackers and their malicious payloads.

DeceptionGrid is also tightly integrated with McAfee DXL. DeceptionGrid can send IOC data through organizational DXL messaging, for use by McAfee products such as ePolicy Orchestrator (ePO), Threat Intelligence Exchange, and Active Response.

**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.

Our support and service experts are available to help with product installation, support services, system health checks, and special services, including comprehensive forensics. Support includes a basic service-level agreement, with unlimited service requests and ongoing case management. We also provide the latest hotfixes and service packs, major upgrades and enhancements, and proactive escalation. We’re also here to help during critical periods of incident response and crisis management.

Professional services can augment your team with additional support resources, locally and remotely, with cybersecurity consulting, deep analysis, and assistance. Our team supports every aspect of your DeceptionGrid environment, including operational deployment, upgrades, and ongoing management. Our team is also available for hands-on training, customized to your environment and deployment. Our team members’ backgrounds and qualifications can be matched to the vigorous requirements of the most secure government, military, and enterprise requirements.

For the most current information on our partner ecosystem, please refer to our website: [http://trapx.com/partners/](http://trapx.com/partners/)
About TrapX Security

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

TrapX, TrapX Security, DeceptionGrid and CryptoTrap are trademarks or registered trademarks of TrapX Security in the United States and other countries. “Cyber Kill Chain” is the trademark of Lockheed Martin. Other trademarks used in this document are the property of their respective owners. © 2017 TrapX Security. All Rights Reserved.