TRAPX
SECURITY

DATA SHEET

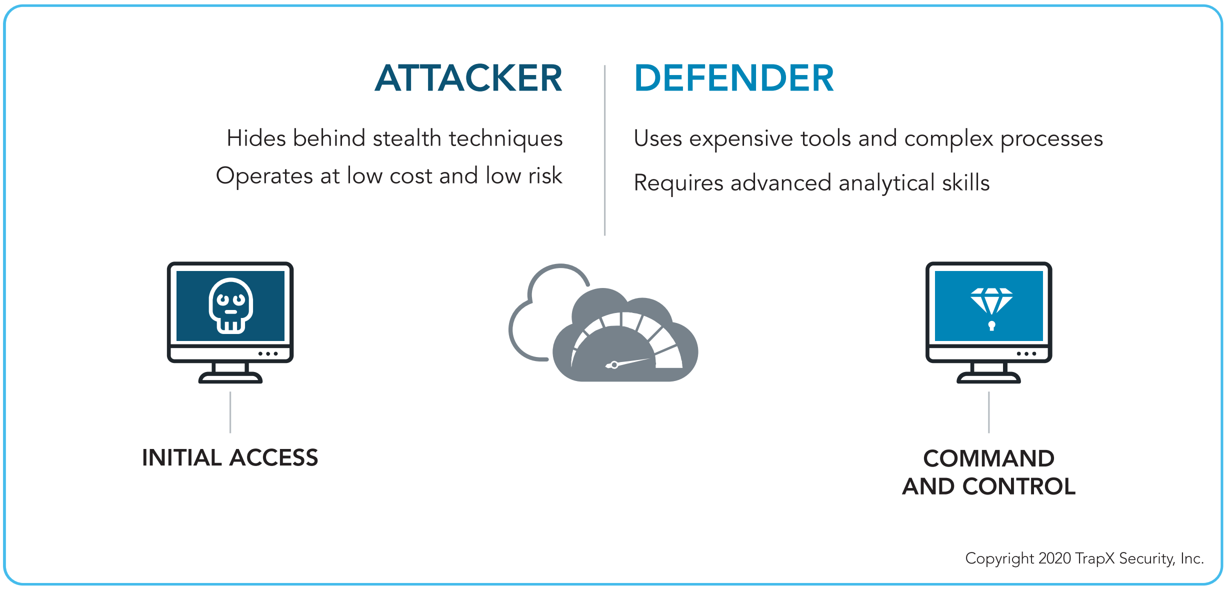
DECEPTION WITHOUT LIMITS

A Technical Product Overview

Digitally signed by Cojocari Andrei
Date: 2022.01.14 15:07:57 EET
Reason: MoldSign Signature
Location: Moldova

Why Deception?

Business is moving and changing at an exceptional rate. Digital transformation has accelerated. Remote work is the new normal and security is being pushed into a new reality of surface area expansion, blind spots and risk exposure. Lateral movement visibility and the disparity between attack and response velocity remains a serious concern. Traditional monitoring and controls simply do not fit in this new paradigm, leaving more devices, systems and processes exposed, and more risk unaddressed.


ATTACKER
Hides behind stealth techniques
Operates at low cost and low risk
DEFENDER
Uses expensive tools and complex processes
Requires advanced analytical skills
INITIAL ACCESS
COMMAND AND CONTROL

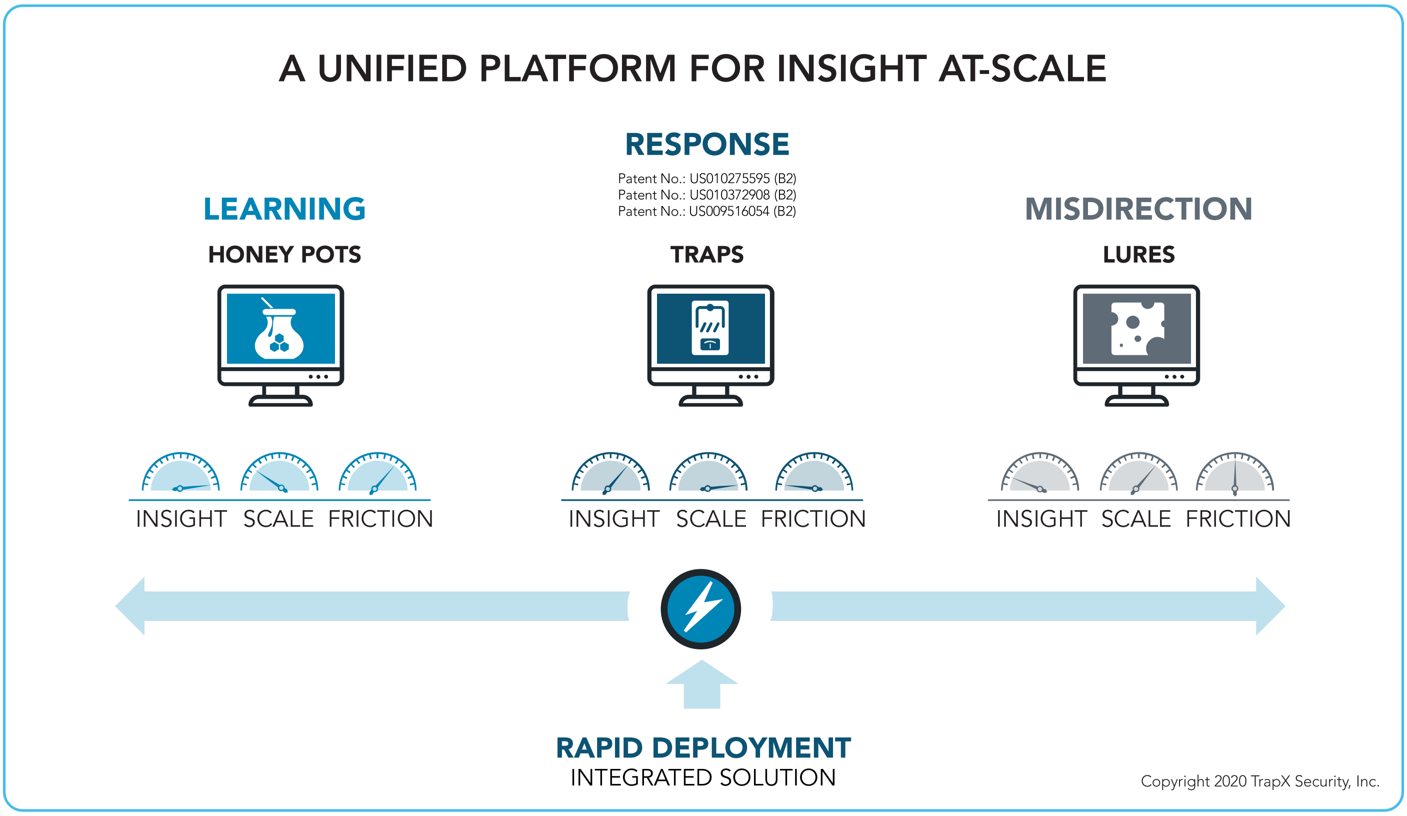
Copyright 2020 TrapX Security, Inc.

Deception has emerged as a technology that fills a vital gap in layered cybersecurity. A light, fast and transparent solution that covers the entire surface area and disrupts attacks in the network, independent of the state or nature of the endpoint. Deception hides real assets in a crowd of imposters that interact with attackers and misinform them in exchange for insight into their TTPs, allowing for rapid response and containment.

There are several commercial options available on the market. Some facilitate endless interactions with virtualized, full stack traps. They deliver insight, but scale is limited by cost and complexity. Others direct attacks away from assets with endpoint bait. These solutions are lightweight and easy to deploy, but deliver limited visibility and are not applicable to IoT or OT environments. Each approach adds value, but taken alone, forces risk-based trade-offs between scale and insight.

DeceptionGrid™

DeceptionGrid from TrapX is the only Deception platform that delivers both comprehensive protection and full visibility at-scale. In just minutes, our patented emulation technology launches hundreds of authentic traps that engage attackers and malware and generate high-fidelity alerts for rapid response. Our emulated traps can be enriched with high interaction traps and lures to provide an end-to-end solution from a single platform. Unlike anything else on the market, our lightweight, touch-less technology offers non-disruptive support for a broad array of systems and devices, including IT, OT, IoT, SCADA, ICS, and SWIFT, and delivers immediate time-to-value.



Copyright 2020 TrapX Security, Inc.

TrapX Appliance: 500+ emulations across 200 VLANs/appliance

Cloud: Support for both public and private clouds, including AWS EC2 and MS Azure

On-Prem: Support for both physical and virtualized hardware across VMWare, Hyper-V, KVM and OpenStack

TrapX Deception Tokens: Lures deployable via GPO/SCCM

Lures deployable via GPO/SCCM: Purpose-built automatic Incident Response system and Forensics (AIR platform)

The TrapX Difference

Fast

TrapX uses advanced cloud or on-premise Deception technology to detect and divert attacks as they happen, allowing for immediate visibility into malicious activity. A full environment can be activated in minutes for immediate time-to-value.

- Lightweight, rapid deployment and scale
- Hundreds to thousands of traps within minutes
- Authentic OOTB traps
- Standard operating system images
- Native integration with Active Directory

USE CASES

» Ransomware
» Man-in-the-Middle Attacks
» Credential Theft
» AD Reconnaissance Attacks
» Lateral Movement

Flexible

TrapX is touch-less, emulating virtually any asset across any environment, from small private networks to large multi-tenant clouds. TrapX is the only solution that can easily flex between full, medium and low interaction traps.

- 200 VLANs per appliance with no need for 3rd party licensing
- Unlimited VLAN support
- 3-tiered interaction Deception: emulation traps, lures with Full OS via proxy
- Build Your Own Trap (BYOT): easy to build custom traps with no added cost or professional services
- Identifies and automatically adapts to new assets or operating systems on the network
- Dynamic licensing across VLANs
- Multi-tenant and role-based for customized admin roles

Business Benefits

Reduce Risk

Lateral movement visibility

Channels attacks away from assets ahead of remediation; Integrated with Vulnerability Management for real-time asset discovery and risk management

Minimizes time-to-detection, triage and containment

Advanced alert system, attack analysis and threat intelligence combine to deliver real-time, critical mitigation and containment information

Streamline Operations

Easy, non-disruptive deployment; no hardware or OS to license or maintain; simple to operate

Accurate alerts, automated response to network changes minimize overhead

Supplements SIEM and other response data with high-fidelity alerts to drive down false positives and reduce dwell time

Robust ecosystem and open API/SDK kit supporting end-to-end SOC integrations

TRAPX SECURITY

DATA SHEET

Frictionless

TrapX is engineered for simple non-disruptive operation. Our agentless architecture deploys quickly without impacting production environments.

- Out of band, agentless technology
- No endpoint processing or computing needed
- Non-disruptive implementation of even advanced functionality, including attack visualization, misconfiguration and credential review

Complete

TrapX is built to extend across any surface area.

- Detects physical, automated and malware attacks
- Monitoring of internal lateral movement as well as 'known-bad' outbound Internet traffic
- Integrated with MITRE ATT&CK for threat and investigation context
- Real-time analysis of TTPs
- Integration with SIEM, UEBA, NTA, EDR, and Vulnerability Management solutions
- Industrial-grade, fan-less appliance

Out-of-the-Box (OOTB) Traps: Surface Area Coverage

Workstations

» Windows XP, 7, 8, 10

» Mac OS

Servers

» Windows 2003, 2008, 2012, 2016

» Linux Server

» Public Traps

Networking

» Cisco Catalyst

» Cisco PBX (VOIP)

» Juniper EX / Junos

Industrial

» Siemens PLC

» SCADA

» SAP GUI / NetWeaver

» Rockwell PLC

IOT

» Point of Sale (POS)

» Phillips Smart Lights

» Lexmark Printers

» Axis Network Cameras

Medical

» PACS Server and Viewer

» MRI

» CT

Financial

» SWIFT Web, Lite, Alliance Gateway and Access

» ATM

BYOT

» For systems and devices not included above, TrapX provides self-service, 'Build Your Own Trap' capabilities

» Build Your Own Trap (BYOT) enables creation of fake attack surfaces tailor-made to be identical to a user's native environment. Attackers can never tell what's real and what's fake because each trap is designed to look and behave exactly like real assets. Traps can also be camouflaged as any specialized IoT and OT devices.

Product Highlights

Fast and Easy

- Extensive OOTB traps – More than 500 traps deployed in minutes
- Native integration with Active Directory
- Cloud-based and/or on-premise deployment; No excessive hardware or software to license and maintain

Dynamic

- Identifies and automatically adapts to new assets or operating systems on the network
- Lures attackers away from real assets
- Malicious activity triggers only accurate, positive alerts
- Detailed forensic information for insight, analysis and response gives SOC control of the attack

Comprehensive

- Expansive surface area coverage includes IoT, OT, SCADA, ICS as well as a wide range of system and application environments (Legacy, homegrown, SWIFT, Cloud)
- Risk ranked alerting for all trap events, including Scan, Connection, Reconnaissance, Interaction and Infection

Intelligent

- Risk Zones: ability to segment high risk areas
- Accurate alerts with detailed forensics triggered by any attacker action: interaction with lure, scanning, connecting, interacting or infecting a trap
- Threat Intelligence Network: Cloud-based Threat Intelligence anonymously collects detection activity from participating community members for analysis by the TrapX Threat Analysis/Incident Response team. Relevant findings on new attacks along with the IOC (Indicators of Compromise) are shared.

Visual and Connected

- Forensics visualization; statistical and dynamic analysis; correlation connects the dots between events
- Integrated with endpoint and network security products, including Sandbox for files retrieved from traps for end-to-end incident intelligence and response
- Visualization reveals attack path, timestamp and trail to anticipate and respond to malicious actions

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.

TrapX, TrapX Security, DeceptionGrid and CryptoTrap are trademarks or registered trademarks of TrapX Security in the United States and other countries. Other trademarks used in this document are the property of their respective owners.
© TrapX Software 2020. All Rights Reserved.