PRODUCT BRIEF

TRAPX SECURITY

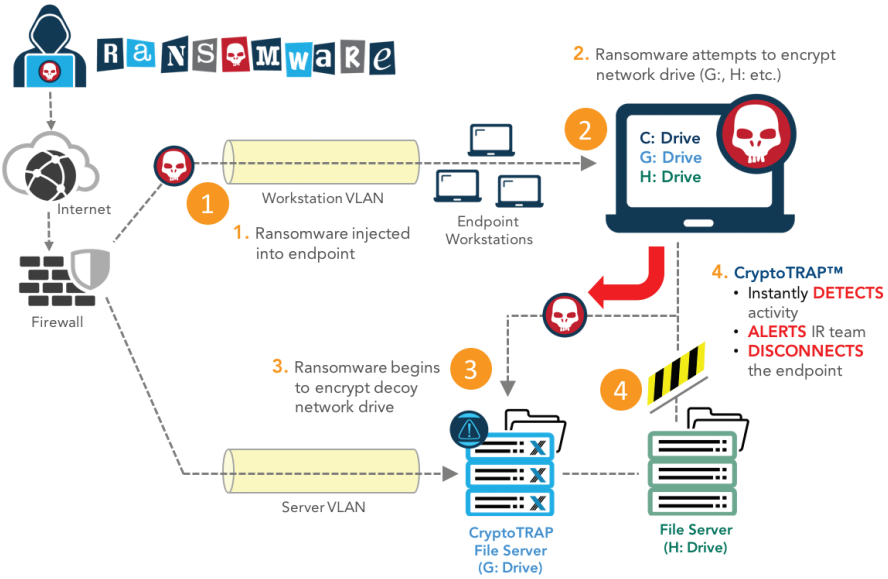
CryptoTrap™

Stop Ransomware Attacks Before They Start

CryptoTrap uses powerful deception to deceive, contain and mitigate ransomware early in the exploitation cycle, halting the attack while protecting valuable network assets. Traps (decoys) are created by CryptoTrap that appear to ransomware as standard SMB network shares. CryptoTrap allows companies to upload their own fake data which is automatically replicated across all the traps. CryptoTrap endpoint tokens (lures) are deployed on users systems to divert network-based ransomware attacks to the traps thereby protecting the real files. As ransomware touches these traps CryptoTrap immediately discovers the attack, and holds it captive with fake data while simultaneously disconnecting the source computer from the network and alerting security personnel.

CryptoTrap is Part of the DeceptionGrid™ Family of Products

CryptoTrap is a new offering for the DeceptionGrid family of products. CryptoTrap allows you to deceive, detect and then decisively defeat attacker's ransomware.



CryptoTrap Value

- Timely detection and defeat of ransomware protects critical corporate data.
- Avoids extensive and potentially expensive disruptions to business operations.
- Eliminates the cost of extortion and ransom payments associated with critical network data.
- Avoids or minimizes liability associated with data breach (ransomware is a data breach under HHS OCR HIPAA) resulting audits and potential litigation.
- Upgrade CryptoTrap when you are ready to add the power of DeceptionGrid to protect the network from sophisticated human attackers and malware.

CryptoTrap immediately discovers the attack, and deceives it by providing large volumes of fake data thus holding the attack captive while simultaneously disconnecting the source computer from the network.

DeceptionGrid Core Functionality

DeceptionGrid automates the provision of hundreds to thousands of traps across internal networks. These traps are designed to deceive attackers that have bypassed traditional perimeter defense systems. Typical traps include a variety of Windows workstations, Windows servers, Lunix systems and network equipment. In addition, specialized traps such as medical devices, point of sale (PoS) systems, automated teller machines and many more can be configured and deployed with a simple click. Endpoint lures, which appear as files and databases, are embedded within real IT assets. This multi-layered approach using both traps and lures will expose, divert and confuse cyber attackers at various phases of the attack.

Full Automated Forensics

Real-time automation isolates detected malware used by attackers and places it within a sandbox server. A static and dynamic forensic analysis of suspect endpoints is created by the DeceptionGrid Advanced Incident Response (AIR) module. Memory within the suspect endpoints is loaded and analyzed, the results are summarized and then all of this data is delivered to the security operations team.

Integrated Event Management and Threat Intelligence

Information from forensic analysis is automatically pulled into the management system, tagged with a unique ID, and then stored within the integrated event management database. The business intelligence engine combines this with threat intelligence data to prevent future attacks. The DeceptionGrid Network Intelligence Sensor monitors outbound activity on real hosts based upon information gathered about malicious activity that has been spotted within the traps.

Deploy In The Cloud or On-Premise

DeceptionGrid is designed to deploy rapidly to support the requirements of the largest enterprise. Automation enables the security team to complete a full deployment in as little as three hours.

DeceptionGrid Value

- Deception technology finds sophisticated attackers within a network that existing solutions miss
- Reduces the time to breach detection lowering the risk of economic loss
- Accurate alerts focus on real threats and eliminate wasted time
- Automated forensics immediately empower the security operations center with accurate and actionable data
- Traps as well as lures uniquely blanket and surround enterprise IT assets
- Emulation provides the best, broadest and lowest cost functionality for the enterprise.
- Deception technology can integrate with your existing operations and defense in depth vendor suites and partners.

DeceptionGrid Differentiation

- Powerful traps emulate industry specific devices such as medical devices, automated teller machines, point of sale terminals and so much more
- Real-time detection of attacker lateral movement anywhere within the vLan
- Real-time detection of attackers within IT endpoints
- A DeceptionGrid alert is over 99% accurate and immediately actionable
- Complete automated forensic analysis of captured malware and attacker tools
- The AIR module delivers an automated analysis of memory for any endpoint suspected of compromise
- Automated deployment
- TrapX partner integrations support a long-term cyber defense strategy

ABOUT US

TrapX Security is a leader in the delivery of deception based cyber security defense. Our solutions rapidly detect, analyze and defend against advanced attacks, insider threats as well as malicious insiders in real time DeceptionGrid provides automated, highly accurate insight into malware and malicious activity unseen by other types of cyber defense. We enable a pro-active security posture, fundamentally changing the economics of cyber defense by shifting the cost to the attacker. The TrapX Security customer base includes global 2000 commercial and government customers around the world in sectors including defense, healthcare, 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