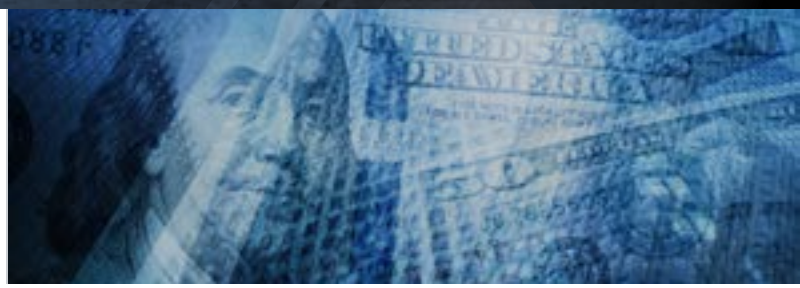
TRAPX SECURITY

PRODUCT BRIEF

Protecting SWIFT® Financial Networks with DECEPTIONGRID™



Protect SWIFT Infrastructure, Surrounding Network Assets & Back Office Systems

According to a December 2019 report from EastNets[1] (*"How Banks Are Combating the Rise in SWIFT Cyber Fraud"*), 4 out of 5 banks surveyed had experienced at least one SWIFT fraud attempt since 2016, and the problem appears to be growing on an annual basis. Conventional security products that rely on defending the perimeter or identifying malware can be circumvented relatively easily by today's skilled attackers (FIGURE 1).

New technologies, such as Deception, are now an important part of the mix for defeating sophisticated attackers. For example, DeceptionGrid from TrapX completely automates the creation and deployment of a network of camouflaged traps (decoys) and tokens (lures).

Traps are emulated systems that can imitate a variety of real IT assets, including SWIFT Alliance SAG, SWIFT Alliance SAA, and SWIFT Alliance Web Platforms for Linux and Windows deployment. These traps appear to be identical to actual SWIFT assets, and can be deployed throughout a customer's network, creating an extensive deception infrastructure.

Attackers using compromised endpoints to conduct reconnaissance are presented with deceptive tokens, such as fake administration of Remote Desktop Protocol (RDP), fake browser histories/bookmarks to Alliance Web Platform, fake SWIFT messages, and fake SWIFT credentials. These tokens lead attackers back to the deployed traps, diverting them away from real SWIFT systems.

Value to SWIFT Users

- Detects, diverts, and confuses adversaries targeting your SWIFT assets by creating a blanket of protection for your SWIFT infrastructure
- Protects against sophisticated SWIFT fraud by deploying proven, state-of-the-art deception countermeasures
- Reduces exposure and liability by quickly and dramatically improving security in and around the SWIFT infrastructure to help comply with SWIFT audits
- Helps your security team harden your perimeter against future attacks with valuable threat intelligence and forensics
- Protects other financial-network assets, including other key applications, workstations, switches, servers, and much more

DeceptionGrid completely automates the creation and deployment of a network of camouflaged traps (decoys) and tokens (lures) imitating real IT assets, including SWIFT Alliance SAG, SAA, and Web Platforms for Linux and Windows.

[1] https://www.cpomagazine.com/cyber-security/swift-fraud-on-the-rise-according-to-eastnets-survey-report

Surrounding the actual SWIFT assets with a blanket of traps and lures leads attackers to attractive decoys that look relatively undefended, no matter where they explore. By providing a full deception architecture using both traps and tokens, DeceptionGrid creates a comprehensive defense layer for your SWIFT network, along with other valuable systems.

Integrated Event Management & Threat Intelligence

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

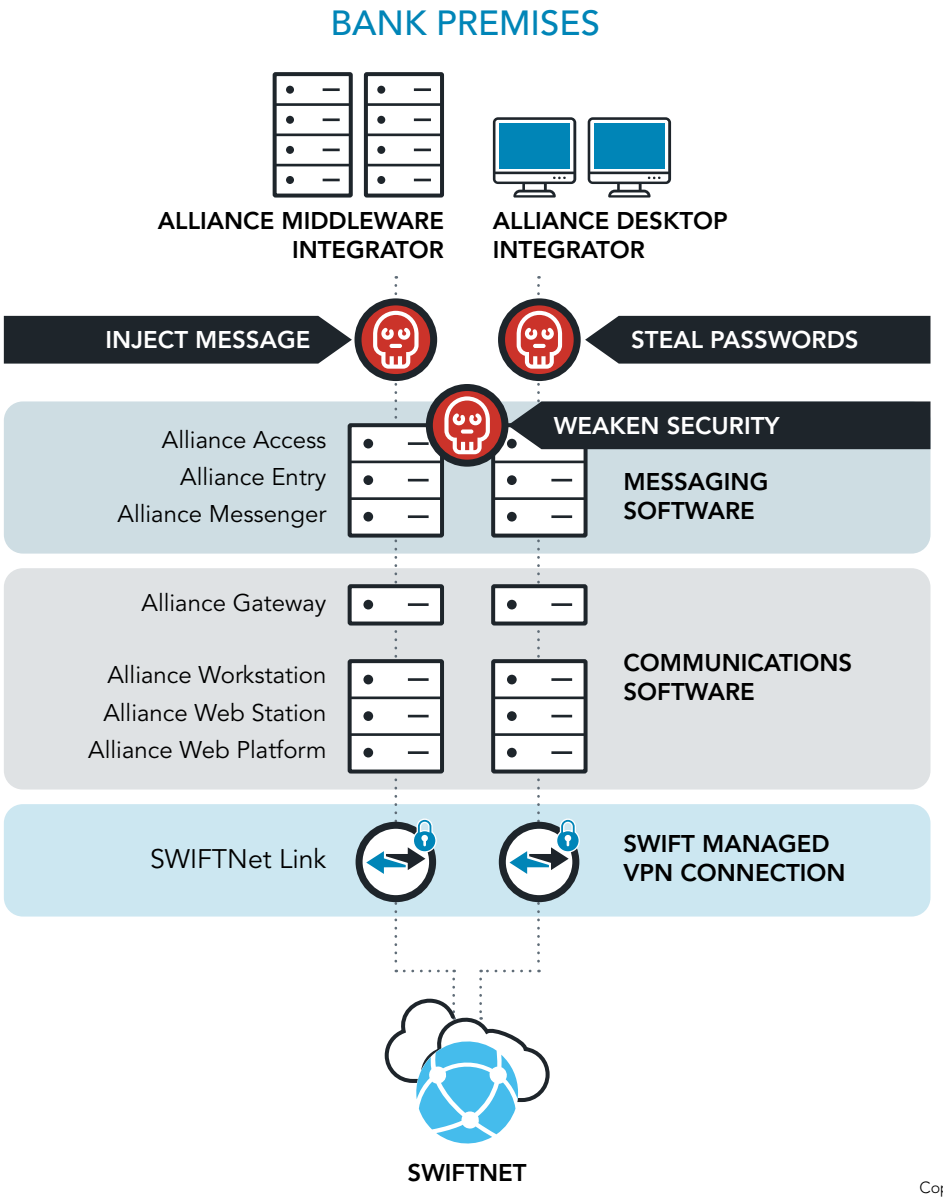
DeceptionGrid Value

- Deception technology finds sophisticated attackers within your network unseen by other solutions
- Traps minimize the risk of economic loss by significantly reducing the time to breach detection
- Eliminates wasted time with accurate, near zero false positive alerts focusing on real threats
- Automated forensics empower your security operations center with the data they need
- Emulated decoys (traps) and embedded lures (tokens) maximize protection by blanketing and surrounding your enterprise IT assets
- Maximizes existing security investments by integrating with your existing operations and defense-in-depth vendor suites and partners

DeceptionGrid Differentiation

- Ease of use and extensive library of pre-built traps enables rapid deployment and time-to-value
- Powerful traps emulate industry-specific devices such as medical devices, automated teller machines, point of sale terminals and more
- Real-time detection of attacker lateral movement anywhere within the vLAN
- Real-time detection of attackers within IT endpoints
- A DeceptionGrid alert is more than 99% accurate and immediately actionable
- Extensive list of TrapX partner integrations support long-term cyber defense strategy

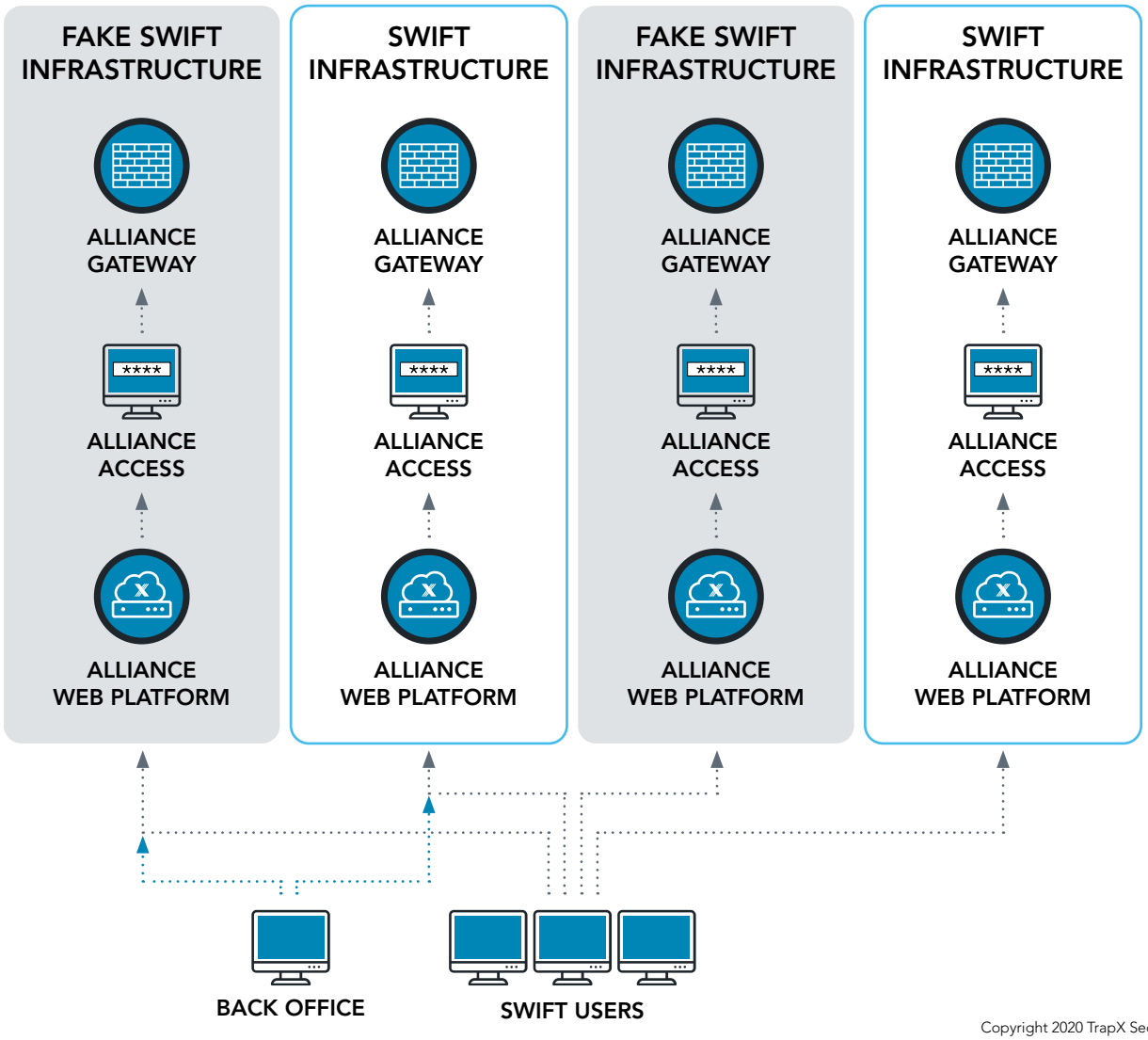
FIGURE 1: **CYBER ATTACK VECTORS ON SWIFT FINANCIAL NETWORK**



Deploy to the Cloud or On-Premise

DeceptionGrid is designed for rapid deployment, without network changes or disruption, to support the requirements of the largest global enterprises. Our automation enables your IT team to complete a full deployment in just a few hours.

FIGURE 2: **DECEPTIONGRID SURROUNDS AND PROTECTS REAL SWIFT ASSETS**

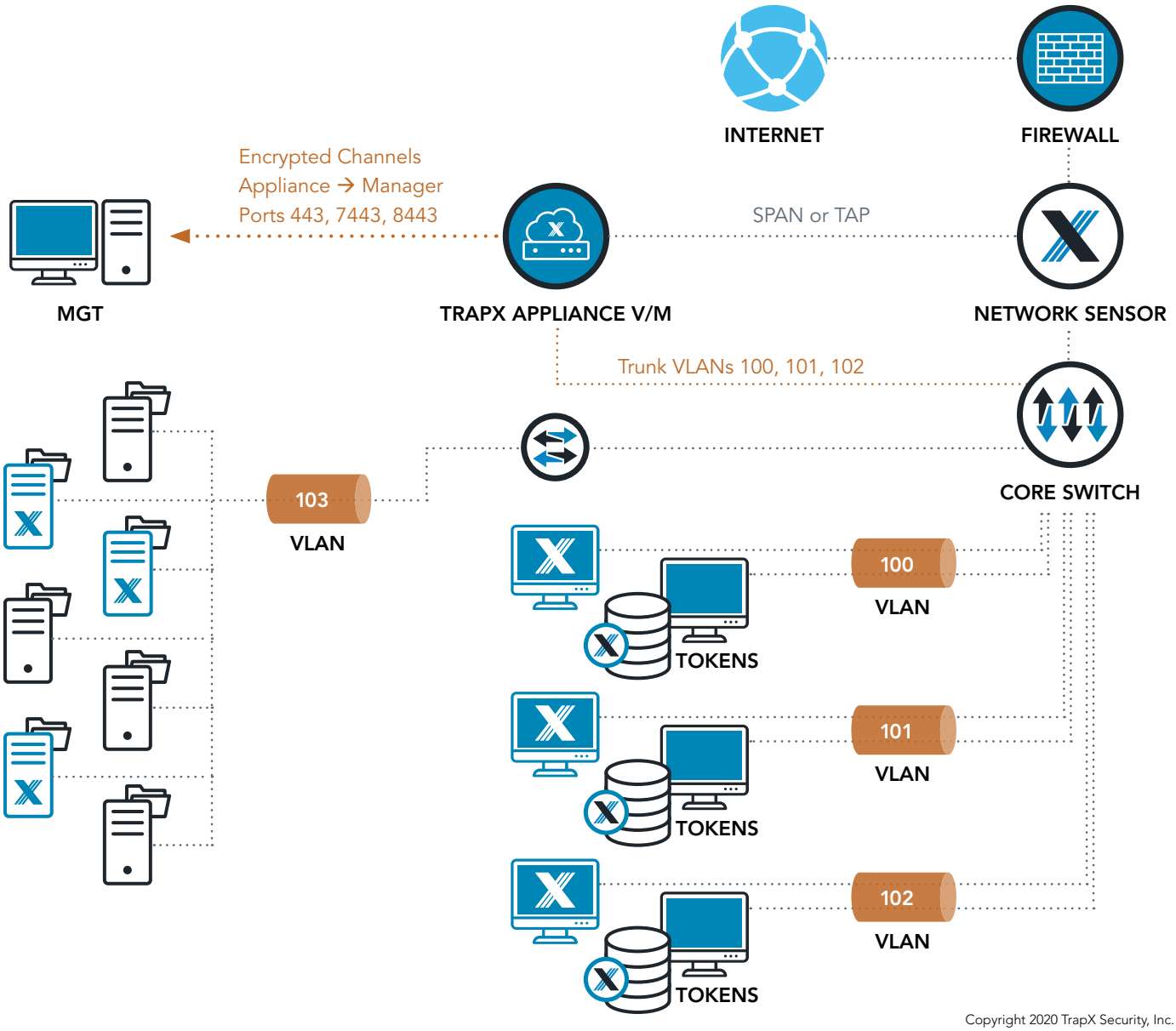


DeceptionGrid Functionality for SWIFT

DeceptionGrid automates the provision of hundreds to thousands of emulated traps (decoys) across your internal networks, with a small footprint and no network changes. Traps are designed to deceive attackers that have bypassed conventional perimeter-defense systems (FIGURE 2).

Typical traps include a variety of Windows workstations, Windows Servers, Linux systems, and network equipment. Also, specialized decoys such as SWIFT servers, Point of Sale (PoS) systems, automated teller machines (ATMs) and more, can be configured and deployed with a simple click of a button. Endpoint tokens (lures), such as fake SWIFT messages, credentials, and bookmarks are embedded within real IT assets, redirecting would be attackers back to the traps. This multi-layered approach is designed to expose, divert, and confuse cyber attackers at various phases of the attack lifecycle (FIGURE 3).

FIGURE 3: **DECEPTIONGRID ARCHITECTURE**



Fully Automated Forensics

Real-time automation isolates detected malware used by attackers and can forward it to advanced malware analysis systems. This malware analysis may be provided by the customer, based on our ecosystem integration, or TrapX can provide a cloud based analysis option.

The additional threat intelligence gained from these systems is combined with the trap activity to deliver a comprehensive assessment to your SOC team. An additional Network Intelligence Sensor (NIS) capability included with DeceptionGrid performs analysis of outgoing communications, combined with intelligence gathered from Trap activity, to construct a complete picture of compromised assets and attacker external activity.

Specialized decoys such as SWIFT servers, Point of Sale (PoS) systems, automated teller machines (ATMs) and more can be configured and deployed with the simple click of a button.

Attackers utilizing compromised endpoints to conduct reconnaissance are presented with the deception tokens.

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.