TRAPX
SECURITY

ACTIVE DEFENSE

TrapX DeceptionGrid™ + VMWare Carbon Black® EDR®

TrapX Security and VMWare Carbon Black® have joined forces to provide real-time visibility and threat detection, improved incident response and rapid threat containment.

The Joint Solution

VMWare Carbon Black EDR is a highly scalable, real-time Endpoint Detection and Response (EDR) solution with unparalleled visibility for top security operations centers and incident response teams.

This integration enables DeceptionGrid to provide actionable threat intelligence and initiate rapid threat containment actions or interdiction throughout the VMWare Carbon Black security ecosystem.

The joint solution offers customers early detection capabilities for advanced targeted attacks, Zero Day malware, and human threat actors operating on endpoints, along with the ability to quickly and proactively isolate compromised assets, thereby shutting down attackers in real time.

TrapX's DeceptionGrid

DeceptionGrid is based on TrapX's Deception-in-Depth architecture, which combines wide-ranging Deception capabilities to bait, engage, and trap attackers. Deception-Grid's multi-tier architecture presents Deception attack surfaces that match attacker activity adaptively, creating a tempting environment for attackers on various types of endpoints.
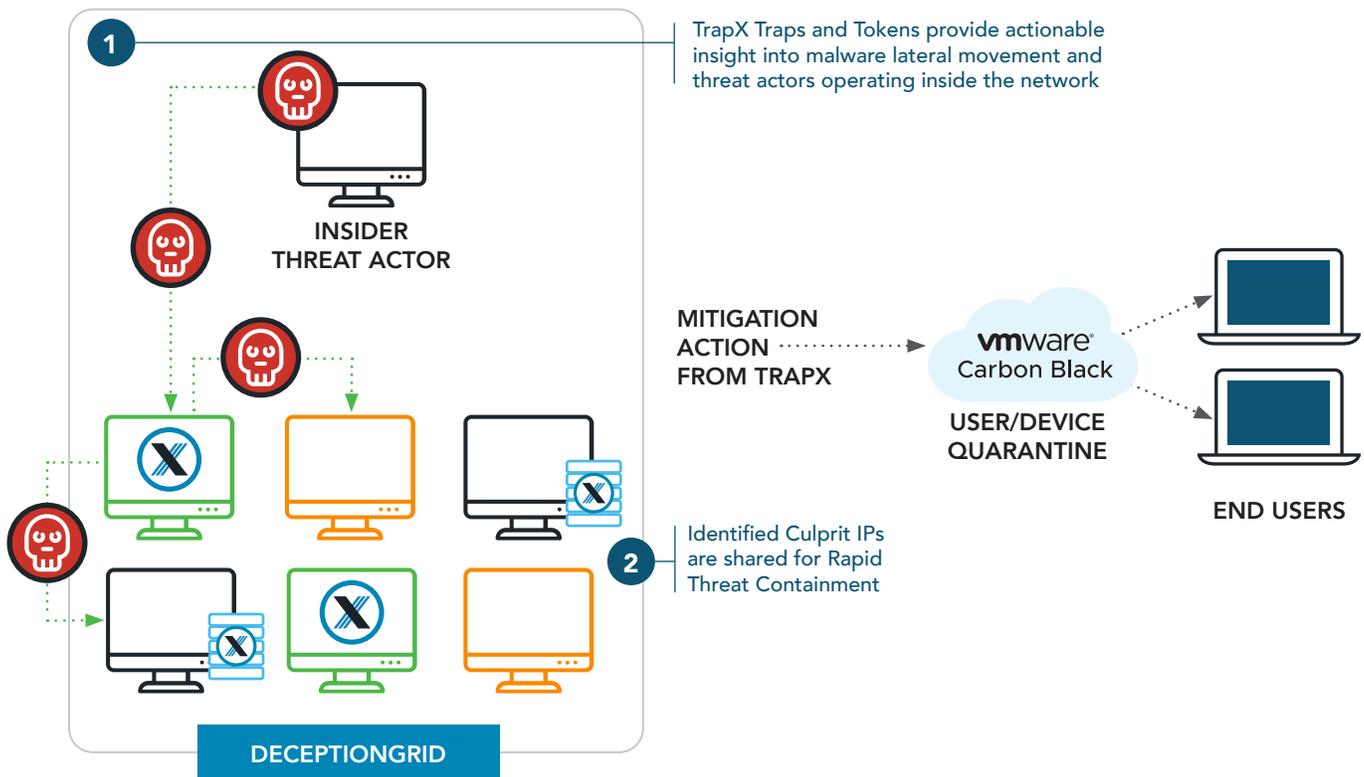
DeceptionGrid baits attackers by deploying automated, camouflaged tokens (lures) with the addition of medium and high-interaction traps (decoys) among authentic IT resources. The Traps appear identical in every way to real IT assets and connected Internet of Things (IoT) devices. The attacker sees an array of camouflaged traps which appear as tempting medical devices, servers, automated teller machines, retail point of sale workstations, switches, industrial control system components and more. DeceptionGrid even maintains a facade of convincing network traffic among the traps, thereby enhancing the illusion of authenticity and further engaging sophisticated attackers.

How will you know if one of your endpoints has been compromised?

How quickly will you know that your current security protections have failed?

How quickly can you isolate and shut down the attack and return to normal operations?

REAL-TIME ADAPTIVE PERCEPTION
RAPID THREAT CONTAINMENT

1 TrapX Traps and Tokens provide actionable insight into malware lateral movement and threat actors operating inside the network

INSIDER THREAT ACTOR

MITIGATION ACTION FROM TRAPX

vmware Carbon Black

USER/DEVICE QUARANTINE

END USERS

2 Identified Culprit IPs are shared for Rapid Threat Containment

DECEPTIONGRID

Copyright 2020 TrapX Security, Inc.

The Use Case

When malicious activity is identified by one of DeceptionGrid's sophisticated traps, an alert is sent automatically to VMWare Carbon Black EDR for isolation based on policy (risk-based) rules. Users can also isolate the endpoint manually with VMWare Carbon Black EDR through the TrapX Security Operations Console (TSOC).

After the malware or human threat actor is completely shut down, security teams can leverage VMWare Carbon Black EDR to take remediation actions, including enterprise-wide hash banning, drilling down to root cause, and the ability to create automated watch lists to alert on similar malicious techniques in the future.

Benefits for Your Organization by Deploying DeceptionGrid

» **Reduced time-to-breach detection**—DeceptionGrid detects malware and human threat actor movements inside the perimeter immediately.

» **Powerful situational awareness**—DeceptionGrid detects lateral movement that is often missed by other cyber tools and defenses.

» **Highest-fidelity alerts**—DeceptionGrid generates a very low volume of highly accurate alerts.

» **Deception-in-Depth integrated product platform**—Deception-in-Depth brings the industry's most comprehensive and powerful suite of Deception techniques together in one multi-tier architecture to bait, engage and trap attackers.

» **Ease-of-deployment**—DeceptionGrid deployment is simple and fast, using custom-built proprietary emulations and powerful automation.

» **Actionable intelligence**—Information flows across the integrated network to uncover hidden threats that target critical assets in both IT and OT infrastructures.

» **Deep visibility into internal networks**—The DeceptionGrid/VMWare Carbon Black joint solution provides augmented and actionable real-time visibility into lateral movement by attackers, targeting special endpoints including IoT, SCADA, ICS, PoS, and medical devices.

» **VMWare Carbon Black integration**—VMWare Carbon Black EDR integrates seamlessly with DeceptionGrid for fast deployment, trouble-free administration and automated rapid threat containment. TrapX also provides MSSP partners that bring the expertise and skills needed to supplement constrained in-house teams.

TRAPX
SECURITY

vmware® Carbon Black

TrapX Security is the leader in deception technology. Their DeceptionGrid solution rapidly detects, deceives, and defeats advanced cyberattacks and human attackers in real time. The DeceptionGrid also provides automated, highly accurate insight into malicious activity unseen by other types of cyber defenses. By deploying DeceptionGrid, you can create a proactive security posture, fundamentally halting the progression of an attack while changing the economics of cyberattacks by shifting the cost to the attacker. The TrapX Security customer-base includes Forbes Global 2000 commercial and government customers worldwide in sectors that include defense, healthcare, finance, energy, consumer products, and other key industries. www.trapx.com.

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit www.vmware.com/company

VMware and Carbon Black are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and other jurisdictions.

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.