The DeceptionGrid in the Microsoft Azure Cloud

Introducing DeceptionGrid into Microsoft Azure Cloud

Organizations everywhere are increasingly moving towards cloud based data centers to support on-demand, scalable computing infrastructures. TrapX’s famed DeceptionGrid now provides comprehensive support for Microsoft Azure Cloud.

DeceptionGrid support for the Microsoft Azure cloud, enables customers to enjoy the full benefits of a Deception in Depth architecture to deceive, detect and defeat attackers within their cloud-based deployments. The DeceptionGrid for Microsoft Azure provides unparalleled security and support for the most sensitive and critical applications deployed in your cloud. In addition, DeceptionGrid support for Microsoft Azure enables customers to deploy the TrapX Security Operations Console (TSOC) within the cloud to simplify management of their deception environment.

The DeceptionGrid dynamically baits, engages, and traps attackers across all areas within the Microsoft Azure cloud.

Protecting Hybrid Corporate Network / Cloud Environments
Automated deployment of deception Traps and Tokens provide comprehensive and unparalleled support for the Microsoft Azure cloud. In addition, lateral movement within the Microsoft Azure cloud, movement from internal networks into the Microsoft Azure cloud and lateral movement from another resource group in the event of a failed partition will be immediately detected. An alert will be sent immediately to the security operations center team. Ecosystem integrations will then shut down the attack to facilitate the rapid return to normal operations.

Visibility into the Cloud is Key

Hybrid environments in general, make life very difficult for security operations teams. In today’s hybrid environment, the question isn’t whether attackers will penetrate your in-house and cloud-based networks, but when and how often? Attackers are using increasingly sophisticated techniques to penetrate the most robust perimeter and endpoint defenses and gain access to your internal networks.

TrapX’s Deception in Depth architecture addresses these important questions along with the powerful DeceptionGrid’s technology to deceive, detect, and defeat sophisticated attackers at every step. The DeceptionGrid provides accurate detection and extensive visibility into the lateral movement of threats within the evolving cloud attack surface. This visibility closes the gap in attacker detection. This full and unparalleled visibility to attacker movement also enables you to rapidly detect an intruder in your Microsoft Azure cloud and to isolate and shut down the attacker.
The Broadest Deception Capability for Your Cloud

DeceptionGrid offers a full suite of deception techniques, including the automated deception Tokens (lures) as well as medium and high-interaction Traps (decoys). It baits attackers by deploying camouflaged Traps and Tokens among your actual IT resources. The DeceptionGrid’s Traps appear identical in every way to your operational IT assets and your 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 the DeceptionGrid’s Traps. When cyber attackers penetrate an enterprise network, they move laterally to locate high-value targets. The DeceptionGrid dynamically 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. The DeceptionGrid integrates with key elements of the network and security ecosystem to contain attacks and it enables a quick return to normal operations.

DeceptionGrid Automation Supports Rapid Deployment and Ease of Operation

The DeceptionGrid was developed to overcome the limitations of conventional perimeter defenses, signature-based tools, intrusion-detection methods, and honeypots. The DeceptionGrid scans your existing network and provisions hundreds to thousands of deception components within your Microsoft Azure cloud. Deception Tokens, or lures, which appear as ordinary files and databases, are embedded within real IT assets. Traps are decoys that emulate servers, workstations, network switches, and more.

High Accuracy and Minimal Alerts Keep Your Cloud Safe

In large enterprises, conventional cyber-defense technologies, such as firewalls and endpoint security, can generate thousands or even millions of alerts daily, overwhelming cybersecurity operations. Unfortunately, just one successful penetration can compromise an entire network. The DeceptionGrid takes a different approach: Unlike firewalls and endpoint security methods, which generate alerts based upon probability, The DeceptionGrid alerts are binary. Attackers either attempt to engage the traps or they do not. If they touch a Trap, you know with nearly 100 percent certainty that it’s an attack.

TrapX’s Partner Ecosystem

The DeceptionGrid provides the advanced business analytics and smart cloud intelligence needed to correlate threats across our partner ecosystem. TrapX empowers partner organizations to make data driven security decisions, better engage customers, manage customer environments and gain a distinct competitive advantage.
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.

Benefits For Your Enterprise By Deploying The DeceptionGrid

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

» **Powerful situational awareness** – The DeceptionGrid detects lateral movements that are often missed by other types of cyber tools and defenses.

» **Highest-fidelity alerts** – The 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** – The DeceptionGrid’s deployment is simple, fast and uses our proprietary emulations and powerful automation.

» **Actionable intelligence** – Information flows across our integrated network to leverage discovery and uncover hidden threats that target critical assets in the cloud, IT and OT infrastructures.

» **Deep visibility into internal networks** – The DeceptionGrid provides augmented and actionable real-time visibility into lateral movements from attackers, targeting special turnkey systems such as IoT, SCADA, ICS, POS, and medical devices.

About TrapX Security

TrapX Security is the leader in deception-based cybersecurity defense. Their DeceptionGrid solution rapidly detects, deceives, and defeats advanced cyber attacks 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 cyber attacks 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. Learn more at www.trapx.com