TRAPX SECURITY

PRODUCT BRIEF

DECEPTION TECHNOLOGY
for KVM Virtualization

An Introduction to DeceptionGrid™

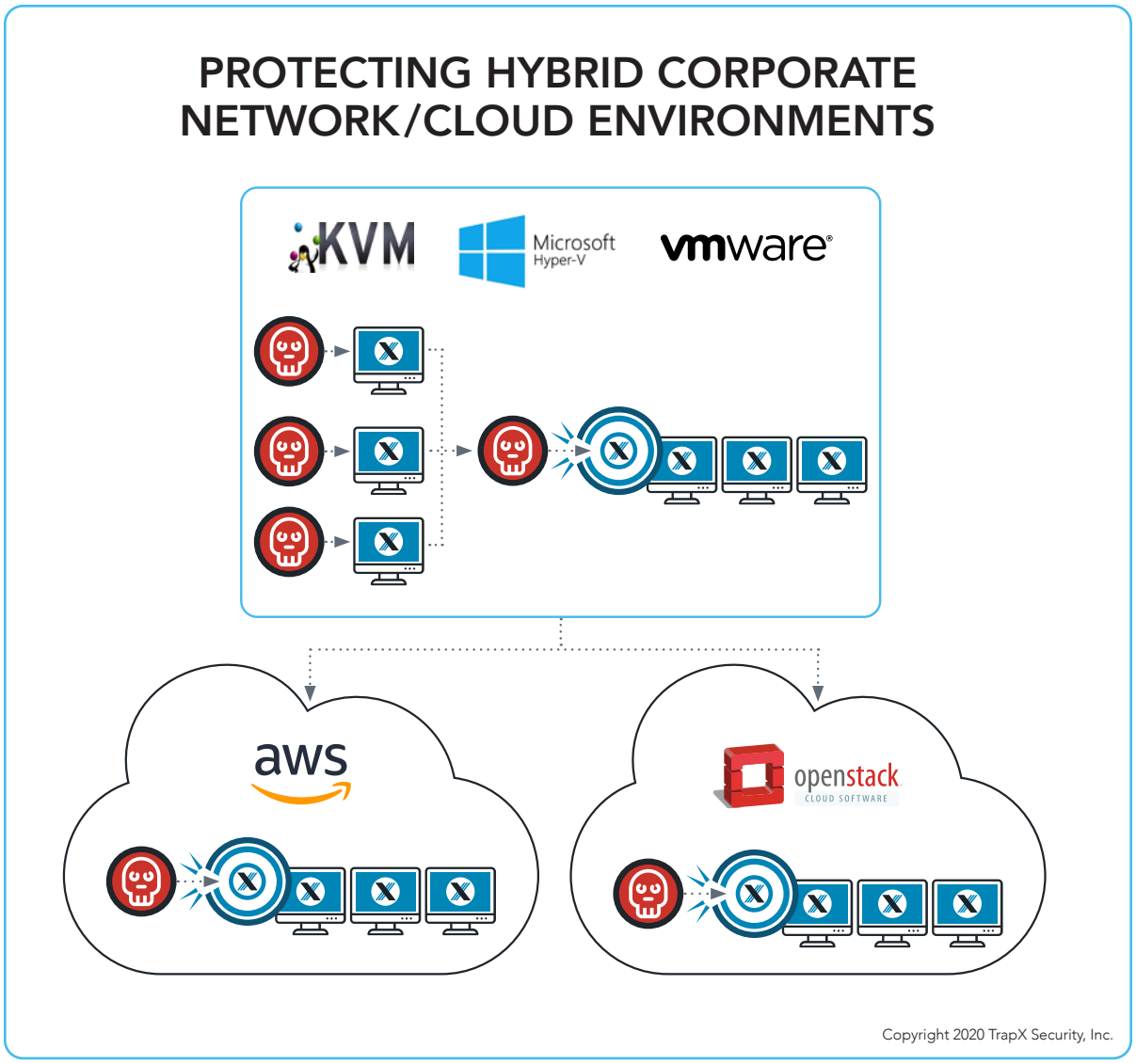
Organizations globally are increasingly moving towards cloud-based data centers to support an on-demand, scalable computing infrastructure. By providing comprehensive support for the Kernel-based Virtual Machine (KVM) hypervisor used in large scale OpenStack Linux environments, TrapX customers can enjoy the full benefits of a Deception-in-Depth architecture to deceive, detect, and defeat attackers within their cloud-based deployments. DeceptionGrid for KVM OpenStack provides unparalleled security and support for the most sensitive and critical applications in both private and public clouds.

DeceptionGrid dynamically baits, engages, and traps attackers across all areas within the KVM cloud.

Customers deploy DeceptionGrid within the cloud to simplify management of their Deception environment. Automated deployment of deceptive traps and tokens provides comprehensive coverage for KVM OpenStack private cloud instances that can be deployed in a matter of minutes. Lateral movement within the cloud, movement from internal networks into the cloud, and lateral movement from another user in the event of a failed partition is detected immediately, and an alert is sent to the security operations center team. Ecosystem integrations shut down the attack to facilitate a rapid return to normal operations.

Visibility is Key

Today's hybrid environments make it much more difficult for security operations teams. Attackers are using increasingly sophisticated techniques to penetrate the most robust perimeter and endpoint defenses and gain access to your internal networks. The question isn't whether attackers will penetrate your in-house or cloud-based networks, but when and how often. TrapX's Deception-in-Depth architecture addresses these challenges with powerful technology to lure and then engage sophisticated attackers. 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 and enables SOC teams to rapidly detect an intruder in the cloud, isolate them, and shut down the attack.



The Broadest Deception Capability for Your Cloud

DeceptionGrid is a complete Deception platform, including automated tokens (lures) as well as medium- and high-interaction traps (decoys). It baits attackers by deploying camouflaged traps and tokens among actual IT resources. Traps appear identical in every way to IT assets or 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 traps. When cyber attackers penetrate an enterprise network, they move laterally to locate high-value targets. DeceptionGrid dynamically baits, engages, and traps attackers across all areas of the network. Just one touch of DeceptionGrid by the attacker sets off a high-confidence alert. DeceptionGrid integrates with key elements of the network and security ecosystem to contain attacks and enable a return to normal operations.

Automation Supports Rapid Deployment and Ease of Operation

DeceptionGrid was developed to overcome the limitations of conventional perimeter defenses, signature-based tools and intrusion-detection methods, and honeypots. Our multi-tier Deception-in-Depth architecture includes powerful automation for scalability, which is essential to supporting large enterprises and government systems without the high cost of configuring individual Deception nodes manually. DeceptionGrid scans your existing network and provisions hundreds-to-thousands of Deception components within your KVM OpenStack 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.

DeceptionGrid takes a different approach. Unlike firewalls and endpoint security methods, which generate alerts based upon probability, DeceptionGrid alerts are binary. Attackers either attempt to engage our traps or they don't. If they do touch a Trap, you'll know with nearly 100 percent probability that it's an attack.

High Accuracy and Minimal Alerts Keep Your Cloud Safe

In large enterprises, conventional cyberdefense 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. DeceptionGrid takes a different approach. Unlike firewalls and endpoint security methods, which generate alerts based upon probability, DeceptionGrid alerts are binary. Attackers either attempt to engage our traps or they don't. If they do touch a trap, you'll know with nearly 100 percent certainty that it's an attack.

Partner Ecosystem

DeceptionGrid provides the advanced business analytics and smart cloud intelligence needed to correlate threats across our partner ecosystem. We empower partner organizations to make data-driven security decisions, better engage customers, optimize 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.

How do you know if an attacker has penetrated your network? How can you identify them quickly? What are their intentions? How quickly can you stop an attack and return to normal operations?

Key Benefits of DeceptionGrid

» **Targets the new breed of cyber attackers.** Deception technology finds sophisticated attackers that existing vendors cannot detect and that may already be inside your network.

» **Reduces or eliminates economic losses.** Accurate and rapid detection reduces the risk of economic loss due to destruction of enterprise assets, theft of data, and overall impact to business operations.

» **Reduces time to breach detection.** Advanced real-time forensics and analysis, coupled with high accuracy, uniquely empowers your security operations center to take immediate action to disrupt all attacks within the network perimeter.

» **Comprehensive visibility and attack surface coverage.** Defense-in-Depth provides comprehensive visibility into internal networks, revealing attacker activity and intentions, and terminating the attack.

» **Supports compliance processes.** Makes it easier to meet PCI and HIPAA data breach laws, along with other regulatory requirements in various countries.

» **Lowest cost of implementation.** Deception-in-Depth provides the greatest breadth and depth of Deception technology at the lowest cost to your enterprise.

» **Compatible with existing investments.** Deception technology easily integrates with your existing security investments, including SIEM, SOAR, and endpoint monitoring.

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.