Deception in the Amazon EC2 Cloud

An Introduction to DeceptionGrid

DeceptionGrid now provides comprehensive support for Amazon’s EC2 Cloud. Organizations globally are increasingly moving towards cloud-based data centers to support on-demand, scalable computing infrastructure. DeceptionGrid support for the Amazon EC2 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. DeceptionGrid for Amazon EC2 provides unparalleled security and support for the most sensitive and critical applications deployed in your Amazon cloud.

DeceptionGrid support for Amazon EC2 enables customers to deploy the TrapX administration and console within the cloud to simplify management of their deception environment. Automated deployment of deception Traps and Tokens provide comprehensive and unparalleled support for AWS private cloud instances. Lateral movement within the AWS cloud, movement from internal networks into the AWS cloud, and lateral movement from another VPC user in the event of a failed partition is detected and an alert is sent to the security operations center team immediately. Ecosystem integrations shut down the attack to facilitate the rapid return to normal operations.

Visibility into the Cloud is Key

Hybrid environments make it much more 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 Deception in Depth architecture addresses these important questions with powerful DeceptionGrid technology to deceive, detect, and defeat sophisticated attackers at every step. 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 enables you to rapidly detect an intruder in your Amazon EC2 cloud and to isolate and shut down the attacker.
The Broadest Deception Capability for Your Cloud

DeceptionGrid is 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. Our 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 our Traps. When cyberattackers 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 the 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.

DeceptionGrid 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 multitier 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 Amazon 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 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, we 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, 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.

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, we know with nearly 100 percent probability that it’s an attack.
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 cyberattackers. 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 coverage. Defense in Depth provides comprehensive visibility into internal networks, revealing attacker activity and intentions, and terminating the attack.

» Improves compliance. 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 can integrate with your existing operation.

ABOUT US

TrapX has created a new generation of deception technology that provides real-time breach detection and prevention. Our field proven solution deceives would-be attackers with turn-key decoys (traps) that “imitate” your true assets. Hundreds or thousands of traps can be deployed with little effort, creating a virtual mine field for cyberattacks, 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. Uniquely our automation, innovative protection for your core and extreme accuracy enable us to provide complete and deep insight into malware and malicious activity unseen by other types of cyber defense. TrapX Security has many thousands of government and Global 2000 users around the world, servicing customers in defense, health care, finance, energy, consumer products and other key industries.