TRAPX SECURITY

White Paper

Enabling the New World of Cloud and Containers

The shift to remote or hybrid work environments has accelerated cloud adoption and digital transformation. The Cloud offers security advantages and disadvantages over on-premise IT. Security is relieved of protecting a physical environment. Under the shared responsibility model, you are still responsible for protecting sensitive data, user access, VM's, containers and application code and access. This presents an entirely new challenge — keeping pace with a far more dynamic environment that traditional tools and practices simply cannot address.

	On-prem	IaaS	PaaS
Application user access management	◉	◉	◉
Application specific data assets	◉	◉	◉
Application specific logic and code	◉	◉	◉
Application / platform software	◉	◉	◉
Operating system and local networking	◉	◉	◉
Virtual Machine / server instance	◉	◉	◉
Visualization platform	◉	◉	◉
Physical hosts / servers / compute	◉	◉	◉
Physical and perimeter network	◉	◉	◉
Physical datacenter environment	◉	◉	◉

CSP Responsibility ◉ Your Responsibility ◉

Figure 1: Cloud Security Alliance, Shared Responsibility Model

Early Cloud adopters soon discovered the disparity between traditional controls, configuration and change management, and the highly dynamic nature of cloud-based resources. They also learned that the Cloud offers attackers new ways to execute and new places to hide.

DevOps and containers take the dynamic and ephemeral nature of Cloud resources to a new level. Containers can be developed and deployed quickly. They also expand and contract to consume or stop consuming resources on demand very quickly.

Where VMs can be spun up and down in minutes, containers can be spun up and down in seconds. Containers are agile, evasive and, since they live in open environments, easily accessed by attackers. Your challenge is to match container dynamics and prevent them from being exploited for data theft or weaponized for DoD and Cryptojacking campaigns such as Hildegard.

DeceptionGrid™ Reduces Risk in AWS Environments

TrapX DeceptionGrid has a twofold effect on risk reduction — simultaneously reducing the likelihood of an attack on a real asset while closing the gap between an attacker's meantime to collection and your meantime to response.

Reduced Threat Frequency

Adding decoys to the attack surface decreases the likelihood that a threat event will effect a real asset.

Reduced Materiality

Attacks on traps deliver high-fidelity alerts that speed response to minimize an incident's impact.

Reducing Threat Exposure

When an attacker accesses an AWS environment that is void of deceptive assets, it is 100% certain that every VM and every container is real. Even if an attack is discovered and shut down, the attacker can apply what they've learned when they reestablish a foothold. With DeceptionGrid™ every asset is *not* real. TrapX patented technology surrounds VMs and containers with traps that are indistinguishable from real assets. One VM/pod shadowed by one trap reduces the likelihood of an attack on that VM/pod by 50%. More traps in the path of that asset reduces the likelihood more. Simply put, more traps equal less risk.

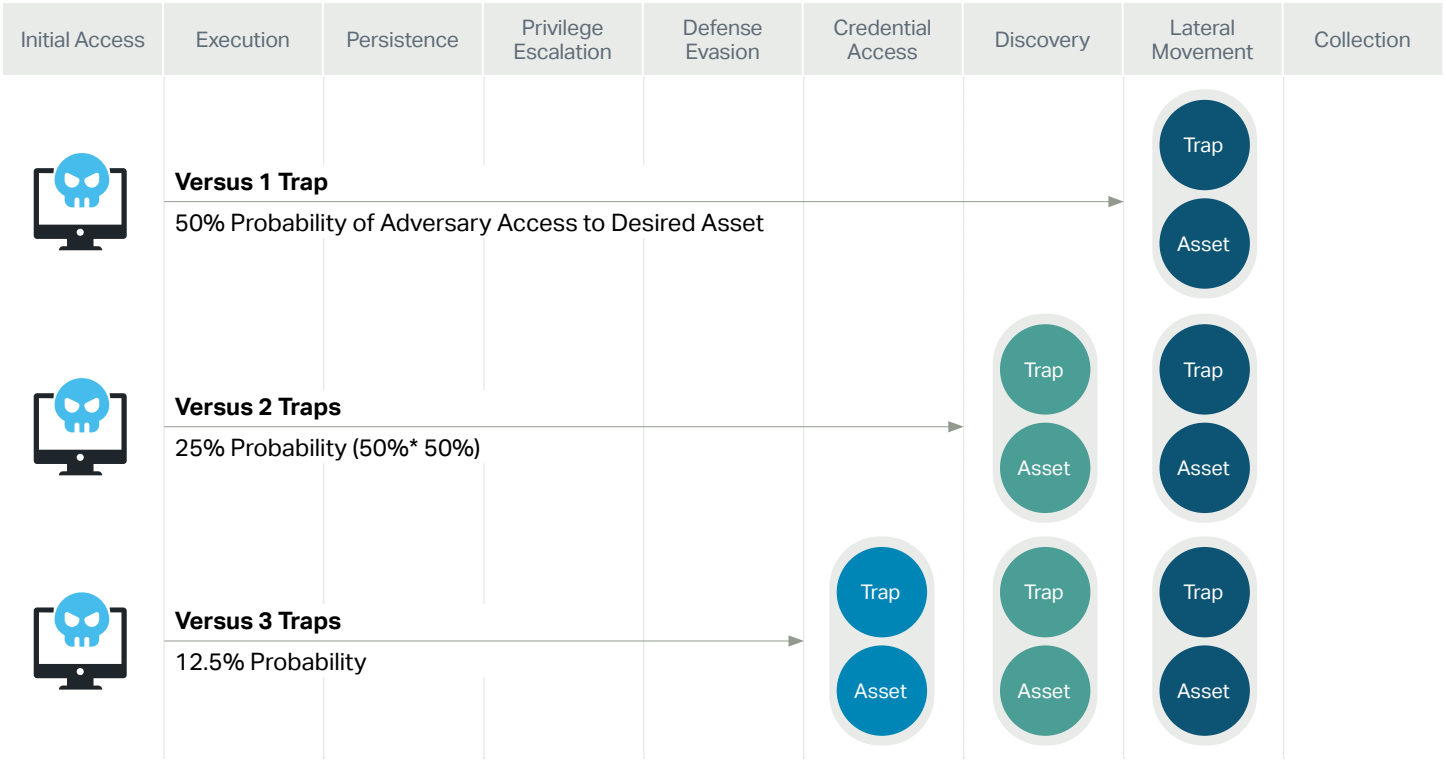

Figure 2: Simple Threat Frequency Model

Reducing Meantime to Response

Traps also reduce risk by closing the gap between attack speed and response speed. Traps can only be seen by attackers — they are invisible to legitimate users and systems. Four things happen immediately and simultaneously when an attacker engages a trap. The trap interacts as a real asset occupying their time. The trap feeds the attacker false data that can be traced back to them. The attacker harmlessly shares techniques and location and a high-fidelity alert triggers remediation. Since traps are only accessible to attackers, it is highly unlikely (less than 1%) that the alerts are false positive. These early warnings spearhead context derived from SIEM and other sources to reduce alert volume and speed response. The combination of attack delay and response acceleration closes the attack/response gap to reduce the impact of incidents once they occur.

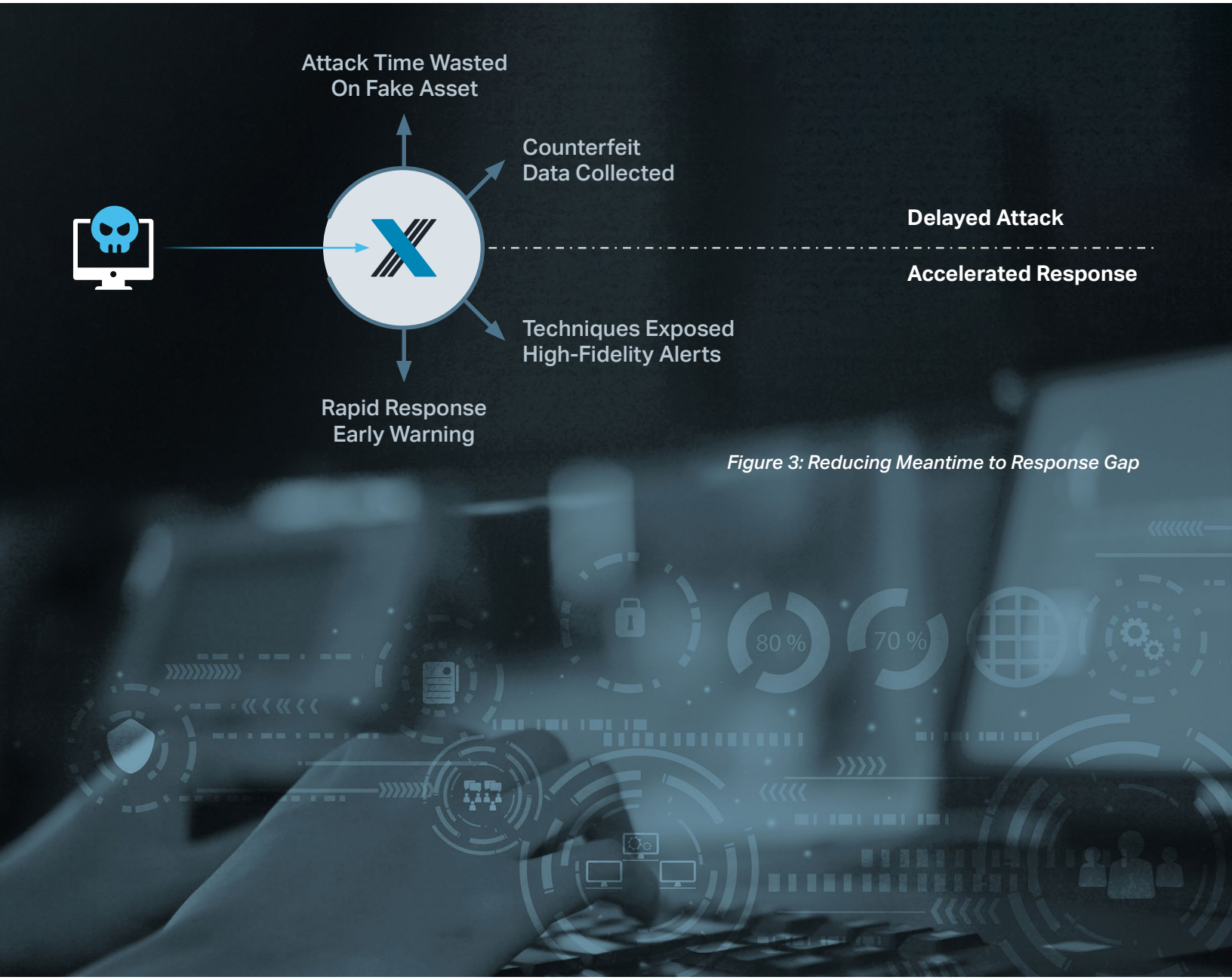

Figure 3: Reducing Meantime to Response Gap

Protecting Virtual Machines

DeceptionGrid runs natively within AWS providing automated Trap deployment to protect private cloud instances. Lateral movement within the AWS cloud, a breach from an external facing asset (e.g., webserver), movement from internal networks into the AWS cloud, and lateral movement from another VPC user alerts the security team immediately. DeceptionGrid alerts are tagged with MITRE ATT&CK techniques so you can track incidents back to attack groups and assess the trap deployment against the MITRE ATT&CK Kill Chain.

The DeceptionGrid Active Defense Scorecard is the industry's first dynamic heatmap that enables you to test and validate your coverage without disrupting the production environment or enlisting red teams.

Ecosystem integrations then shut down the attack to facilitate the rapid return to normal operations.

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection
T1190: Exploit Public-Facing Application	T1098: Account Manipulation	T1078: Valid Accounts	T1562: Impair Defenses	T1110: Brute Force	T1078: Account Discovery	T1530: Data from Cloud Storage Object
T1199: Trusted Relationship	T1136: Create Account		T1578: Modify Cloud Complete Infrastructure	T1552: Unsecured Credentials	T1530: Cloud Infrastructure Discovery	T1074: Data Staged
T1078: Valid Accounts	T1525: Implant Container Image		T1535: Unused/Unsupported Cloud Regions		T1538: Cloud Service Dashboard	
	T1078: Valid Accounts		T1078: Valid Accounts		T1526: Cloud Service Discovery	
					T1046: Network Service Scanning	
					T1069: Permission Groups Discovery	
					T1518: Software Discovery	
					T1082: System Information Discovery	
					T1049: System Network Connections Discovery	

Figure 4: DeceptionGrid Coverage of the MITRE ATT&CK AWS Matrix

Anatomy of an Attack: Defending AWS

DeceptionGrid was developed to overcome the limitations of conventional signature-based tools and intrusion-detection, and honeypots. DeceptionGrid architecture is built for speed, agility and scale. Scanning the Amazon cloud environment and provisioning hundreds-to-thousands of traps with minimal manual effort. These traps emulate a variety of automation servers, operating systems and platforms such as Jenkins, Ubuntu and Gitlab delivered as Machine Images or containers. Deception files, data, browser history and credentials, are integrated to draw the attack away from real assets and toward traps. Our solution compliments AWS Security Best Practices and is integrated with the leading AWS Security Competency Partners.

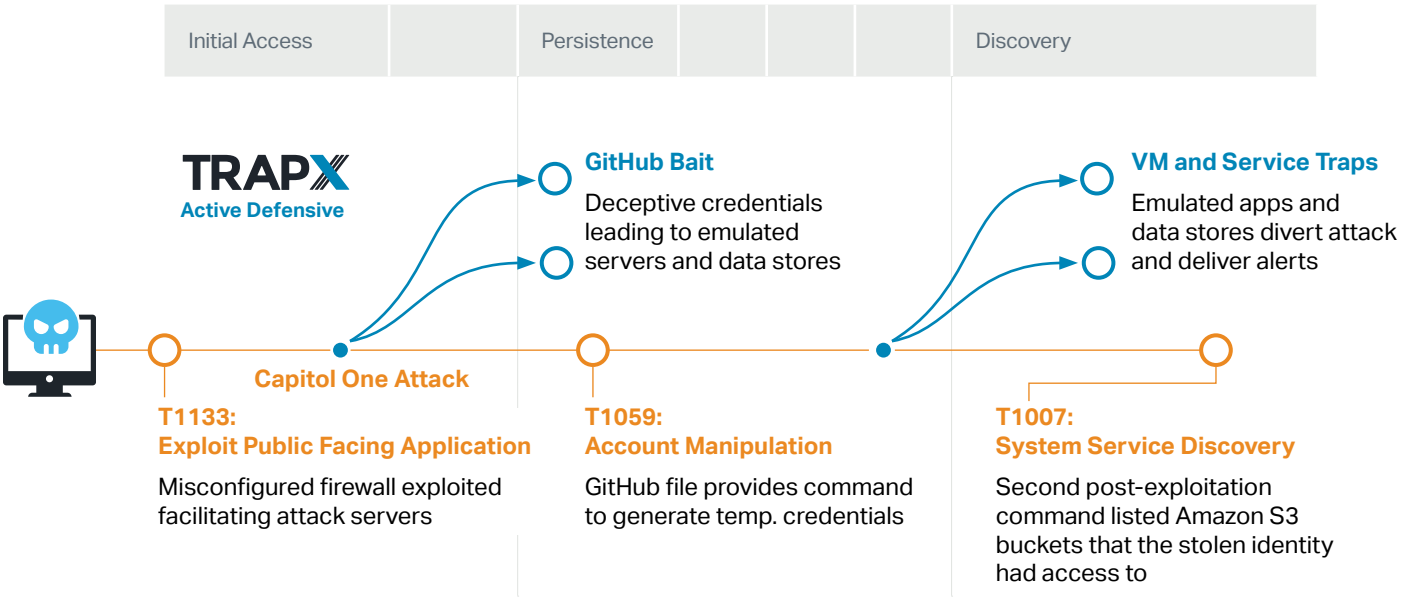

Figure 5: How TrapX Can Disrupt Capital One Attack Techniques

Protecting Containerized Environments

Attacks are following the migration to cloud and container environments to tap a wealth of sensitive information and computing resources. Groups such as TeamTNT, known for stealing AWS credentials and deploying malicious Docker container images, now enter Kubernetes environments by exploiting misconfigured nodes. Once in, they scan the internal network and rather than move laterally from system to system, they move laterally to other vulnerable nodes to exploit underlying hosts and drain you of the resources you are paying for — compromising the performance of your critical applications. In the end, attackers are simply taking advantage of a new and more open channel with the same end goals in mind and their attack sequence should strike a familiar chord.

- Exploit vulnerable entry point
- Establish a C2 connection
- Hide malicious process behind a known process name
- Encrypt malicious payload inside a binary

DeceptionGrid runs natively in a Kubernetes environment and deploys traps that hide real Kubernetes containers in a crowd of fakes which trigger an alert once the attacker or malware interacts with it.

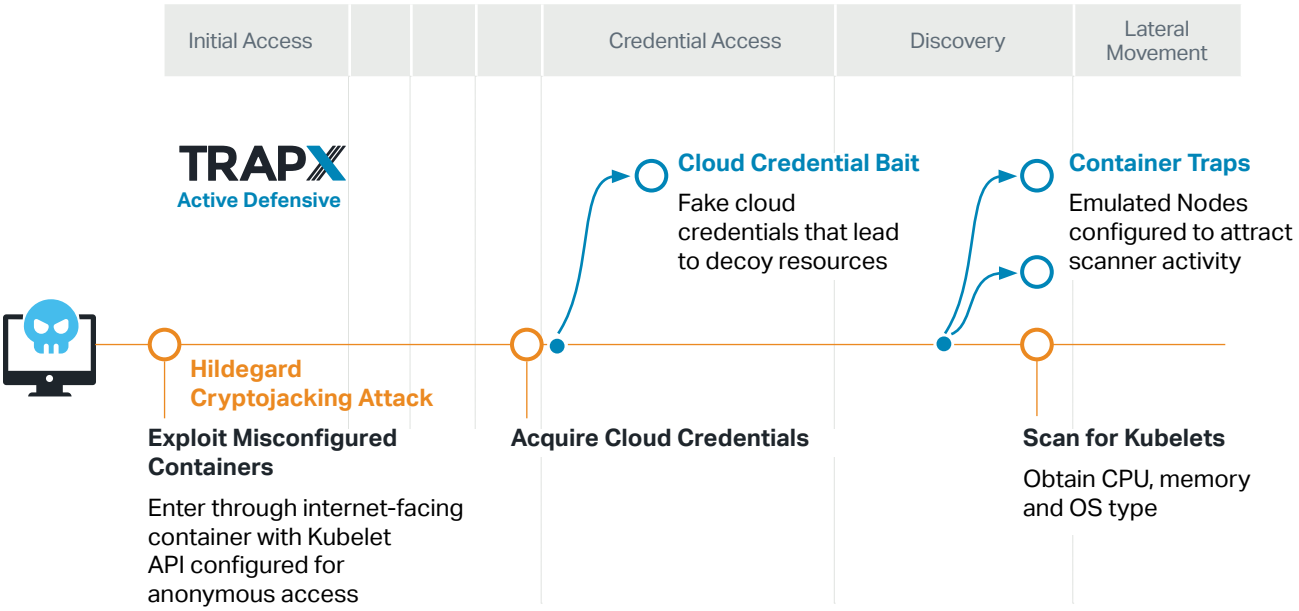

Figure 6: How TrapX can disrupt techniques used in Hildegard Cryptojacking attack

Conclusion

VMs and Containerized environments introduce a level of sprawl and dynamic change that security simply cannot match with traditional tools and methods. From the beginning, attackers have used deception to gain the upper hand. Today security has the opportunity to do the same — leveraging modern deception technology to simultaneously impose uncertainty and risk on the attacker, while reducing risk and improving visibility within their AWS environment.

DeceptionGrid™ Benefits

- Patented emulation technology for easy, rapid deployment and change at scale
- 100% Passive — no agents or resources required
- Non-disruptive visual trap testing and validation against MITRE ATT&CK
- Wide coverage of IT and IoT devices
- Automatically triggers mitigation action in security eco-system for fast remediation
- A Pioneer with proven track record of over 200 production customers
- Dozens of case studies and successful bake-offs

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 protects AWS with real-time threat detection and prevention. Our field proven solution deceives would-be attackers with traps that are indistinguishable from real assets. Hundreds or thousands of traps can be deployed with little effort, creating a virtual mine field for cyberattacks, providing 99% true alerts to any malicious activity immediately. Our solutions enable our customers to rapidly isolate, fingerprint and disable new zero-day attacks and APTs in real-time. Automation, innovative protection and extreme accuracy provides complete and deep insight into malware and malicious activity unachievable by other types of tools. 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.

For more information, visit **www.trapx.com**.