SOLUTION BRIEF

Threatwise™ 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 provides new efficiencies and considerations for businesses, such as enhanced security capabilities. As the shared responsibility model is a standard for popular cloud vendors, understanding it is key for a robust security strategy. According to the shared responsibility model you are still responsible for protecting sensitive data, user access, VMs, 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.

Early Cloud adopters soon discovered the disparity between traditional controls, configuration and change management, and the highly dynamic nature of cloud-based resources.

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. The customers' challenge is to match container dynamics and prevent them from being exploited for data theft or weaponized for DDoS and Cryptojacking campaigns such as Hildegard.

	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

THREATWISE REDUCES RISK IN AWS ENVIRONMENTS

Threatwise 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	Reduced Materiality
Adding decoys to the attack surface decreases the likelihood that a threat event will effect a real asset.	Attacks on threat sensors deliver high-fidelity alerts that speed response to minimize an incident's impact.

REDUCING THREAT EXPOSURE

When an attacker accesses an AWS environment 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 reestablishing a foothold. With Threatwise, not every asset is real. Threat sensors are replicates of real network assets that are spun up in bulk around cloud, on-premises, and SaaS instances to detect, divert, and alarm malicious intent and activity. Commvault's patented deception technology surrounds VMs and containers with decoys, or threat sensors, that are indistinguishable from real assets. One VM/pod shadowed by one threat sensor reduces the likelihood of an attack on that VM/pod by 50%. More threat sensors in the path of that asset reduces the likelihood more. Simply by increasing threats sensor coverage per real asset reduces risk.

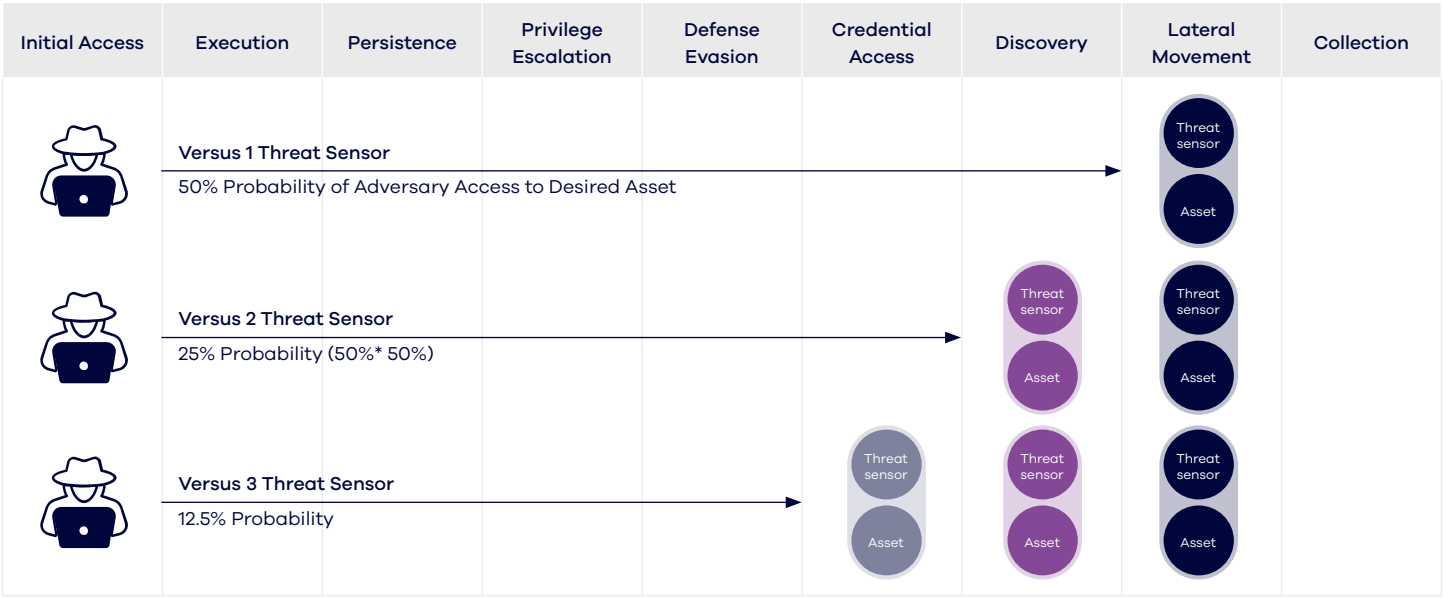

Figure 2: Simple Threat Frequency Model

REDUCING MEANTIME TO RESPONSE

Threatwise also reduces risk by closing the gap between attack speed and response speed. Threat sensors 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 sensor. First, it interacts as a real asset occupying their time. Secondly, the attacker is fed false data that can be traced back to them. Thirdly, threat intelligence collecting used techniques and the location of the threat actor. And lastly, immediate alerts are sent out to key stakeholders and security tools. Since threat sensors are only accessible to attackers, it is

highly unlikely (less than 1%) that the alert is a false positive. These early warnings spearhead context 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.

THREATWISE EARLY WARNING SYSTEM

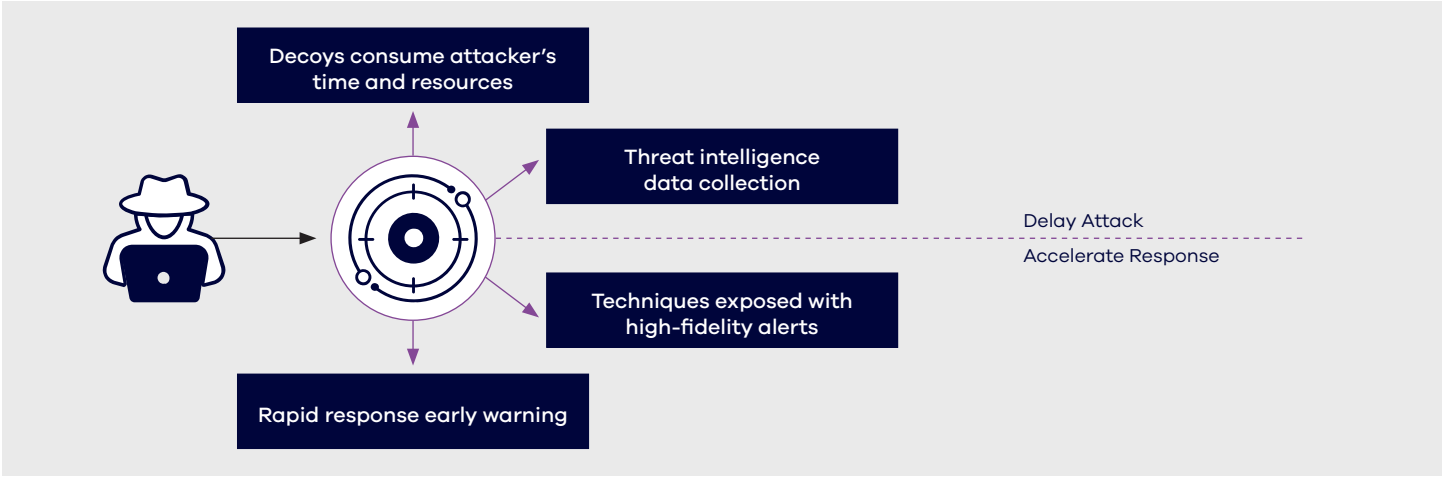

Figure 3: Reducing Meantime to Response Gap

PROTECTING VIRTUAL MACHINES

Threatwise runs natively within AWS, providing bulk threat sensor deployment to protect private cloud instances. Reconnaissance within AWS instances, a breach from an external facing asset (e.g., webserver), movement from internal networks into the AWS environments, and lateral movement from another VPC user alerts the IT and IT security teams immediately. DeceptionGrid alerts are tagged with MITRE ATT&CK techniques so you can track incidents back to attack groups.

The Threatwise 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.

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

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

ANATOMY OF AN ATTACK: DEFENDING AWS

Threatwise was developed to overcome the limitations of conventional signature-based tools, intrusion detection, and honeypots. Its architecture is built for speed, agility, and scale. Scanning the Amazon cloud environment and provisioning hundreds-to-thousands of threat sensors with minimal manual effort. These sensors mimic a variety of 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. Threatwise complements AWS Security Best Practices and is integrated with the leading AWS Security Competency Partners.

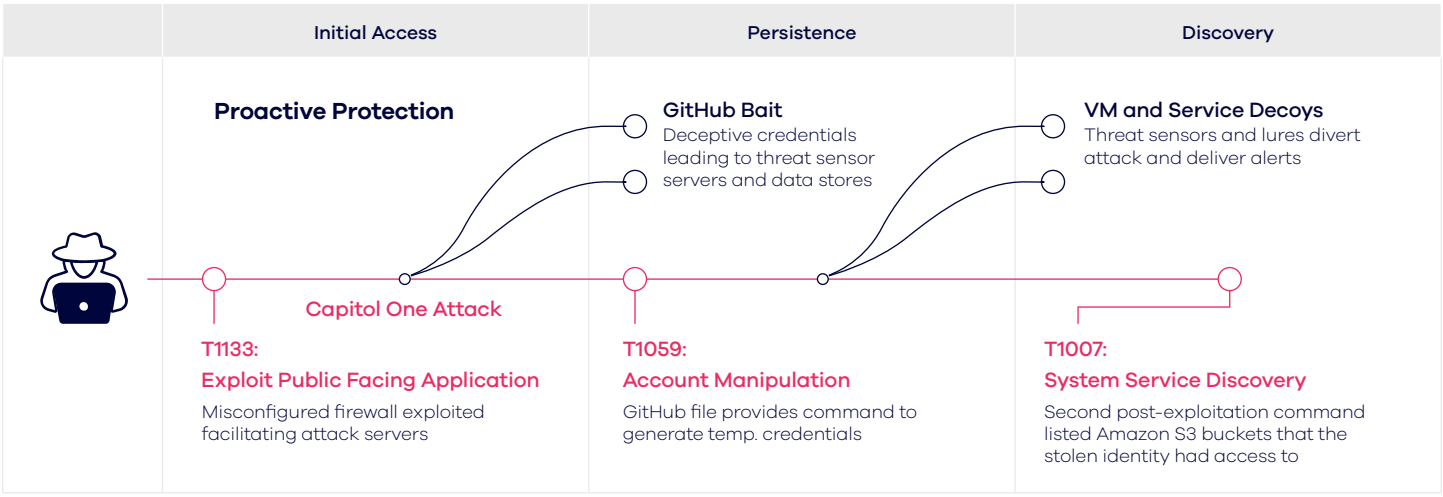

Figure 5: How Threatwise Can Disrupt Capital One Attack Techniques

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 simply take 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

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

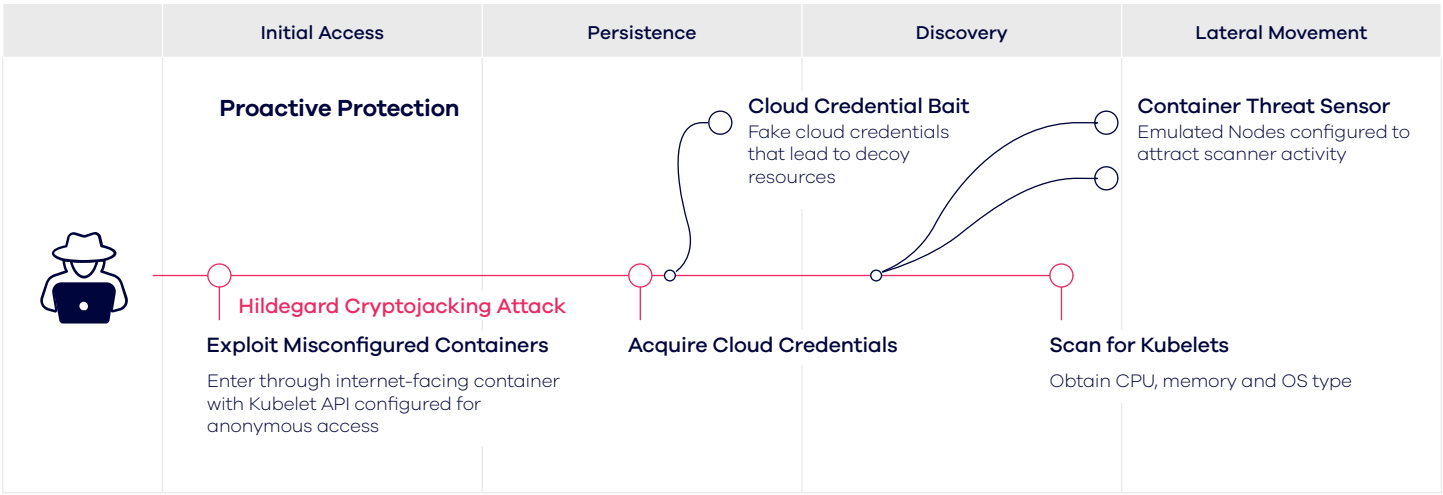

Figure 6: How Threatwise can disrupt techniques used in Hildegard Cryptojacking attack

CONCLUSION

VMs and Containerized environments introduce 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.

THREATWISE BENEFITS

- Early threat detection of advanced attacks and stealth techniques
- Highly scalable across the entire surface area
- Lightweight and agelessness solution operating non-disruptive
- Wide coverage, including testing and validation against MITRE ATT&CK
- Seamless SIEM integration

Learn more about Metallic data backup solutions for Kubernetes, visit **commvault.com/free-trial**