eBOOK

Commvault® Cloud Threatwise™

# Critical Deception Use Cases

Commvault

# Introduction

This eBook takes a thorough look at the principles of cyber deception from a theoretical, practical, and technical perspective. It will help the reader to understand it's components, the value that it provides to an organization, and how to implement an advanced deceptive network that evolves.

## SCIENTIFIC FRAMEWORK

The MITRE corporation has been a signpost in the security field. Their database of known vulnerabilities (CVE) and mapping of cyber criminals' tactics, techniques, and procedures (MITRE ATT&CK) are indispensable resources. Until recent days these frameworks are a go-to place for the cybersecurity workforce, but security providers have struggled to draw a line between their solutions and the researchers' findings. In efforts of MITRE to round off their compilation of cybersecurity and support organizations' defensive efforts, new frameworks of countermeasures are now publicly available (MITRE D3FEND and MITRE Engage). Both mappings include deceptive multiple approaches, demonstrating how powerful deception technology is for the mitigation of cyber risk. The MITRE D3FEND framework, which maps applied defense techniques to the TTPs of MITRE ATT&CK, will be referenced throughout this eBook and is the foundation for Commvault's data-minded deception deployment best practices.


The pressure for IT and IT Security teams to install effective defenses against threat actors is increasing as costs associated with attacks are climbing. The emphasis concentrates on the effectiveness of the security strategy, raising the question of which attacks these teams can prevent and how much they protect the company by doing so. The game 100 against 1—security having to protect 100% of their surface area while threat actors need to find only one entry point—has been played and lost in many attacks. Deception technology is known to take another perspective by adopting an attacker's perspective. Today modern data-minded deception is taking it to the next level and closing the gap from the inside out. The crown jewels of an organization, its data, are protected by a robust system expanding throughout the network. This approach reflects principles of the Crown Jewel Analyses (CJA) a framework compiled by MITRE's engineers on the

basis of helping practitioners acquire robust systems and proficiency in best security practices to protect and hardened their most critical assets. CJA will be explored further in the chapter Deception Approach 1—Critical assets, intellectual property/ PII data with the focus on its risk mitigation strategy.

## Why do I actually need deception in my organization?

Deception technology is rooted in the idea of deceiving threat actors to expose their malicious intentions and disable successful execution. While the basic concept is easy to grasp, the application of deception can vary widely. To illustrate how early detection and automatic remediation can be achieved in real-life, 6 use cases are explored in the following chapters:



The challenges that are tackled by deception are continually changing. Ransomware is growing its level of sophistication, ways of distribution and overall impact. With More than 700 million ransomware attempts in 2021 breaches are happening and the question of "if" shifts to the forecast of "when".[1] Organizational networks are growing complexity, creating a dense tangle for IT and IT-security to manage, maintain, monitor, and protect data across platforms. The constant flow of information induces a flood of network data that overtones the warning signals of existing security tools. Despite the use of conventional security tools, bad actors are still getting in—creating the need for solutions and new approaches that surface threats which have silently bypassed security defenses. Further dwell time is a decisive factor for data protection, especially with the current trend of ransomware to leak, exfiltrate or steal sensitive data even before encrypting it.

So how can companies discover threats before they reach the crown jewels and do this in a timely manner despite a growing footprint across multiple platforms, keeping up with modern life speed? A data-minded deception approach masks the path to the data stacking up early warning layers from the inside out. Shielding mission critical data and detecting malicious behavior early on to give it and security stakeholders a crucial head start to mitigate the threat and protect business continuity.

## COMMVAULT® CLOUD THREATWISE™

The Commvault Cloud is the first cyber resilience platform delivering data-centric cyber deception, Threatwise. Using a trusted and proven technology to safeguarding data in production, Commvault offers intelligent early warning that's purpose built to keep your crown jewels safe. Through a large variety of sensors, replicating network assets, the paths to your production data becomes a minefield for bad actors. The sensors inform immediately about any malicious activity while staying invisible to the legitimate user. With flexibility, accuracy, and automation built in, Threatwise is highly scalable, allowing users to spin up a deceptive network in just seconds. Multi-cloud, on-premise and hybrid environments are equipped with high-fidelity alerting to spot threats early, enabling organizations to surface, contain, and act on threats—before data is compromise.

Figure 2 shows the high-level architecture elevating Commvault's core deceptive elements:

1. **Threat Sensors**, seamless replicates of real network assets.

2. **Full System Sensors**, based on real Windows or Linux systems.

3. **Lures**, also known as baits, tokens or decoy objects.[2]

Via the hosted management console, the Threatwise Security Operations Console (aka TSOC), the deceptive network is spun up. In accordance with real-life capabilities, different levels of interaction are provided by each deceptive asset the sensors, also known as traps or decoys. Creating a seemingly legit experience for attackers while in reality spiraling down the rabbit hole.


**Figure2:** Threatwise™ Architecture

## 1 Threatwise Threat Sensors

At the core of Commvault's deceptive network stands the threat sensor, a lightweight, but sophisticated decoy—designed to actively engage bad actors. Over 500 threat sensors can be connected to the TCP stack level of each organizational network VLAN per appliance while requiring no more than available IP addresses. Real network assets are replicated by either choosing a preconfigured sensor from the wizard or creating your personalized adaptive sensor, which can mimic any exotic or highly specialized network component of your environment.

To provide an authentic experience, threat sensors are blended in through multiple layers. Various services are configured for authenticity and can be adjusted to match network configurations. According to the type of asset, i.e., server, workstation, container, or really anything you can think of, the threat sensor responds realistically to attackers showcasing a medium level of interaction. Alerts are triggered upon the first touch. The sensors' invisibility to non-malicious users prevent false positives and optimization engines filter out any unnecessary noise.

## 2 Threatwise Full System Sensors

Additionally, a modern implementation of the classic honeypots can be deployed via the TSOC that are based on real Windows/Linux system. These full system sensors provide a high level of realism, unlimited interaction and full attack monitoring. For example, for a Windows full system sensors the host computer can be installed from your corporate image and configured with any software, data, and settings. Further, threat sensors are proxied to the full system sensor to project the high interaction levels on the decoys. The full system sensor machine will monitor and record not only inbound connections but also outbound activity. A classic example is the tracing of connection attempts from a full system sensor to another endpoint or to the Internet.

## 3 Threatwise Lures

The lures are objects deployed as baits across the organization, covering strategic pivot points such as endpoints, Windows, macOS and Linux servers and workstations. Lures are various data items and configuration entries that drive malicious activity to the sensors, giving attackers illusive ways to elevate privileges, move lateral, or collect intelligence. As soon as the attacker follows his "lead" (the lure) to connect to sensor's services, a real-time alert is triggered.

For example, the cached credentials lure places a threat sensor's IP address with specified credentials in endpoints' Windows Registry. Attackers attempting to expand access by extracting credentials from the vault are lured to a threat sensor and revealed. The use of Mimikatz, a tool to gather and dump credentials and the number one attack tool in 2021[3], displays the impact the mitigation of this attack vector has. Another commonly applied lure is the deceptive file, which places a DOCX or XLSX on employees' machines, invisible to any legitimate user but triggering alerts when opened, copied or lures come in various forms further examples are cited in the following use cases.

## INDUSTRY DIFFERENTIATOR

Commvault Cloud Threatwise offers businesses a unique approach to deception, by deploying data-driven deception layers from the inside out. The combination of all the 3 key deception elements (threat sensors, full system sensors, and lures) in unison engages threats in early stages for faster remediation to limit the blast radius by diverting traffic away from real and critical assets. By proving the attacker with different levels of interaction his strategy is identified uncovering his path and enabling IT and security teams to get ahead. The utilization of various deceptive decoys optimizes the usage of resources to cover the surface area throw-out.

For instance, in a network segment with 200 IPs in use, one Full System Sensor (i.e., Windows 2019 Server) and 100 threat sensors deployed (emulating an SAP, Oracle or SQL database) the organization has created an attack surface of seamlessly integrated deceptive devices. From the attacker's point of view, the attack surface has been extended with 30% of the footprint now sending out high-fidelity alerts upon any first touch. The experience is 100% realism making sensors and real assets indistinguishable for bad actors. The time invested by an attacker in engaging with Commvault Cloud Threatwise is time wasted on corrupt or useless activities. In addition, all attacker activity is recorded, and automation processes give the customer full control to disconnect or quarantine the attack in earliest stages.

## Deception use case 1
### Critical assets, intellectual property/PII data

Although attacks are vastly carried out without an explicit goal—e.g., a pre-defined network location, a specific asset, or a clear-cut of data—there has been a general common target towards the companies' most valuable assets, especially ransomware related. Depending on business vertical crown jewels vary, making it hard for organizations to know what these crown jewels are in the first place. Developed by MITRE the CJA is a framework to identify the most valuable assets.

Dependency maps are created that tie business objectives to information technology data via functions and tasks. In reverse, the dependency maps uncover the effect a compromise can cause on core business objectives (see Figure 3). According to MITRE, the crown jewels of your business may represent only 2% of your total business data but dominate 70-80% of your business value.[4]

With Commvault's data-minded approach, Commvault Cloud Threatwise offers users a strategic advantage. Unlike other technologies that go threat hunting generically, Commvault Cloud Threatwise takes the attackers' gaze into account to intelligently deploy threat sensors along the path to the data, protecting your crown jewels in a meaningful way. The prioritization of backup processes is based on the classification and criticality of the data, allowing Commvault to draw an immediate line to the appropriate deception deployment around the organizations' data.

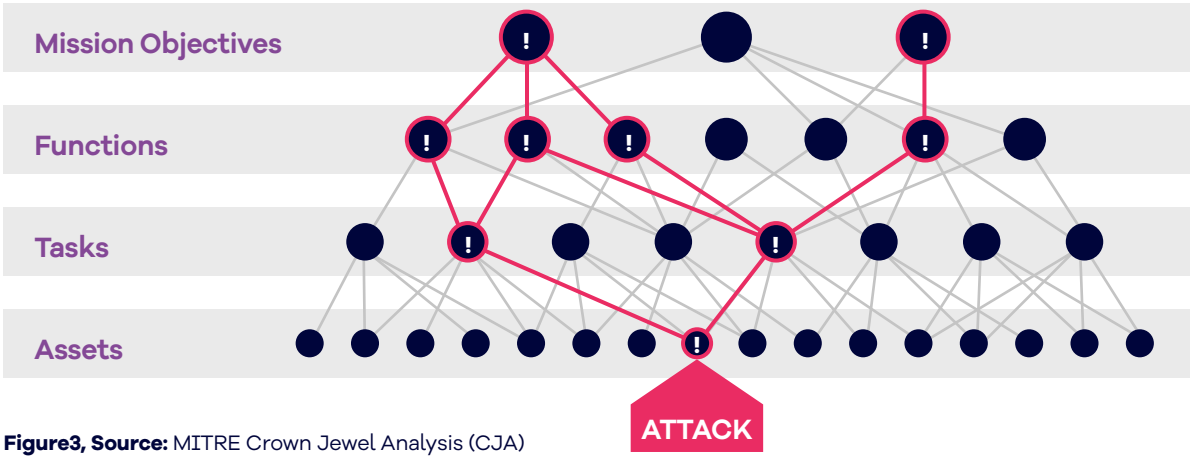



**Figure3, Source:** MITRE Crown Jewel Analysis (CJA)

With Commvault Cloud Threatwise coverage is on your side. Using look-a-like decoys, you can increase your (deceptive) attack surface with sensors sitting alongside real assets to reduce cyber risk. By flooding your surface area, the likelihood of threats touching these increases—more sensors equal less risk.

Via one Commvault Cloud Threatwise appliance, you can rapidly configure over 500 lightweight threat sensors, replicating environment devices. There is no additional hardware or licensing, constant support is deployed in seconds. The only resources you'll need for increasing your sensor coverage per asset are available IP addresses. The allocation of available IPs is adjustable, due to the dynamic ability to change decoys allowing you to scale up and down according to the current need.

## Deception use case 2
### Ransomware

The setbacks organizations experience from ransomware are profound, with attackers going beyond the original route of data encryption. While the average number of ransomware payouts decreased in 2020 by 34% (as more victims refused to comply with bad actors demands)[5], Cybersecurity researchers reported a 78% rise in the average payouts in 2021. Researchers attribute this spike in ransomware pay- outs directly with the rise of data leakage, and the threat that this type of extortion poses to businesses.[6]

The good news, as ransomware evolves so do defense strategies. While commonly associated as a last line of defense, modern data protection solutions can come into play before your data is compromised—to spot data threats before leakage, damage, or exfiltration. As attacks become faster and more sophisticated, organizations have a narrowing window to detect threats early—which often determines the success or failure in the protection of your crown jewels.

With Commvault Cloud Threatwise, businesses get high-fidelity alerts based on a wide variety of coverage. Threat sensors are invisible for legitimate users, triggering a touch-to-event mechanism only for malicious activity. By covering the path of the data from the inside to the outside, as determined by the Crown Jewel Analysis, Commvault Cloud Threatwise protects customer crown jewels in a cost-efficient way, instead of relying on uncertain factors such as flawless perimeter security or signature detection.

Take the impact of just one deceptive asset as an example: the deceptive file (Commvault Cloud Threatwise lure) can spoof more than a quarter of techniques (50+) of all that are listed in MITRE ATT&CK.[7] Before this lure is placed on likely entry points, the endpoints, a deceptive web has been spun with threat sensors mimicking assets in strategic places. Deception is expanded to various layers to avoid a single line of defense and business interference simultaneously. For a data-minded and strategic deception deployment Commvault provisions your organization's journey with best practices built-in based on the above delivered scientific framework throw-out the process.

## Deception use case 3
## The human factor

Today's most common attack vector is sophisticated phishing, or in general attacking end-user devices.[8] Awareness of cyber threats is growing but the prevention of attacks is not in the primary focus of the usual employee, as the vast majority are not hired in the field of cybersecurity. Remote work has been a catalyst for exponential growth of this risk factor in recent years.

Corporate VPNs are often targeted by attackers because they are public facing—so breaching a remote endpoint and obtaining credentials and bookmarks to corporate VPNs is highly attractive. Commvault Cloud Threatwise recommends the deployment of VPN sensors that can be placed on corporate DMZs or in the Cloud. Threats with a focus on VPNs will get caught by the sensor and diverted.

To provide a realistic user experience for the attacker fake cached credentials are also placed on the employees' endpoints in combination with a URI browser token leading to the deceptive VPN. As these artifacts are hidden from legitimate users the sensor and lures will stay in stealth until triggered by malicious activity.

## Deception use case 4
## Dark corners of the network

Tools are means to an end and IoT devices have endless use cases from smart locks and appliances, building management systems, cameras, industrial equipment, and smart sensors. The connectivity of IoT devices has significantly grown in recent years, expanding the attack surface by number and extensive additional risk. Visibility into the internal processes of these light IT assets is difficult, leaving a blind spot for security. These factors have made IoT and industrial IoT devices a prime target for cyber threats.

There are three approaches to deploying deceptive sensors to the dark corners and across the network. One, using the inbuilt scanning facility you can identify assets, two reviewing a vulnerability scan report or three, providing a topology of the assets. Any of these options then allows Commvault Cloud Threatwise to deploy a deceptive replicate of these devices across the infrastructure without requiring agents. Through a combination of preconfigured sensors and adaptive sensors, the organization covers significant unprotected areas and brings light to the darkest corners of the network.

## Deception use case 5
### Vulnerable assets

Check Point Research has shown that years old vulnerabilities are a continuous target. In 2021 a breath taking 65% of attacks involving vulnerabilities can be traced to those discovered in 2017 or earlier.[9]

Exchange servers, printers or remote connections, certain systems are a reinforced target and of high interest simply due to their type of connection or wide spread of use. Thanks to bug bounty programs new vulnerabilities get disclosures and patched by vendors in a time sensitive manor. With each discovery of a new vulnerability a new patching cycle is started. Often including dreadful processes to test patches, find maintenance windows and connect sensitive machines to the internet. Patching introduces risk before any risk can be mitigated. These high levels of time and resources demanded until vulnerabilities are resolved making them a low-hanging target.

Vulnerability probing is done by hackers using ransomware and other self-spreading malware. Scanning and staying undetected can be accomplished in many ways: use fragmentation, ARP scans, idle scans, Dirbuster, Metasploit or just staying "low and slow" often works to stay under the radar of your SIEM, IPS or NTA. In fact, SIEMs cover on average less than 5 of the top 14 techniques detected in the wild in 2021 by threat intelligence teams.[10] Taking these numbers further Cardinal Ops reported, that only 20% of all 190+ techniques listed in MITRE ATT&CK (v10) are covered by SIEMs.[11] This has driven the rise in deception technology as an alternative countermeasure. By placing threat sensors around assets with a high frequency of vulnerabilities is a powerful detection tool.

Commvault Cloud Threatwise introduces a unique way to mitigate risk caused by newly disclosed vulnerabilities and related patch cycles. Through integration with vulnerability scanners, Commvault Cloud Threatwise can deploy sensors around impacted assets. As a first step, this multiplies the protection layer to vulnerable assets and buys time to complete adequate testing prior to rolling out the patches. Further, these sensors are a great detection mechanism for threat actors beyond the patching phase as even five-year-old vulnerabilities stay relevant for attackers today as Check Point Research has shown.

## Deception use case 6
### Lateral movement and reconnaissance across platforms

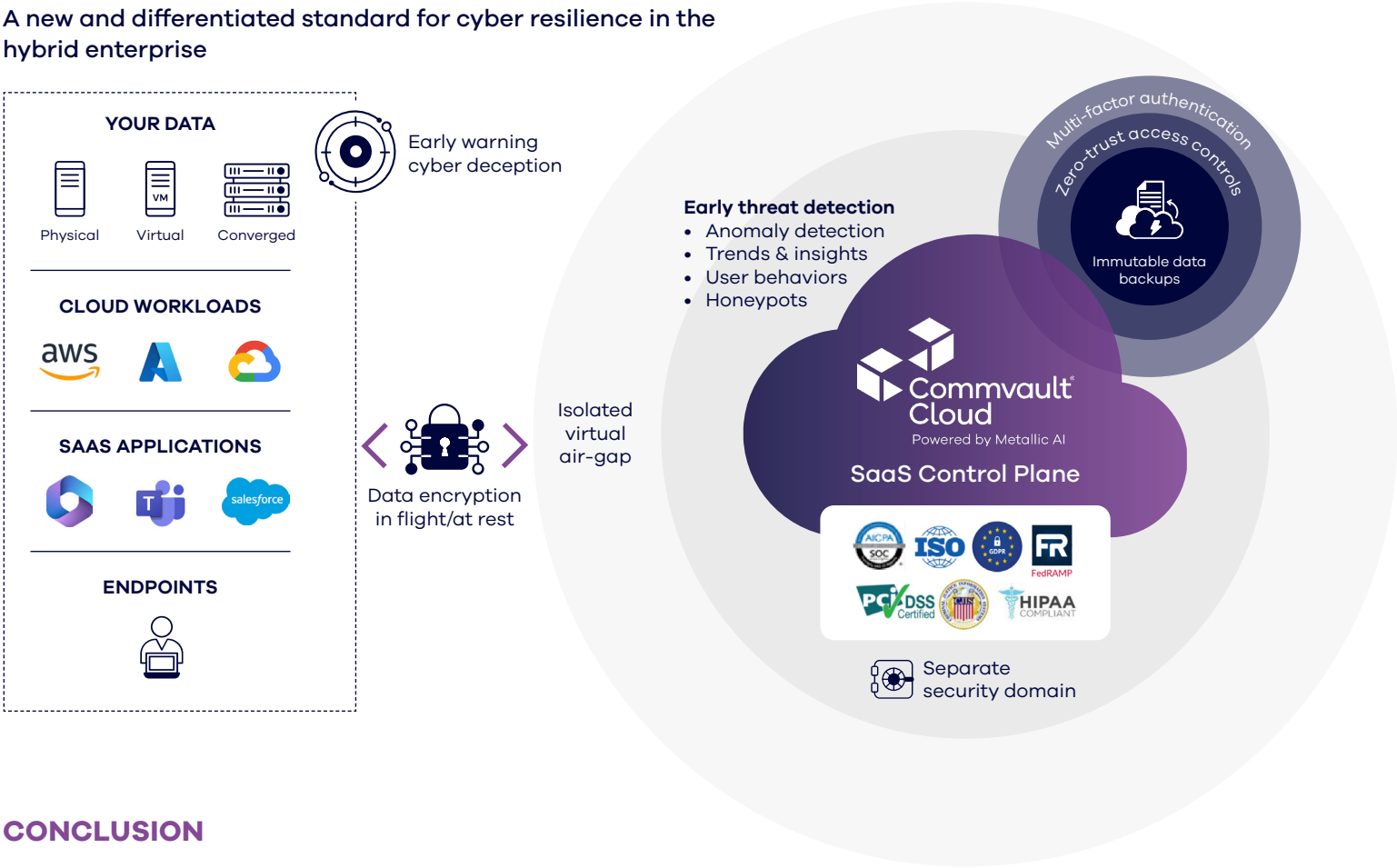
From any initial entry point of an attack, the threat spreads by moving laterally through multiple network systems until the end goal is reached. Attaining that objective involves gathering information about multiple systems and accounts, obtaining credentials, escalating privileges, and ultimately gaining access to the identified target.

There are numerous ways an attacker can move undercover. A commonly used attack strategy for moving laterally is the escalation of privileges, making the active directory server (AD) a popular target. For layered security, threat sensors are placed around the AD replicating the server. Further, dedicated AD lures spread fake credentials in the AD immediately detecting any malicious activity and directing attackers to sensors and away from real assets.

Mechanisms and triggers of traditional security systems can be researched and therefore be avoided. With Commvault Cloud Threatwise, the system doesn't react as a security device, and the variety of deceptive assets blended into the real environment makes them undetectable without triggering alerts. With enough sensors placed in strategic places, cyber risk is effectively mitigated by reducing the likelihood of undetected malicious behavior.

## OUR MULTI-LAYERED PROTECTION APPROACH

A new and differentiated standard for cyber resilience in the hybrid enterprise




## CONCLUSION

Deception has the independent backing of MITRE1, as a recommended countermeasure. It provides both protection and remediation and is a complimentary measure to your existing toolset with the ability to be deployed quickly and easily, ensuring a short return on investment. Enhance your data protection according to the motto “Make Security Valuable and Attacks Costly” (Chris Krebs at Black Hat, 2022). With the combination of the three core components of Commvault Cloud Threatwise, companies of all sizes can strategically deploy comprehensive deception as a service to improve the current defensive measures for their crown jewels, implementing 9 MITRE D3FEND countermeasures and defending against the 6 use cases described above.

1. https://www.computerweekly.com/news/252513735/Backups-no-longer-effective-for- stopping-ransomware-attacks
2. In MITRE D3FEND D3-DO https://d3fend.mitre.org/technique/d3f:DecoyObject/
3. ISACA, State of Cybersecurity 2022, p.34 and Sophos, 2022 Threat Report p.19
4. https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis
5. BillSiegel,“RansomwarePaymentsDeclineinq42020,“Coveware(Coveware:Ransomware Recovery First Responders, June 9, 2021)
6. Unit 42, Palo Alto Networks. https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html
7. https://d3fend.mitre.org/technique/d3f:DecoyFile/ (accessed 16.07.2022)
8. Reference (SocialEngineering,humanfactor,etc.)
9. Cyber Security Report 2022, Check Point Technologies, P.54

To learn more, visit **commvault.com**