SOLUTION BRIEF

Commvault

Modern cyber deception

Redefining cyber protection through early warning detection

Ransomware is always evolving, and has transformed into a new form of organized digital crime, breeding more sophisticated technologies and tactics. It's a relentlessly expanding and adaptive enterprise that continuously sharpens its tactics and techniques while it lowers the barrier to entry for new actors to get into the game. One thing that hasn't changed, however...the pursuit of your data.

Data is the crown jewel for educational institutes and is the chief target of ransomware attacks. As new and advanced threat vectors emerge, it's never been more important to consider robust tools that proactively insulate your organization from these risks. With the use of data-minded cyber deception, companies of every size get modern ransomware protection to spot and mitigate threats earlier.

RECOVERY ALONE IS NOT ENOUGH

Conventional ransomware attacks revolved around data encryption. Their primary objective: to deny access to critical system and application data, rendering it useless—severely disrupting (and potentially halting) operations. However, proven data protection solutions offered organizations a way out against these traditional attack methods. Rather than paying lofty ransomware demands in exchange for their data, educational institutes could maintain clean and recoverable backup copies, to independently get their operations back online. Bad actors understood this and flipped the script.

Today, 83% for ransomware attacks involve some form of data leakage, exfiltration, theft, or damage.[1] Put differently; the majority of cyberthreats are designed to do more than just deny you access to your own data. From stealing trade secrets, to selling sensitive data on the dark web, and everything in between, today's ransomware is purposefully executed to exploit organizations in new ways. Ways that recovery alone cannot safeguard from.

And as if double and triple extortion tactics alone weren't enough, cyberattacks are moving faster than ever. Experts project that the average breakout time of an attack (the time taken by attackers to move from initial access to infection within victim environments) is roughly an hour and 30 minutes.[2] With this accelerated timeframe, businesses need new ways to surface threats sooner. By spotting threats earlier in the attack cycle, educational organizations can respond faster and safeguard critical business data and assets prior to impact.

83% of ransomware attacks involve some form of data leakage, exfiltration, theft, or damage.[1]

MODERN CYBER DECEPTION

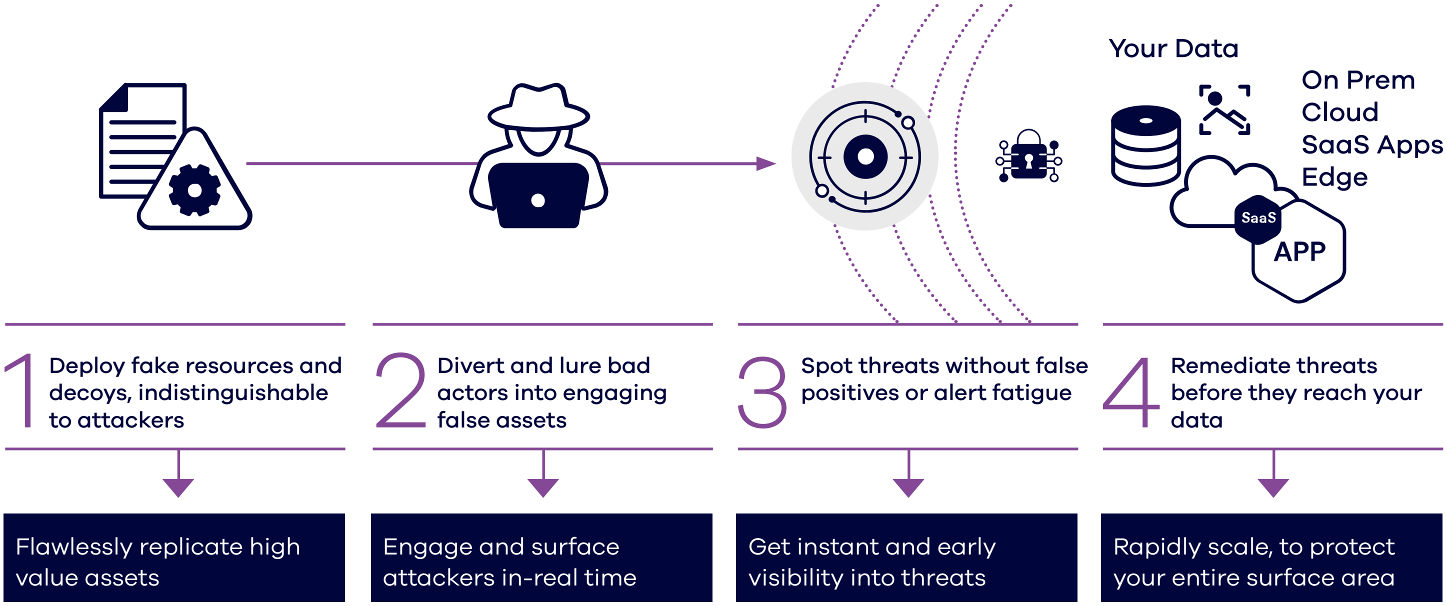
As bad actors shift their attention, businesses must also reorient. Organizations must reimagine their data security and cyber resiliency strategies to focus on proactively responding to threats before their data is compromised, not just recovering from them.

Cyber deception is proven to aid in this effort, equipping businesses with powerful active defense capabilities to secure their data sooner. By disguising itself as legitimate business resources, modern cyber deception solutions engage bad actors the moment an attack begins, in production environments. By luring bad actors into compromising fake assets, cyber deception provides early warning signals into unknown threats, exposing attackers and empowering organizations to proactively contain threats. It is a recognized technology and approach within the defensive MITRE frameworks (MITRE D3FEND and MITRE Engage), demonstrating its efficacy as a countermeasure in the mitigation of cyber risk.

COMMVAULT® CLOUD THREATWISE

Leveraging patented deception technology, Threatwise changes the game in ransomware protection, combining sophisticated early warning with comprehensive data security. It enables institutions of every size to see and minimize silent attacks before they cause harm; detecting and diverting the stealthiest of zero-day attacks which evade conventional detection technology and circumvent security controls.

Unlike traditional honeypot technologies, Threatwise is lightweight, fast and easy—enabling you to dynamically deploy more deceptive assets sooner at a much lower cost. It is purpose-built to directly engage threats during recon, discover, and lateral movement. By immediately alerting organizations into attacks in progress, organizations can uncover advanced cyber threats silently traversing environments, before data leakage, encryption, exfiltration, and theft.



1 Deploy fake resources and decoys, indistinguishable to attackers

Flawlessly replicate high value assets

2 Divert and lure bad actors into engaging false assets

Engage and surface attackers in-real time

3 Spot threats without false positives or alert fatigue

Get instant and early visibility into threats

4 Remediate threats before they reach your data

Rapidly scale, to protect your entire surface area

[1] https://www.computerweekly.com/news/252513735/Backups-no-longer-effective-for-stopping-ransomware-attacks
[2] https://www.sophos.com/en-us/press-office/press-releases/2022/06/attacker-dwell-time-increased-by-36-percent-sophos-active-adversary-playbook-2022-reveals

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