SentinelOne eBook

SentinelOne®

Deception Technology
A Critical Component of a Modern Cybersecurity Stack

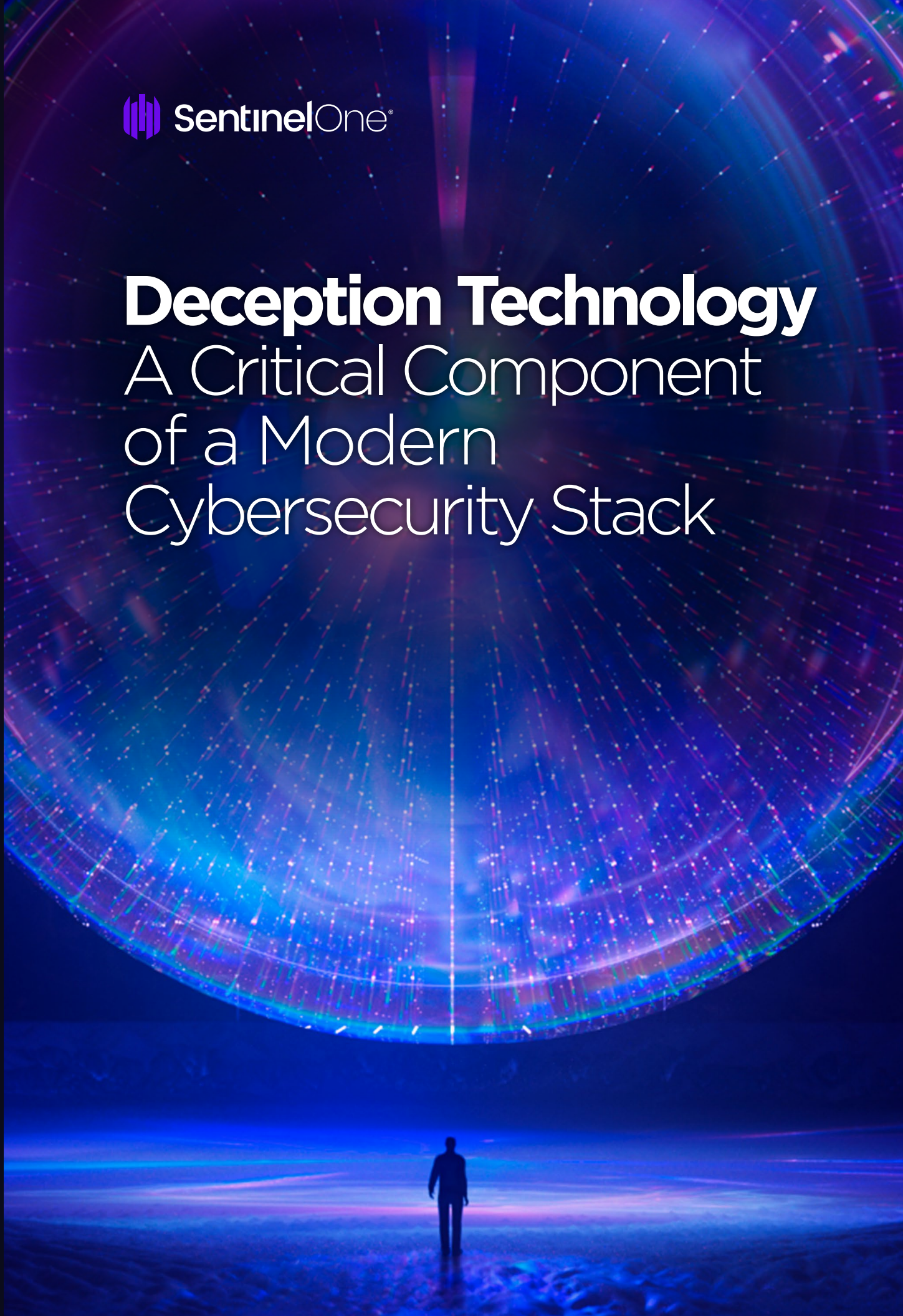



Table of Contents

Introduction	**3**
What is Deception?	**3**
What Does Deception Mean for Cybersecurity?	**4**
How Does SentinelOne Bring Deception to Cyber Security?	**5**
Summary	**7**

Introduction

As the number of reported breaches per year continues to escalate, enterprise security teams need to deploy comprehensive and adaptive cybersecurity measures that combine native prevention, detection, and response capabilities to execute an unified cybersecurity strategy that can stand up to both known and emergent threats. Whether they are external or insider threats, attackers continually adapt to evade existing security measures. In response, analysts are turning to deception-based solutions to prevent data exfiltration, theft of sensitive information, or damage to an organization's critical infrastructure, brand, or reputation.



Today, we will explore why deception has become a critical element of a modern cybersecurity stack, and a core capability to implement in your security strategy.

01

What is Deception?

While people have used deception to effectively confuse and outmaneuver their opponents for millennia, cybersecurity professionals apply deception to create uncertainty for an attacker and trick them into making mistakes that reveal their presence, adversarial techniques and motives, creating unfavorable attack economics for them.

With deception technology, security teams can move away from a reactive posture and deploy concealment technology in the form of bait, lures, and decoys designed to derail attacks early and throughout the attack lifecycle.

Attackers typically harvest credentials, conduct reconnaissance, and move laterally to complete their attack. Using a deception solution, organizations can hide production data (such as credentials, Active Directory objects, and data) to create a virtual minefield of misdirection. By deploying decoys and credential bait which mirrors an environment's operating systems, applications and data, security teams can use engagement-based alerts based on attacker discovery actions or interaction with a decoy to receive high-fidelity information to help a team understand and neutralize a threat.

Unlike other detection tools, a deception environment built specifically for high levels of interactions can allow analysts to safely gather intelligence on their opponents. By gaining insight into the attacker's tools, methods, and intent, your enterprise security team can arm

themselves with deeper knowledge to strengthen overall defense strategies and level the playing field with their opponent, with little risk or harm to the threat actor's intended target.

02

What Does Deception Mean for Cybersecurity?

As attackers continue to successfully evade perimeter defense, traditional prevention postures are clearly inadequate against sophisticated threat actors, leading to longer dwell times and compromised enterprise resources. Existing security controls will only detect an attacker once they infiltrate a targeted network and attempt lateral movement.

With billions of networked devices and millions of applications, the reality of modern cybersecurity is that static defenses no longer suffice. In this landscape, deception technology is a key element of an enterprise's cybersecurity infrastructure.

A deception-based solution will make it harder for threat actors to conduct their activities covertly. Crafting decoy assets indistinguishable from production systems makes differentiating between them virtually impossible for an attacker. With decoys, bait, and lures deployed within an environment, attackers must be cautious at every stage of the attack chain. After all, a single scan or attempt to access a deceptive asset or object in an endpoint or network will trip an alarm. Because these alerts are engagement-based, deception does not generate false positives.

The core concept of modern deception technology is that no one should ever interact with any deceptive asset. Thus, employees would not be able to encounter these assets in their day-to-day activities because these deceptive assets have no production value, and any detection will indicate anomalous and likely malicious activity. This concept is instrumental in detecting insider threats engaging in atypical or suspicious activity.

The next generation of deception technology takes misleading attackers even further than decoys and bait. These solutions hide and deny access to production files, folders, and storage. This potent tactic restricts an attacker's ability to identify production data and storage locations, limiting visibility to decoy assets that force threats actors to engage with the deception environment. Furthermore, cutting-edge deception solutions can misinform and redirect the attackers away from production assets when they attempt discovery or reconnaissance activities, channeling their lateral movements away from critical systems by deflecting their attacks to decoys.

Recent research also proves that deception technology enables security teams to act more efficiently. Unlike traditional detection solutions, which generate too many false positive alerts, deception-based alerts reduce the number of false positives and include detailed intelligence about the attack and the threat actor responsible, significantly increasing response capabilities and reducing the amount of time it takes to identify false positives. Compared to existing point solutions and legacy tools in an enterprise technology stack,

deception-based autonomous cybersecurity is much simpler to design, deploy, and operate. When factoring in time gained from streamlining SOC operations with investigation efficiencies, deception technology can reduce SOC costs by an additional $4,600 per analyst per year for a total per analyst savings of almost $23,000 per year or a decrease in SOC analyst costs of 32%. Furthermore, when factoring in deception's ability to reduce attacker dwell times by 91-97%, or down to 5.5 days, it can reduce data breach costs by 63%, an average savings of $2.49 million per incident or $51.41 per compromised record.

03

How Does SentinelOne Bring Deception to Cybersecurity?

Deception platforms detect and analyze internal attack activity, including discovery, credential theft, privilege escalation, lateral movement, and data collection. The **Singularity XDR** platform stands at the forefront of deception-based identity security, using fully customizable virtual machines as decoys to mimic production assets, ranging from Windows and Linux servers to network infrastructure, IoT, and SCADA devices, projecting them throughout an environment.

To an attacker looking for critical systems, credentials, shared drives, and sensitive data, these decoys appear as tempting targets indistinguishable from production assets and worthy of exploration.

Singularity Hologram provides a much-needed detection solution for today's modern security teams of any size. It allows security teams to focus on finding and responding to attacks and giving them visibility into new and complex tactics by turning the entire IT environment into a trap. Additionally, the high fidelity and low volume of alerts allow the system to run with low maintenance and overhead while providing incredibly accurate and relevant threat data.

Deception technology is straightforward and quick to deploy. Security teams can project thousands of automatically customized decoys and bait through their network shortly after installing Singularity Hologram, providing deception and early alerting. With a proper "crawl, walk, run" strategy, this can mature into a fully integrated and authentic deception layer that will fool and catch even the most careful and mature threat actors.

Singularity Identity also allows organizations to create deceptive credentials, fake objects such as SSH tokens, cloud platform keys, and SMB shares on existing production systems that lead attackers back to the decoys. The hidden SMB-mapped shares act as lures for ransomware seeking to spread via network drives, stalling the malware by continuously feeding it data while throttling the connection to give security teams time to respond. Additionally, Singularity Identity looks for unauthorized Active Directory (AD) queries and intercepts the results, hiding sensitive or critical objects and returning deceptive lures in their place. The Deflect function also makes any production endpoint a decoy that redirects attacks targeting ports and services into the deception environment for engagement, essentially locking down endpoints from attacker lateral movement.

Singularity Identity identifies credential exposures and misconfigurations on endpoints that allow attackers to move laterally across the network from system to system. The solution maps connections and indexes the data for searching and analysis. By identifying such vulnerabilities, the security team can eliminate these stored credentials, fix the misconfigured policies, or add decoy credentials to defend endpoints further.

When an attacker engages with the deception environment, Singularity Hologram immediately alerts on the activity for security teams to quickly identify the source of the attack for automated incident response. When the attacker directly accesses a decoy or engages with a webpage or SMB share on which it is hosted, the platform logs all activity, displaying it to the security team in the dashboard. The platform captures the forensic data providing information for incident response and remediation actions, including recording all command and control (C2) traffic and conducting memory forensics analysis. For the security team, this is a wealth of organization-specific threat intelligence they can use to further improve their defenses.

Hologram Extender scales across on-premises, remote offices, and cloud environments. The forwarder comes as a VM, endpoint module, or containerized application. It can run on endpoints, servers, VM environments, or switches that contain a hypervisor or can run container applications. This deployment flexibility benefits organizations with extensive and varied network infrastructures.

The DecoyDocs function creates deceptive files with an embedded beaconing function that notifies security teams of improper access. When alerting within the network, the solution provides the full details of the host accessing it. If the attacker exfiltrates the document, it will beacon home with the geolocation of every IP address that opens it. This capability gives security teams knowledge of what attackers are targeting and their potential motives.

Overall, Singularity Hologram and Singularity Identity provide a comprehensive and easy-to-use threat deception solution that scales across any size network, regardless of location, and accelerates incident response while providing critical adversary intelligence to improve defenses.

04

Summary

As part of the Singularity XDR platform, Hologram and Identity are critical in empowering a threat-informed defense with real-time threat detection, credential and Active Directory vulnerability assessments, attack forensic analysis, and integrations to accelerate incident response dramatically. High-fidelity threat information reduces alert fatigue among security teams.

The Singularity XDR platform serves as a force multiplier, improving existing technologies, processes, and resource productivity and ultimately reducing the time to detect and remediate an exploit or malicious threat actor. With its many partners, SentinelOne continues to expand its platform and 3rd-party integrations to deliver the fastest detection and incident response to stop attackers in their tracks.

About SentinelOne

SentinelOne's cybersecurity solution encompasses AI-powered prevention, detection, response and hunting across endpoints, containers, cloud workloads, and IoT devices in a single autonomous platform.

sentinelone.com

Ready to take the next steps?

Contact us to learn more about the SentinelOne Singularity Platform, or request a free demo.

Get a Free Demo

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- 100% Protection. 100% Detection.
- Top Analytic Coverage 3 Years Running
- 100% Real-time with Zero Delays

Gartner peerinsights 4.9

99% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity

FedRAMP

AICPA SOC

TEVORA PCI DSS Attestation HIPAA Attestation

VB 100 VIRUS virusbtn.com

AAA

SE Labs BEST Innovator WINNER 2021



SentinelOne

Contact us

sales@sentinelone.com

+1-855-868-3733

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

sentinelone.com

S1-EBOOK-005_DECEPTION_TECHNOLOGY-11032022

© SentinelOne 2022