SentinelOne White Paper

SentinelOne®

Deception for **Inside-the-Network Threat Detection**



Table of Contents

A New Approach to Network Security	**3**
Targets	**3**
Advanced Persistent Threats and BOTs	**3**
Points of Vulnerability to APTs and BOTs	**5**
APT Attack Processes	**6**
Deficiencies of Current Prevention Solutions in Combating Cyber Threats	**8**
Benefits of Active Deception and Decoy for Threat Detection	**9**
Functional Requirements of an Effective, Real-Time Threat Detection System	**10**
Singularity Hologram Offers Active Deception for Threat Detection Solutions	**11**
Disrupting Cyber Attackers at Every Step	**13**
SentinelOne Advantages	**13**
Conclusion	**15**
Tomorrow's Threats Require a New Enterprise Security Paradigm	**16**

01

A New Approach to Network Security

As cyber attacks increase in sophistication and penetrate networks with ever-greater frequency and effectiveness, security professionals are expressing growing concerns about being able to quickly detect and stop inside-the-network threats from both internal and external threat actors.

The growing number of these cyber attacks and the increased volume of stolen records being detected by external sources has driven many organizations to a new adaptive approach to network security. This new approach assumes that an organization's perimeter has already been breached and that persistent attackers are going to penetrate it.

A modern adaptive defense based on this assumption brings with it a new set of security goals. These goals are no longer solely based on stopping attacks, but focus on detecting and neutralizing attacks in real-time.

02

Targets

Organizations that store large quantities of technical, financial, medical, or business data on their networks are at high risk of being targeted by advanced persistent threats. Such organizations include:

- Financial institutions
- Healthcare organizations
- Government agencies
- Oil and gas companies
- Educational institutions
- Media and entertainment companies

03

Advanced Persistent Threats and BOTs

Advanced Persistent Threats

Advanced Persistent Threats (APTs) are attacks that penetrate a network and remain there, undetected, for extended periods of time, typically gathering valid user credentials, especially administrative ones, and moving laterally across a network, identifying sources of high-value data and analyzing network vulnerabilities that can give them access to that data.

The objective of an APT attack is to maintain access without discovery and to steal as much high-value information as possible. “Advanced” points to sophisticated techniques using malware to exploit vulnerabilities in systems. “Persistent” indicates that an external command-and-control system is continuously monitoring and extracting data from a specific target.

Because of the technical difficulties inherent in maintaining an undetected presence on a network for an extended period, intruders utilizing APTs must frequently rewrite code and employ sophisticated evasion techniques. Additionally, once network access has been achieved, an attacker usually establishes a “back door” for the purposes of data exfiltration and undetected escape.

BOTs

BOTs represent another highly sophisticated form of Internet crimeware and are created by attackers repeatedly infecting victim computers. Tasks that BOTs can perform run the gamut from sending spam to blasting websites off the Internet as part of coordinated denial-of-service attacks.

BOTs do not work alone but as part of networks of infected machines called “BOTnets”, with each zombie machine controlled by a command-and-control server.

BOTs spread themselves across the Internet by searching for vulnerable, unprotected computers to infect. When they find an exposed computer, they quickly infect the machine and then report back to the command-and-control center that manages them.



04

Points of Vulnerability to APTs and BOTs

Several elements factor into a modern network's vulnerability to APT and BOT attacks. They include:

Web Services

The steady increase in Web services that are available to users of all kinds makes it difficult if not impossible to identify all the malicious web links and sites being used as command-and-control servers.

Zero-Day Exploits

Zero-day exploits (also known as zero-hour or 0-day vulnerabilities) exploit undisclosed and uncorrected vulnerabilities that adversely affect computer applications, data, additional computers, or an entire network. Zero-day exploits are attempted on or before the day notice of the vulnerability is released to the public and corrected code has been made available.

Stolen Employee Credentials

With geographically dispersed and varied user populations, it is almost impossible to ensure the integrity of the credentials of every employee, contractor, and 3rd-party vendor that accesses a network, a situation that automatically brings security risk.

Endpoint and Personal (BYOD) Devices

BYOD devices are ideal targets for zero-day exploits as they are difficult to detect and provide an entry point to attackers attempting to penetrate a network.

Phishing Email Attacks

Phishing campaigns typically occur through fraudulent emails that appear to be legitimate. Individuals receiving such fraudulent emails inadvertently provide attackers with sensitive information by clicking on malicious links in such emails, downloading malware and handing over account details. Hackers can quickly infiltrate corporate networks and find ways to exfiltrate business data and sensitive information through phishing campaigns.

05

APT Attack Processes

Systematic Approach

To break into a network, implant advanced malware, and sustain an indiscernible presence for many months to siphon off the data that they have targeted, APTs usually adhere to a systematic attack process. APT processes maintain a high degree of covertness over a long period.

Most APT attacks have two phases: a reconnaissance phase in which intruders penetrate a network, implant malware, and sustain a presence and (2) an exfiltration phase in which data is stolen.

Attack Threat Vectors

Reconnaissance	Ransomware	Stolen Credential Attacks	Phishing
• Attackers scan a network to identify best sources of data assets to attack. • Attacks can originate anywhere on a network. • Attackers launch malware required to carry out an attack.	• Attackers seek to encrypt and erase networked drives: Ransom payment required to restore data. • CryptoWall, WildFire, Zepto, and CryptoJoker are varieties of ransomware. • Backup files are also often corrupted and data restoration can fail.	• Attacker steals cached credentials from an endpoint they have infected. • Disguised as that endpoint, attacker uses stolen credentials to mount persistent attacks. • Stolen data is exfiltrated via backdoors established by attacker.	• Attackers trick users into downloading malware or revealing passwords or other personal information. • Malware will then spread laterally throughout an organization for attack escalation. • Phishing circumvents traditional prevention systems and detection because it is activated by insiders.

Threat Vectors

Attackers are in general either scanning a network to find hosts with services or applications to compromise or seeking to exfiltrate employee credentials or data. Either way, attackers and their automation tools rely on the responses they receive throughout the attack process they undertake to achieve success in their attacks:

Attacks That Begin With Reconnaissance

Attacks begin with a scan of the network from the infected endpoint to locate the asset and services an attacker wants to target.

SentinelOne's identity security solutions engage attackers by hosting network services across multiple virtual machines, IP services, and subnets luring attackers into revealing themselves as soon as they start to look for your high-value assets.

Attacks That Begin With Stolen Credentials

An attacker exploits the infected endpoint to extract credentials and location of the assets that it wants to target.

Singularity Identity provides a customizable and nonintrusive technology that lures such targeted attacks to its solution to detect infected endpoints, servers, and VMs.

Attacks That Begin With Ransomware

Attacks begin with the encryption or erasure of a system. The attacker will then seek out the next network drive to continue its attack.

Singularity Hologram engages the attacker by directing him to "deception drives" that appear as networked drives. Once the attacker is engaged, alerts are raised so the infected system can be quarantined off the network and remediated.

Attacks That Begin With Phishing

Attacker uses phishing emails to engage a user into providing their credentials or downloading malware.

Singularity Identity simplifies the detection and analysis process by enabling users to submit suspicious emails to the BOTsink analysis engine so that the email can be analyzed for malicious intent. Submissions can also be submitted directly into the BOTsink Analysis Engine for investigation. Once the attack information is analyzed, attacks can be automatically or manual blocked and quarantined.

> "
>
> There's two kinds of CIOs: ones who have been hacked and know it, and those who have been hacked and don't yet realize it. But the reality is, you've been hacked.
>
> Tony Scott, Federal CIO

Typically, an APT Involves the Following Phases

Phase	Description
Target Selection	Perpetrators of APTs scour the Internet for networks that are exploitable or focus on pre- selected companies or networks.
Footprinting	Attackers use various surveying tools to create a blueprint of a target's IT infrastructure, including details about sites, network topology, domain, internal servers, and DHCP servers.
Malware engineering	Attackers plan their incursions upon their targets' exploitable vulnerabilities. On this basis, attackers engineer or procure the malware required to carry out an attack.
Initial breakthrough	Attackers often phish their target company's employees into downloading malware. Alternatively, they can also exploit any zero-day vulnerabilities in the software used by the target company.
Capturing admin privileges	In almost all APT attacks, hackers attempt to steal local administrator credentials and then domain-level admin credentials. Backdoors are created to exfiltrate stolen data or inject more malware.
Internal reconnaissance	Attackers explore the network from inside to identify individuals with privileged access and vulnerabilities that are suitable for creating backdoors.
Expansion of access	Attackers that are successful in penetrating an organization will usually attempt to compromise more systems within that organization.

06

Deficiencies of Current Prevention Solutions in Combating Cyber Threats

Many organizations have deployed a strong security perimeter based upon firewalls, Intrusion Protection Systems, sandboxes, and end-point security solutions. Unfortunately, even best-of-breed perimeter and end-point security solutions cannot reliably detect sophisticated attacks from BOTS, APTS, ransomware, and phishing. Such attacks are therefore evading traditional security measures and penetrating networks undetected.

A deficiency found in traditional breach-detection solutions is the generation of large numbers of false positives that are often referred to as "alert noise". Because this noise, traditional means of attack detection lead to time-consuming processes, rendering organizations unable to respond to alerts in time to prevent network attacks. Most APTs and BOTs take months to discover when traditional detection systems are used.

Prominent companies, agencies, and analysts, therefore agree that traditional security measures are no longer sufficient to protect against breaches. In healthcare environments, for example, 1 in 5 breaches are identified by an external source such as a patient whose information was compromised. Across all industries, it is estimated that a full 40% of malware alerts go undetected.

> “
>
> Deception as an automated responsive mechanism represents a sea change in the capabilities of the future of IT security that product managers or security programs should not take lightly.
>
> Lawrence Pingree, Gartner Research Director

07

Benefits of Active Deception and Decoy for Threat Detection

A shift from a defensive to an offensive security posture is necessary if organizations with sensitive and high-value data assets are to wrest the upper hand in their battle against hackers. In assuming such a posture, organizations now look to deception-and-decoy systems for post-infection breach detection.

An effective inside-the-network attack system must address all threat vectors and enable an organization to:

Quickly identify and stop attacks during all phase of attack

- Lure attackers into revealing themselves as soon as they start looking or moving laterally across network services, virtual machines, IP services, and subnets for high-value data assets
- Reduce attack detection time by accurately identifying infected clients, including sleeper and time-triggered agents, thus enabling full analysis of an attack before it causes damage
- Stop advanced threats with real-time notifications and automated incident response actions
- Generate only substantiated, actionable alerts. No false positives and noisy alerts
- Utilize authentic deception and decoy technology that catches zero-day attacks and is not dependent on known signatures.

Access forensic data and defense against future attacks

- Capture actionable information by identifying infected systems and analyzing information on the time, type, and anatomy of an attack. Catalog all attack activity to understand an attack’s anatomy and objectives.
- Provide a threat intelligence dashboard and Indicators of Compromise (IOC) reports that provide detailed attack information to prevention systems through UI, PCAP files, Syslog, IOC, and CSV report formats.

08

Functional Requirements of an Effective, Real-Time Threat Detection System

IT professionals have an overwhelming range of security solutions available to them. The purpose of the following section is to provide guidance relative to the critical capabilities of effective deception-based threat detection solutions.

Requirement	Highlights
Real-time Advanced Threat Detection	• Effectively lures attacks away from sources that store high-value corporate data assets Low-friction BOT and APT detection
Authenticity	• Runs on real operating systems with full network services, protocols and data elements Provides VM import and full customization to match an organization's "golden image" Does not rely on signatures or database lookup
Coverage	• Provides network threat detection for networks, data centers and the cloud: VMware, Amazon Web services, OpenStack, IoT, and ICS-SCADA • Detects threats in East-west data center traffic
Speed of discovery and alerts	• Eliminates alert noise: only positive alerts based on real-time engagement with attackers • Alerts prevention systems to shut down attacks promptly and to prevent future attacks
Deployment flexibility and security	• Does not require signatures or database lookup • Is not in-line and does not require heavy computation • Can be deployed as an appliance or on a VM • Interspersed with production networks • Data never leaves the organization's premises for external computation
Scalability	• Scales to hundreds of subnets • Network, data center, private and public cloud Centrally managed for global deployments
Interoperability and visibility	• Seamless interoperability with devices required to defeat breaches and prevent future attacks • Provides network VLAN visibility and analytics
Adaptability	• Identifies network breaches as the next layer of security for perimeter solutions when they fail • Provides a high degree of scalability and flexibility to address zero-day attacks
Forensics and Threat Intelligence	• Provides the containment environment to explode out exploits or phishing emails for post-compromise malware analysis • Can track back to command and control to analyze a hacker's methodologies and intent • Threat intelligence dashboard and IOC reports in UI, PCAP files, Syslog, IOC, and CSV formats • Provides a training and education environment for understanding of the anatomy of an exploit

09

Singularity Hologram Offers Active Deception for Threat Detection Solutions

Singularity Identity detects BOTs and APTs as they move laterally inside an organization's network and data center.

Deception and Decoy

Designed to augment existing security systems and detect inside-the-network threats, the SentinelOne's platform of threat-detection systems uses deception techniques to deceive, detect, and defend against threat actors as they begin scanning, targeting, and probing network clients, servers, and services for targets.

Based on active decoy and deception technology, SentinelOne's identity security solutions engage with attackers in real-time, immediately notifying prevention systems and stopping attackers in their tracks. They are designed so that they don't generate a lot of alert noise and alerts are based on actual engagement with BOTs and malware, greatly reducing the time it takes to detect real threats and remediate them before they can damage an organization.

These solutions are designed for networks, data centers, and cloud, ICS-SCADA, and IoT environments. Available as appliances and virtual machines, Singularity Hologram is designed for rapid deployment defeating APTs and BOTs that are already propagating inside a network.

Every Node and Subnet Becomes a Trap

Attivo solutions are designed to turn every node and subnet into a trap that can lure attackers into engaging, quickly identify an infection, and provide a full set of forensics for prompt remediation. Leveraging virtual honeynets in conjunction with its patented technology, The ThreatMatrix Platform is built for an adaptive defense and provides predictability into an attacker's attack path based on misconfigurations and misused credentials, early detection of the lateral movement of an attacker within a network, accelerated response with complete attack analysis, and integrations with prevention systems to automate and accelerate the blocking and quarantine of an attacker.

By luring BOTs and APTs into engaging with the BOTsink engagement servers vs. company servers, attackers are deceived into revealing themselves and through engagement within the Sinkhole, identified and profiled to understand the attacker's intent.

Remediation Support

ThreatMatrix BOTsink solutions will detect and capture actionable information for remediation, such as:

- Addresses of infected machines
- Username and password combinations
- Any dropped payloads including location and type of attacks
- Attack activity, including any data it's targeted for download or export
- Any system/kernel changes, process creation, process injection, registry and network activity

Data for Forensics

The ThreatMatrix solution also captures and catalogs all attempted communications and propagation activity for future forensics. Using the BOTsink's Analyze, Monitor, and Record (AMR) Engine feeds events to SentinelOne's patented Multi- Dimensional Correlation Engine to generate attack sequences.

ThreatMatrix provides a threat intelligence dashboard with the forensics required to capture attacker method and intent, update prevention systems and prevent future attacks. IOC reports are provided to update prevention systems in various reporting formats.

Efficient Architecture

The ThreatMatrix Deception Platform is known for its highly efficient architecture that operates without requiring computing overhead or a need to do signature database look up to detect attacks. Instead the ThreatMatrix:

- Uses IPs from the dark/unused space to insert the ThreatMatrix in the network and does not generate any traffic on the network
- Provides lures for targeting attackers to follow back to ThreatMatrix Deception Platform

10

Disrupting Cyber Attackers at Every Step

Singularity Hologram is based on a high-interaction distributed decoy system that lures the BOTs and APTs launched by attackers.

Singularity Hologram engages APTs and BOTs—trapping their activities, preventing communications and stopping their propagation and exfiltration of data. Once an attack is underway, and threat actors have been engaged by the engagement servers, in-depth visibility on the full cycle of the kill chain will be provided including IP addresses of infected clients.

Once Hologram sinkholes the BOTs and APTs, SentinelOne can identify the breach and all infected endpoints. A port from the sinkhole can also be opened to connect to the hacker's Command and Control server (C&C) and to collect additional information about the intent of the attack.

Sleeper agents, time-triggered, and polymorphic attacks can all be safely analyzed for an extended period within Singularity Identity. Any attempts at outbound C&C communication are captured for forensic analysis and threat intelligence for prevention systems.

11

SentinelOne Advantages

SentinelOne delivers a broad set of unique capabilities to its users:

Enhanced Prevention

Strengthen prevention systems with tools to assess attack path vulnerabilities and risk. Attack analysis is shared through integrations with prevention systems improve incident response by automatically blocking and quarantining attackers.

Real-time Detection

Deception-based detection authentically matches production assets to deceive attackers into revealing themselves. Detect targeted, stolen credential, ransomware, Man-in-the-Middle, and phishing attacks during reconnaissance and lateral movement within user networks, data centers, clouds, IoT, and SCADA environments.

Detailed Attack Analysis

Collect Time, Techniques, and Practices (TTP) of BOTS, APTS, insider threat actors based on malware attack and phishing email analyses.

Substantiated Alerts

Actionable alerts are raised based actual attacker engagement. Alerts provide detailed information on infected systems, attacker activity, and signatures.

Actionable Forensics

Attack findings can be reported for information sharing in the Attivo Threat Intelligence Dashboard and in popular IOC, STIX, SYSLOG, PDF, CSV, and PCAP formats.

Accelerated Incident Response

Attack forensics can be passed to prevention systems and SIEMS manually or automatically to block and quarantine the attacks.

SentinelOne's identity security portfolio delivers real-time identification of APTs and BOTs without generating false positives, adding friction to a computing environment or requiring significant management overhead



10

Conclusion

By adopting an offensive posture relative to network security, organizations are deploying deception-and-decoy systems to quickly detect and identify the lateral movement of attackers before a breach or other impact to critical infrastructure occurs.

Organizations of all industries are turning to SentinelOne's identity security solutions to protect their critical company information and infrastructure and to gain the confidence to know in real-time that they have not been breached.

- Real-time, accurate visibility into attacker threat paths, attackers within their networks, and the existence of network breaches
- In-depth attack forensic analysis and zero false positive substantiated alerts
- Updating of anti-incursion systems that shut down present and prevent future attacks

Singularity Hologram is the most authentic and accurate way to identify network intrusions before they steal critical corporate data or cause other damage. SentinelOne's solutions provide the best possible adaptive defense in the war against cyber attackers with a critical tool in the war against cyber attackers.

Tomorrow's Threats Require a New Enterprise Security Paradigm

SentinelOne provides one platform to prevent, detect, respond, and hunt ransomware across all enterprise assets. See what has never been seen before. Control the unknown. All at machine speed.

Autonomous EPP + EDR

Real-time detection and remediation of modern attacks at the endpoint, at machine speed, and without human intervention.

Unprecedented Visibility

Contextualize and identify threats in real-time. Storyline™ technology reduces manual effort and automatically strings together related events in an attack storyline.

Frictionless Threat Resolution

Patented Storyline™ enables 1-click remediation and rollback to accelerate recovery to real-time. Storyline Active Response or STAR™ provides proactive detection and response. For threat hunters and responders, remediation is integrated as a standard EDR response.

Simplified Experience

One agent consolidates security functions and reduces agent count. One console unfies administration of devices and cloud workloads. Fast to deploy. Easy to manage.

Exceptional Customer Experiences

Customers are our #1. The proof is in our high customer satisfaction ratings and net promoter scores that rival the globe's best companies.

SentinelOne Vigilance

Get answers, not alerts, with our managed detection, investigation and response service.

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733

Get a Free Demo

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2022 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 Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP

TEVORA PCI DSS Attestation HIPAA Attestation

AICPA SOC

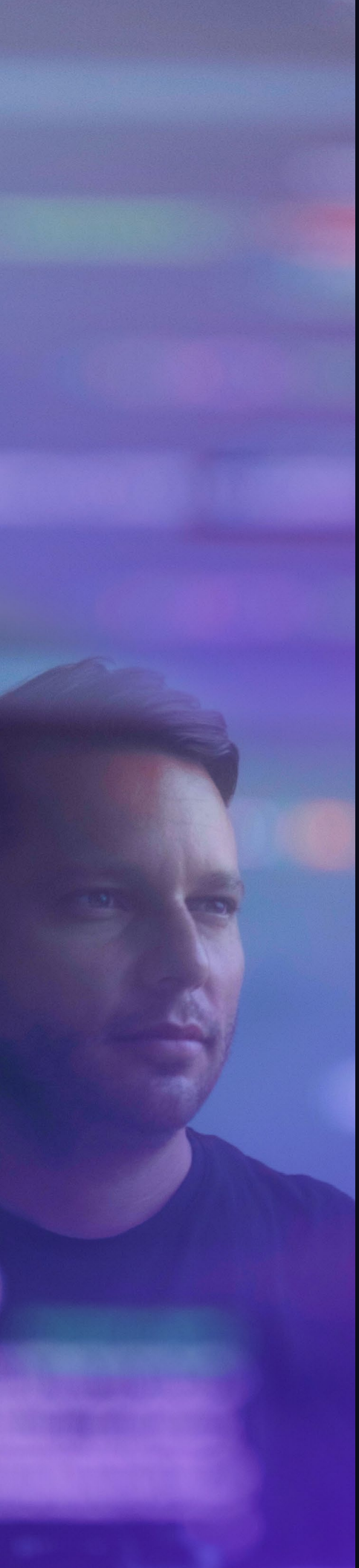
STAR LEVEL ONE

VB 100 VIRUS

SE Labs BEST Innovator WINNER 2021

AAA

Trusted Cloud Provider CSA



SentinelOne

Contact us

sales@sentinelone.com

+1-855-868-3733

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

sentinelone.com

Deception_for_Inside-the-Network_Threat_Detection_05162023

© SentinelOne 2023