SentinelOne White Paper

SentinelOne®

Moving to an Endpoint-Centric **Zero Trust Security Model with SentinelOne**

October 2021

Table of Contents

01

Abstract

Zero Trust Network (ZTN) concept follows the mantra of never trust, always verify. Through this approach, organizations can reduce their open attack surface and adopt enhanced security capabilities beyond traditional defenses. In this paper, you will learn how SentinelOne can help enterprises embrace an endpoint-centric zero trust strategy using the SentinelOne Singularity™ platform.

02

Introduction

The requirements for security professionals have changed dramatically in recent years with the rapidly evolving threat landscape, redefinition of how and where employees work, and adoption of new technologies like cloud computing, Internet of Things (IoT), and 5G. Today, security teams embrace the concept of assuming breach, as many understand that it's not if you will be compromised, but when. Therefore, organizations invest in people, processes, and technology that help them protect, detect, respond, and recover from threats as effectively as possible.

Historically, most corporate applications and solutions that store corporate data were protected behind the corporate network. With the adoption of cloud applications and the mobile workforce, this has changed dramatically. Today, many applications or storage solutions that were unthinkable to be accessible outside the corporate network are hosted on cloud-native solutions and are accessible from virtually anywhere. For this reason, the old perimeter that security professionals would set and protect no longer exists, and perimeter-based security models are obsolete. As a result, many organizations are looking for a new security model that helps them to protect against the modern threat landscape, supports remote work scenarios, and reduces the attack surface to a minimum aperture. These are all critical capabilities of Zero Trust, and when successfully adopted by an organization, they can equip organizations with a robust and flexible security model.

Today, endpoints represent the most significant attack surface, with over 70% of breaches[1] originating on the endpoint. Organizations have a heterogeneous mix of them connected to their network, whether laptops, mobile endpoints, servers, or IoT devices. Therefore, SentinelOne recommends an endpoint-centric Zero Trust security model that works regardless of where the user is located, whether in the corporate network, at a coffee shop, or at home. SentinelOne's approach brings trust verification as close to the user as possible, turning endpoints into effective zero-trust policy enforcement mechanisms.

1 IDC: 70% of Successful Breaches Originate on the Endpoint (Rapid7)

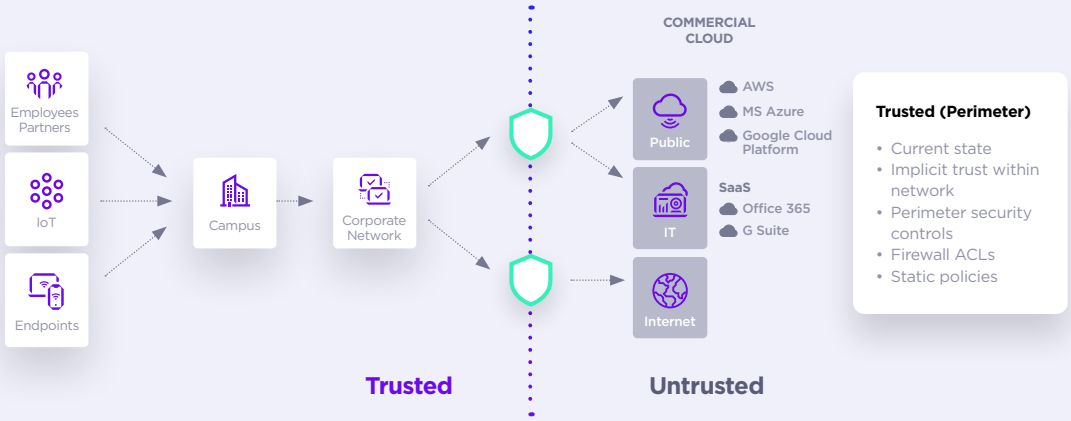
03

History

There have been many security paradigms over the past decades including defense-in-depth, least privilege, micro-segmentation, containerization, and Multi Factor Authentication (MFA). Each of these paradigms represents a mindset of how the different security tools in your organization should be architected to work with each other.

Layered network defenses have been the traditional approach to security for decades. Network-centric methods relied heavily on physical sensors—like firewalls, Intrusion Prevention System (IPS), and Intrusion Detection System (IDS)—to control and secure north-south traffic. Access to corporate resources was binary, based on whether the user was inside or outside the firewall. Once inside the firewall, trust was implicit and given freely.

Legacy Perimeter



In recent years, rises in phishing, supply-chain-based attacks, insider threats, and credential compromise attacks have made organizations reconsider the 'trust by default' approach. Insider credentials can be taken advantage of for elevated access, therefore presenting themselves as attractive targets for attackers. In contrast to attacks originating from outside of the corporate network, adversaries can leverage the implicit trust given to identity to move laterally within an organization's network.

Additionally, the COVID-19 pandemic has accelerated digital transformation efforts for many organizations. IT teams were forced to rapidly stand up infrastructure to support an instant remote and later hybrid workforce. New solutions were deployed to enable business continuity, including cloud infrastructure and Software-as-a-Service (SaaS) platforms like Zoom and Office 365. IT teams adopted solutions that could scale and deploy without needing access to the physical data center, in some cases deploying applications that were exposed to the open internet. In parallel, many organizations needed to provide endpoints for new remote employees and roll out bring your own device (BYOD) programs. In reality, securing these new operating environments was a secondary concern.

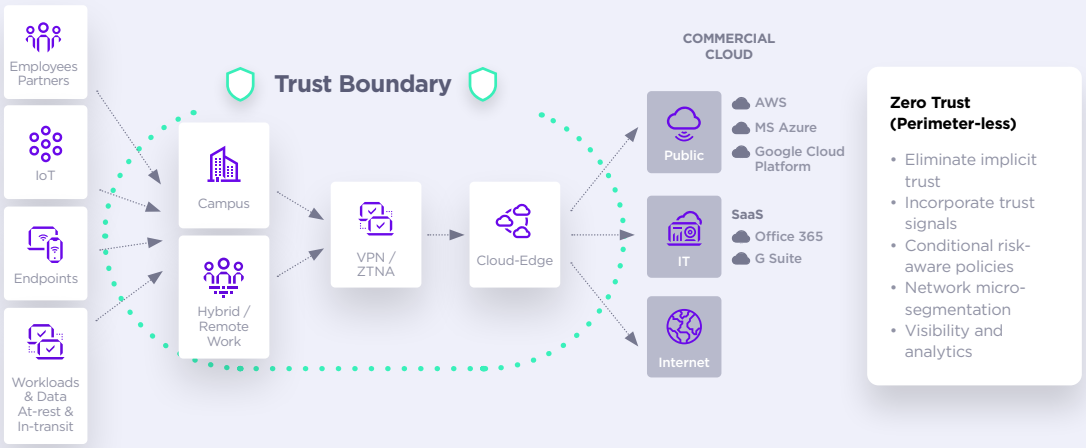
All of these radical shifts resulted in users accessing applications and data outsides of the traditional corporate network. While some organizations tried to scale their on-premises infrastructure to cope, creating a new perimeter around the new compute-where-you-are operating environment with legacy tooling requires too much effort and is prohibitively expensive. Changes in attacks and attack surfaces have necessitated a new approach that ensures every endpoint can be trusted.

04

Zero Trust Overview

Whereas legacy models are focused on neutralizing threats originating outside an organization's network, Zero Trust acknowledges that threats may well exist both inside and outside the network. Legacy security models trust, by default, the endpoints and identities within their sphere of influence; In contrast, Zero Trust follows the principle of never trust, always verify all endpoints, all identities. By successfully adopting Zero Trust, organizations can perform risk-based access control and leverage the concept of least privileged access for every access decision.

Zero Trust Perimeter



Forrester defines Zero Trust as "moving security from a network-oriented, perimeter-based security model to one based on continuous verification of trust." Zero Trust is not a product, but rather a modern security model composed of multiple cooperative trust verification layers that are triggered and tested regardless of the device's location. A Zero Trust ecosystem aggregates multiple sources of trust signals from identity, endpoint, workload, and network to provide a point-in-time access decision.

Guiding Principles of Zero Trust

- **Never trust, always verify**
  Treat every user, endpoint, application or workload, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege required.

- **Assume breach**
  Operate and defend resources with the assumption that an adversary already has a presence within the environment. Deny by default and scrutinize all users, endpoints, data flows, and requests for access.
- **Verify explicitly**
  Dictate access to all resources in a consistent and secure manner using multiple trust signals for contextual access decisions.

05

Attack Simulation

By comparing two attack simulations, we can begin to understand the strengths of Zero Trust' continuous security compared to the prototypical (and now legacy) perimeter-centric security model with a hard exterior and soft interior.

Legacy Architecture

Zero Trust Architecture

06

Zero Trust Maturity Level

As organizations move from a legacy to Zero Trust security model, they look for best practices and guidelines on achieving said model as quickly as possible, but changing the security model of an organization isn't achieved overnight. The journey is a marathon, not a sprint.

While some of the existing investments of an organization can be leveraged or integrated into a Zero Trust security model, the transition will require additional capabilities and resources to fully utilize all the benefits of a Zero Trust security model. To achieve that, SentinelOne recommends the following components:

Traditional – manual configurations and attribute assignment, static security policies, least-function established at provisioning, proprietary and inflexible policy enforcement, manual incident response, and mitigation capability.

Advanced – some cross-solution coordination, centralized visibility, centralized identity control, policy enforcement based on cross-solution inputs and outputs, some incident response to pre-defined mitigations, some least-privilege changes based on posture assessments.

Optimal – fully automated assigning of attributes to assets and resources, dynamic policies based on automated/observed triggers, assets have dynamic least-privilege access (within thresholds), alignment with open standards for cross-pillar interoperability, centralized visibility with retention for historical review.

	Identity	Endpoint	Network	Workload
Traditional	• Password or multifactor authentication (MFA) • Limited risk assessment	• Limited visibility into compliance • Basic inventory	• Large macro-segmentation • Minimal encryption	• Access based on local authentication • General purpose protection for known threats • Some cloud accessibility
Advanced	• MFA • Identity federation with cloud and on-prem	• Compliance enforcement • Data access based on device posture	• Micro-segmentation at ingress/egress • Basic analytics	• Access based on centralized authentication • Protections for known threats with application-specific protection
Optimal	• Continuous validation • Real-time dynamic analysis	• Constant monitoring and validation • Data access relies on real-time risk score	• Distributed micro-segmentation • ML threat detection (NDR) • All traffic encrypted	• Access is authorized continuously • Analytics to provide protections that account for application behavior

Visibility, Analytics & Automation

07

Building a Zero Trust Security Model

Transitioning security models can be complex and time-intensive. Every organization has its own unique requirements, use cases, and existing technologies. These factors can affect the successful transition to a Zero Trust security model. SentinelOne recommends to map based on the Zero Trust maturity level line of businesses and then define a phased approach in transitioning the security model. The below is a suggested approach on how to jump-start the Zero Trust project for your organization.

John Kindervag, former VP & Principal Analyst at Forrester, and creator of the Zero Trust methodology suggests a five-step deployment guide for Zero Trust:

01. Define Your Protect Surface

Most organizations try to reduce the exposed attack surface as much as they can. But in reality, regardless of the investments, there will always be an open attack surface that attackers will find and exploit. Therefore instead of looking for the attack surface, the question becomes what is the protected surface which includes critical data, application, assets, and services (DAAS).

02. Map the Transaction Flows

Most organizations as they transition from networker perimeter-based security to modern architectures are aware of their network and how to protect it. What changes is the fact that organizations need analytical insights of DAAS within the network? How are critical data accessed? How can anomalies be detected?

03. Architect the Environment

There is no such thing as an architectural blueprint that fits all organizations in the world. This statement remains true as organizations embrace the move to a Zero Trust architecture. ZTN designs are unique per organization because they are determined by your protected surface and DAAS. Ideally, you want to bring security controls as close as possible to your protected surface by defining micro-perimeters and ensuring across all aspects that access requests are always verified based on the health state of the entity requesting the access.

04. Create the Zero Trust Policy

Determine the Zero Trust policies by answering who, what, when, where, why, and how should get access to corporate resources and services.

05. Monitor and Maintain the Environment

The final step is about gathering telemetry, leveraging autonomous solutions to perform analytics and detect anomalous and automatically respond based on the defined zero trust policies.

08

Zero Trust Best Practices

SentinelOne can help organizations successfully adopt a Zero Trust security model for their entire organization from the digital estate, including workplace, data center, mobile, and cloud workloads.

Endpoints

Today endpoints, regardless if they are workstations, laptops, mobile devices, or servers, often have different configurations, patch statuses, operating systems, leading to inconsistent approaches to applying security policy. This problem is compounded by the rise of bring-your-own-endpoint (BYOD) and the loss of visibility from legacy network controls due to the rise of remote and hybrid working practices.

Adopting Zero Trust for endpoints can assist organizations in reducing this risk by providing the means to monitor, isolate, secure, control, and remove any endpoint from the network at any time. When integrated into a Zero Trust ecosystem, endpoints can provide valuable trust signals when determining whether to grant network access, including the endpoint's identity, health, and compliance status.

Endpoint Detection and Response (EDR) solutions provide visibility, detection, and response and act as an organization's primary control point for endpoint security. EDR solutions collect telemetry from endpoints, correlate to detect malicious activity, and facilitate the response and remediation of threats. When EDR is paired with Endpoint Protection (EPP) as a preventative control, organizations have a complete understanding of the endpoint attack surface and threat posture.

Integrating endpoint trust signals into a Zero Trust ecosystem can help answer the following questions and deny access to applications and resources based on the policy:

- Is the endpoint currently affected by malware?
- Is the endpoint demonstrating aberrant network behavior?
- Is the user accessing from a corporate managed endpoint?
- Is the endpoint accessing from a known location?

While security teams deploy EPP and EDR controls to endpoints they manage, there are a significant number of endpoints that remain unmanaged or unable to take a management agent.

Unmanaged endpoints are more vulnerable to compromise and introduce risk to the environment if allowed to access corporate resources. Organizations should strive to isolate unmanaged devices, close the EDR deployment gap by leveraging technologies that can perform network discovery, and automatically deploy the EDR agent on unmanaged endpoints.

Workloads

Digital transformation's innovation pace is enabled principally by nimble cloud workload technology. However, organizations have traded reduced time to market for environmental security. Agile development practices that emphasize iteration and speed can overwhelm security teams who are not prepared to secure workloads as fast as they are created. This friction between DevOps and SecOps creates bottlenecks and an incentive for development teams to circumvent security and governance processes. As a result, there are often blind spots for security teams tasked with keeping cloud environments secure.

Governance of workloads is often performed just once when the workload is deployed, or sometimes not at all. And the specific configuration of workloads is inconsistent, with many instances deployed without critical controls. Confusion often abounds and incorrect assumptions made by DevOps regarding workload security according to each cloud provider's shared responsibility model. Regardless of the public cloud environment, it's the organization's responsibility to monitor their cloud attack surface, which is just as vulnerable to compromise as user endpoints.

According to Forrester, "public cloud migrations and other disruptive IT changes have often acted as a good vehicle for achieving a Zero Trust security model." A Zero Trust solution for workloads must provide a repeatable and consistent approach to securing private, public, hybrid, and multi-cloud environments. It requires an active inventory of all cloud assets, configuration status and health, and measures to preserve workload immutability. As such, cloud governance is not a one-time activity but one that happens continuously.

Workload controls can help answer the following questions and adjust container operation based upon policy:

- Is the workload deviating from the baseline?
- Is the workload affected by malicious activity?
- Is the workload vulnerable to attack?
- Who has access to the workload?

Using this information, security teams can create Zero Trust access policies using real-time information about workload's runtime security, compliance status, and security posture.

Identities

Forrester notes that IAM is one of the least mature areas and one of the top 3 vectors for external attacks. Compromised credentials and insider threat attacks are a large and often difficult to mitigate attack surface. With compromised identities, attackers can impersonate employees as well as perform man-in-the-middle attacks to exploit trusted identities for their advantage. Identity is a critical component of a Zero Trust ecosystem and many organizations begin their Zero Trust journey by using identity as a lever.

Identity serves as a one-to-many enforcement point for least privilege and identity and access management (IAM) remains an effective preventative control point. Identity management is complex - tracking employees, customers, partners, and service accounts across environments, each with varying levels of entitlement and privilege. Zero Trust for identity governs entitlement and provides least-privilege access policies.

Rather than providing unfettered access, conditional access policies should provide the least required amount of privilege required to perform a task. Continual authentication for end-users often adds friction, so it is crucial that Zero Trust implementation automates the experience as much as possible.

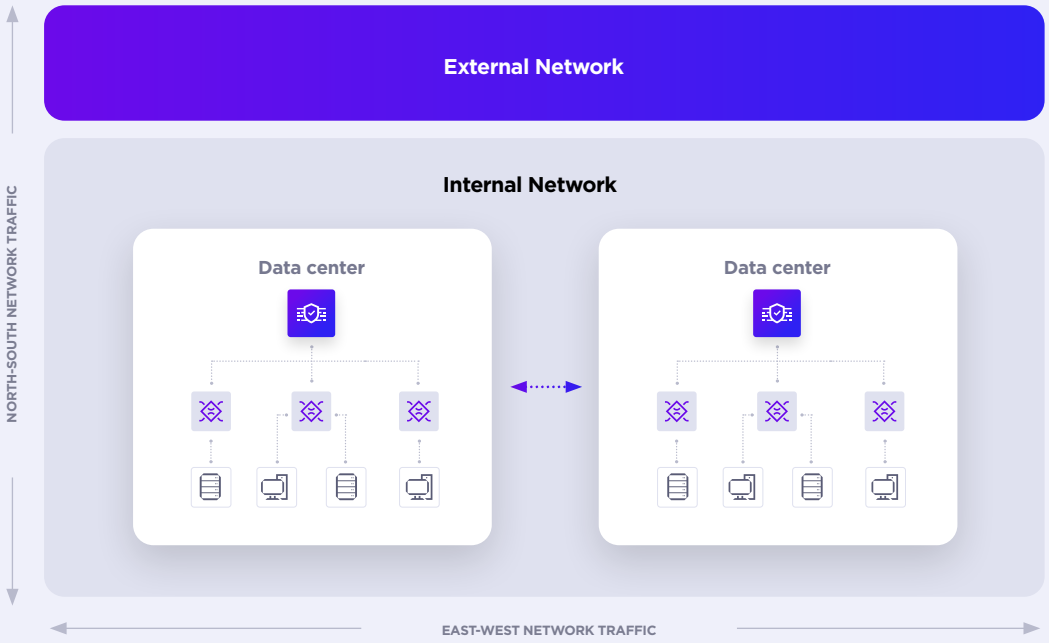
Common implementations of Zero Trust for identity are conditional access, single sign-on (SSO), and multi-factor authentication (MFA). These technologies should be deployed in conjunction with a formalized identity governance and entitlement access reviews to ensure that users are not over-provisioned privileges.

Networks

Networks have evolved due to the rise of remote work, and our perception of the network perimeter has evolved as well. Managed networks are no longer contained to a single location; they exist wherever devices, cloud workloads, and mobile devices access corporate resources.

Previously, it was considered good practice to mirror network security after physical security. Once someone was through the front door, they could move around as needed, whether that was in the building or on the network. Now, with much of the population still distributed and working from home becoming a more permanent part of the culture, the boundary of the workplace moves from the organization's firewall to the endpoints. This means that the assumption must always be made that any endpoint is connected via a hostile network and the operator may not be who they say they are. To operate in this environment, trust must be requested and granted on a granular scale which often means on a per application basis.

Zero Trust for network facilitates the proactive hardening of network-accessible resources and east-west traffic within the network using micro-segmentation. Logical micro-segmentation creates isolated access zones for an application and its associated hosts, peers, and services. Micro-segmentation furthers Zero Trust by limiting the ability for attackers to move laterally within the environment. If a given segment of the network is compromised, micro-segmentation will ensure that the threat actor or ransomware cannot compromise adjacent resources or services.



In a remote environment, Zero Trust Network Access (ZTNA) helps address the security of north-south traffic between the internal network and cloud-based internal resources. Zero Trust Network Access solutions inspect multiple sources of trust signals, from both endpoints and identity providers to ensure that the request is valid before granting access to SaaS applications and corporate resources. Following Zero Trust principles of verifying explicitly and assuming breach, the endpoint must prove that it is trustworthy to gain access. Using ZTNA with endpoints provides the means for a risk-aware network access policy.

Additionally, Network Detection and Response (NDR) solutions provide visibility for detecting and are an effective control point for responding to network-borne threats. NDR solutions log, inspect, and continuously monitor all network traffic for suspicious activity. NDR solutions can help answer a broader range of questions when responding to an incident or hunting for threats, such as:

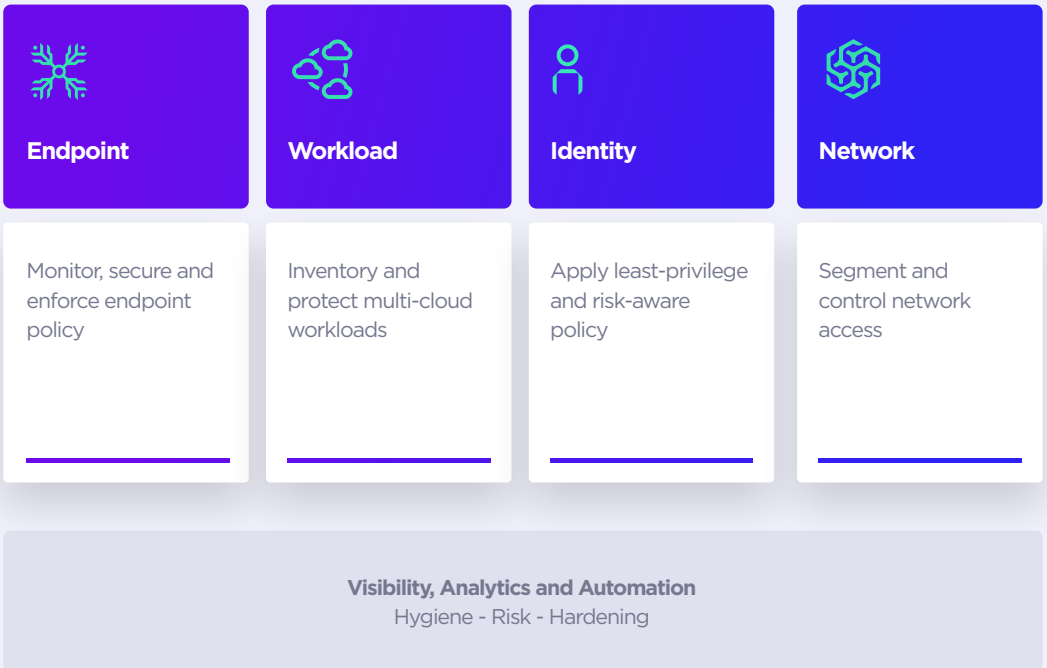
- Did another asset begin to behave strangely after communicating with the potentially compromised asset?
- What service and protocol were used?
- What other assets or accounts may be implicated?
- Has any other asset contacted the same external command-and-control IP address?
- Has the user account been used in unexpected ways on other devices?

08

Zero Trust powered by SentinelOne

SentinelOne's approach to Zero Trust provides the means for security teams to continuously monitor and manage the hygiene, risk, and hardening of their entire estate as part of a Zero Trust strategy.

SentinelOne for Zero Trust



Hygiene

Preventing, detecting, responding, and recovering from cyber threats

In a Zero Trust environment, everything is assumed to be breached, and endpoints and cloud workloads must prove otherwise. Before granting access to corporate resources, a Zero Trust solution must first check whether the device requesting access is compromised.

- SentinelOne's patented on-endpoint Behavioral AI predicts, stops, and corrects the effects of known and unknown threats in real-time. SentinelOne's agent can be deployed across all major operating systems to monitor and continuously assess endpoint health with or without an internet connection.

- Patented 1-click remediation automates threat resolution with fully autonomous responses that trigger protective actions in real-time. SentinelOne provides a clear picture of an endpoint's health, management status, and the ability to automatically quarantine or remediate it to bring the device into compliance.

- SentinelOne Singularity Cloud provides runtime protection and EDR for virtual machines (VMs) and containerized workloads. Organizations can manage and secure hybrid, private, and multi-cloud workloads from a single console with a single agent. Workload health status is available in real-time and automatically brought back into compliance.

- Singularity Mobile brings behavioral AI-driven protection, detection, and response to iOS, Android, and ChromeOS devices. Part of the Singularity™ Platform, SentinelOne delivers mobile threat defense that is local, adaptive, and real-time, to thwart mobile malware and phishing attacks at the device, with or without a cloud connection. And because it's mobile, data privacy is built-in at every level. Singularity Mobile works with or without an MDM, and integrates with all leading MDM solutions. The on-device agent provides protection and detection of both mobile malware and phishing, known or unknown, with minimal battery consumption for an optimal end-user experience.

Risk and Governance

Visualizing, managing, and mitigating risk

Making data-driven decisions is critical for security teams. Organizations need to fully understand possible risks, blind spots and the attack surface before security policies can be effectively applied.

- With the exponential increase of connected endpoints and the often complex and varying configurations of cloud workloads, it has become difficult for organizations to understand who is inside the network and how workloads are configured compared to industry standards like CIS.

- To gain visibility into the network, SentinelOne Singularity Ranger turns endpoints into distributed network sensors that provide monitoring of the enterprise attack surface in real-time. SentinelOne agents actively fingerprint and inventory all IP-enabled endpoints on the network to identify abnormal communications and open vulnerabilities.

- With Ranger, risk from devices that are not secured with SentinelOne can be mitigated by either automatically deploying an agent or isolating the device from the secured endpoints. This is how Ranger can be used to effectively reduce the attack surface.

- Singularity Conditional Policy is SentinelOne's endpoint-centric Conditional Policy engine. SentinelOne empowers organizations to dynamically change security policies based on the risk level of the endpoint through this capability. With that, endpoints are no longer trusted by default but rather are continuously verified. When an incident occurs, the security policies are dynamically hardened in real-time to reduce the attack surface and prevent any potential damage.

Hardening

Designing and implementing preventative measures

One of the core principles of Zero Trust is to embrace the least privilege and default-deny policies until a user can prove they require elevated privileges.

- SentinelOne inventories all locally running applications from across the endpoint fleet and uses Storyline Active Response (STAR) rules to create a default-deny policy. A default-deny policy would restrict access to only approved applications and publishers, allowing the security team to manage by only by exception. This approach would significantly reduce the risk of compromise from unapproved or potentially malicious applications.

- SentinelOne's Device Control suite helps organizations embrace a more hardened posture for data loss prevention by restricting USB, Bluetooth, and Bluetooth Low Energy communications. Admins can restrict by endpoint class - for example, USB mass storage endpoints - which dramatically reduces the potential attack surface for insider threats and data loss.

- Preserving the unchanging, immutable state of a workload is an essential control for cloud workload protection. Application Control preserves the immutable nature of the workload by employing a default-deny posture for any new code not present in the validated initial VM or container image. Not only does this harden the image itself, but it prevents attackers from executing arbitrary code that could be used for compromise or lateral movement. Additionally, cloud application access control enables default-deny policies for access to cloud workloads and services. Cloud services are denied by default, reducing the amount of shadow IT and shadow cloud usage. Only approved endpoints will access the cloud resources and can be managed by exception by the security team.

Singularity Marketplace

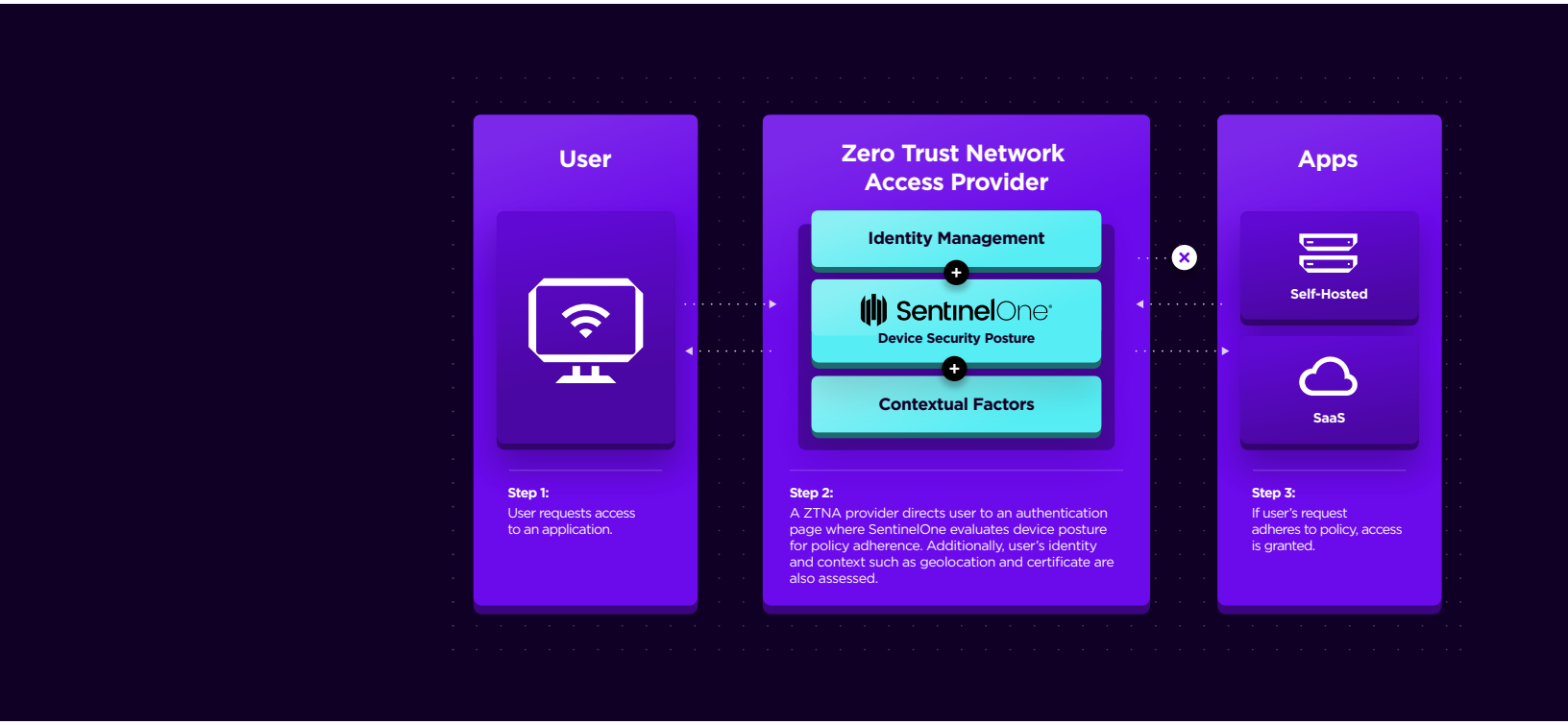
Connecting The Zero Trust Ecosystem

An effective Zero Trust framework integrates best-of-breed solutions and existing infrastructure to fill security gaps without a forklift upgrade of the security stack. SentinelOne has partnered with leading identity and network vendors to deliver validated Zero Trust solutions:

01. Network

SentinelOne's integration with Guardicore provides centralized visibility of network activity, including network data generated from endpoints and cloud workloads. SentinelOne agents report metadata to Guardicore that creates detailed visibility and network topology in the Guardicore for decision-making, forensics, and micro-segmentation policy creation. Policies can be exported from Guardicore, where they are enforced by SentinelOne's native firewall controls. Guardicore can define segmentation and micro-segmentation policies and then use the SentinelOne APIs to enforce them on the agent.

SentinelOne's integrations with Zscaler and Cloudflare use device signals from SentinelOne to inform Zero Trust Network Access decisions. Information about the endpoint, including whether it is managed and has a SentinelOne agent installed, is provided to Zscaler and Cloudflare. This information is combined with contextually relevant information from an identity provider to determine a point-in-time network access decision.



SentinelOne integrates with a number of NDR solutions including Vectra AI, Awake Security (Arista Networks), and Fidelis. The combination of SentinelOne's EDR with partner NDR

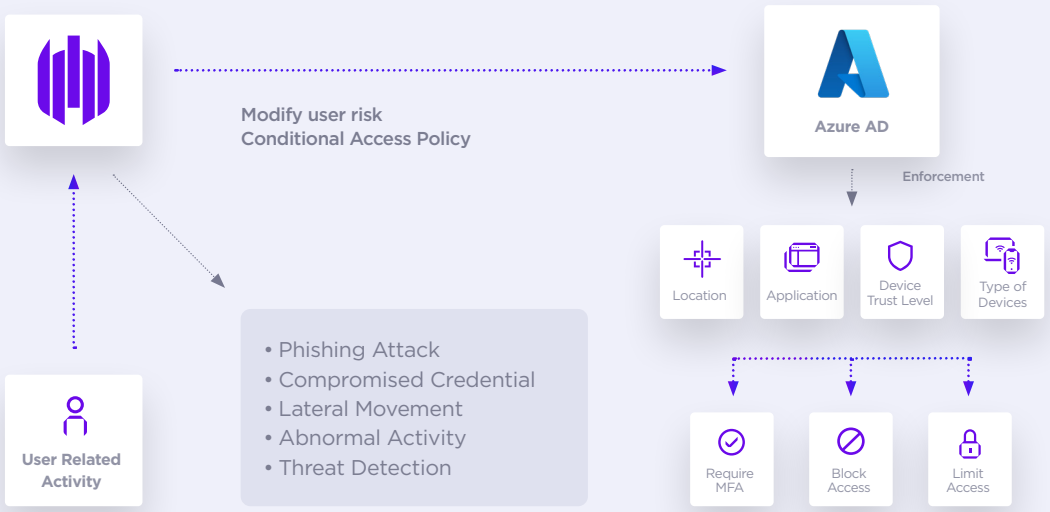
capabilities provides visibility, detection, and response for both managed and unmanaged endpoints. While NDR connects related network activity into a broader attack map, SentinelOne provides contextual awareness by enriching information coming from managed endpoints such as device name, last logged-in user, operating system details, and other endpoint characteristics. This provides comprehensive threat detection, rapid and effective response, endpoint containment, and forensic analysis capabilities.

02. Identity

SentinelOne integrates with Azure Active Directory to provide identity-focused Zero Trust solutions. Conditional access is a key part of Zero Trust because it helps to ensure the right user has the right access to the right resources. Enabling Conditional Access allows Azure Active Directory to make access decisions based on computed risk and preconfigured policies. When an endpoint is compromised SentinelOne pushes this information in real-time to Azure Active Directory ensuring that the organization can leverage their conditional policy to block a user, limit user's access, or trigger MFA.

Enforce Access Control Requirements

Change requirements uppon of detection of risky events or activities



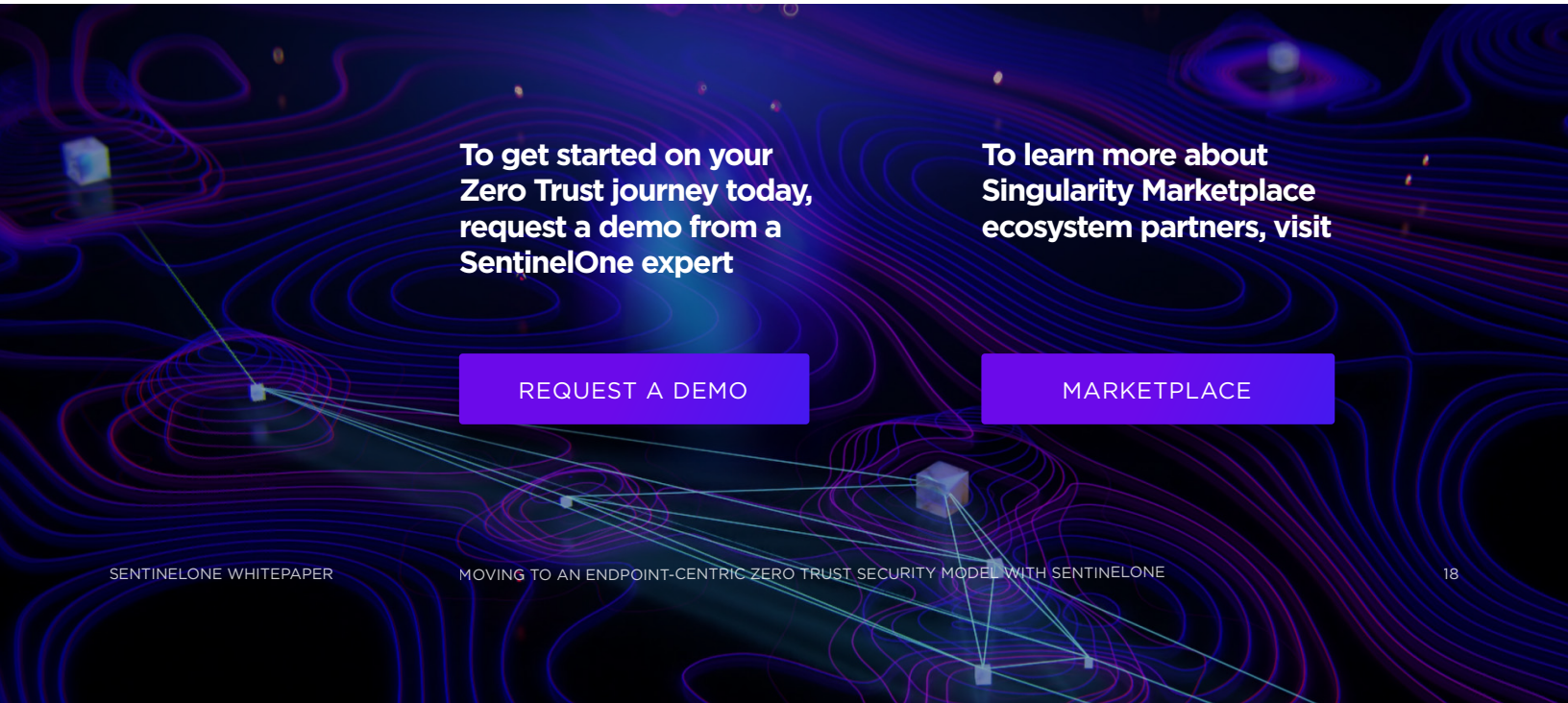
Additionally, SentinelOne can share identity risk information with Azure AD that is factored into conditional policy. For example, if SentinelOne detects an attack on an endpoint, it will provide the last logged-in user to Azure AD with a high user risk level. Using this information, Azure AD will enforce identity policy, such as resetting the password or blocking a user.

Finally, the risk score that Azure AD generates for a given identity can be used in SentinelOne to inform triage and investigation. Identity risk information is surfaced within the SentinelOne console and provides analysts with at-a-glance context about a given identity.

SentinelOne natively integrates with Okta to bring identity context and response actions directly within the Singularity XDR platform. SentinelOne consumes logs and contextual events from Okta and displays them alongside relevant endpoint detections. With identity visibility, analysts can see additional identity activity that may be relevant for an investigation. When corrective mitigation needs to take place, response actions within SentinelOne can revoke an identity or trigger MFA.

10 | Conclusion

SentinelOne's approach helps organizations advance Zero Trust maturity by leveraging existing endpoint, cloud workload, identity, and network security investments. With native capabilities and integrations, organizations can begin the journey to more effectively applying Zero Trust principles.



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

Moving_to_an_Endpoint-Centric_Zero_Trust Security_Model_with_SentinelOne_10142021