TRUEFORT™

SOLUTION BRIEF

TrueFort Platform and SentinelOne

A Zero Trust segmentation and workload protection platform that understands application behavior

Executive Overview

Your applications make you vulnerable to cyberattacks. While most companies focus their security efforts on network and endpoints, they don't adequately invest in security measures within the data center and cloud. To ensure critical workload protection you need to continuously identify suspicious activities as they're happening, through continuous analysis against trust baselines of the workload behavior under the lens of the applications they serve.

TrueFort offers an advanced approach to protecting data center and cloud workloads that makes zero-trust architectures possible. The TrueFort Platform uses application intelligent controls and continuous monitoring to deliver real-time detection and response the minute workload behavior strays from known, understood activity. By absorbing telemetry from the TrueFort agent and third-party agents, we decipher all intra-application communication and trigger alerts based on suspicious activity.

TrueFort extends your SentinelOne investment to deliver Zero Trust segmentation and workload protection by absorbing SentinelOne telemetry to visualize and baseline application flows dependencies. The Platform automatically generates policies from observed behavior, monitors for anomalies and enables policy enforcement. Understanding the context – what, who, when and how of the incident occurred – to enable smart risk prevention.

TrueFort offers an advanced approach to protecting data center and cloud workloads that makes zero-trust architectures possible.

WE PROTECT RUNTIME ENVIRONMENTS IN SIX KEYWAYS:

- **Cloud Workload Protection** – Secure workloads by dynamically adapting to unusual activities detected across on-premises and cloud workloads.
- **File Integrity Monitoring** – Validate any expected and unexpected changes to discover novel malicious activity.
- **Service Account Behavior Analytics** – Identify, monitor, and learn trusted connection patterns and block untrusted connections.
- **Workload Hardening** – Use adaptive configuration policy monitoring against CIS and company specific requirements, with notification when deviation from baseline occurs.
- **Microsegmenting Environments** – Intelligently baseline normal, high-volume activity within and between workloads, limiting future behavior to what should be trusted.
- **Container and Kubernetes Security** – Protect containers from compromise by baselining runtime behavior to find anomalies and respond in real-time.

How It Works

The TrueFort Platform combines visualization and analysis across the network, workload and applications and automates the discovery and mapping of complex security relationships. TrueFort builds upon SentinelOne's endpoint security telemetry with an adaptive trust approach that combines behavior analytics with real-time security telemetry to create a secure trusted behavioral profile for each application. Actionable deliverables include:

Discover and Map Dependencies – By incorporating the SentinelOne telemetry, TrueFort builds a unified, real-time view of all users, network, and process behavior within applications across cloud, virtual, container-based and traditional environment. A continuous application dependency map is built in real-time that captures all relationships within and between applications. This application dependency map serves as the foundation for the trust profile and applications behavioral policies.

Automate Policy Generation – TrueFort creates a trusted profile in conjunction with the TrueFort patented behavioral modeling or set of behavioral policies that are enforced by controls such as microsegmentation, even as applications are added or updated. TrueFort leverages the SentinelOne API's for policy enforcement thus no additional agents are required for microsegmentation.

Application Control Allow-Listing – By focusing on application behavior analytics, TrueFort identifies normal behavior and automate policy controls around execution permissions to the individual process-level. Our platform creates a learned, trusted behavioral profile which governs allow-lists of known running processes and their behaviors. Any executable outside of the allow-list is terminated.

Multi-dimensional Microsegmentation – Microsegmentation policies are based on the behavioral understanding of each application and all dimensions of behavior. TrueFort automatically generates and maintains, accurate segmentation policies without the guesswork or trial and error of competing solutions. Many microsegmentation projects fail because security teams lack context around connections to share with application owners and manage segmentation policies effectively. TrueFort removes the application context challenges by basing its intelligent segmentation policies on what it has learned about how applications behave in each environment and automatically updates segmentation rules, without user involvement, when workloads and IP addresses change.

TrueFort builds upon SentinelOne's endpoint security telemetry with an adaptive trust approach that combines behavior analytics with real-time security telemetry to create a secure trusted behavioral profile for each application.

Detect Anomalies – SentinelOne customers can leverage TrueFort anomaly detection to identify behaviors that may reflect the activities outside of the norm, without installing another agent. Additionally, customers can leverage DVR-like capabilities to play back events during incident response investigations answering which applications may have been impacted and how they were impacted as well as the underlying cause of the anomaly.

Threat Response Management – Response teams are quickly guided to the source of the event and information about its potential impact to applications in the context of the event. The TrueFort Platform includes a real-time security timeline view of event-related changes to the application environment so that response teams can contain incidents as they are happening, using either automation or manual intervention. TrueFort gives instant insight to all surrounding events to determine how localized or widespread an attack in progress has become.

Deployment & Integration

TrueFort can be deployed on-premises, in the customer's cloud, hosted on TrueFort Cloud or through a hybrid approach. It scales to hundreds of thousands of agents, without any latency concerns. For telemetry acquisition, TrueFort supports existing EDR/EPP agents, or existing security data lakes. TrueFort provides its own lightweight agent as an option to cover a wider range of operating systems (OS) and to enable full application protection controls.

TrueFort customers using SentinelOne endpoint security may leverage their existing agents to feed the TrueFort Platform with host telemetry and network segmentation policies. TrueFort will subscribe to SentinelOne's Cloud Funnel to get a constant stream of telemetry.

REQUIREMENTS

- SentinelOne Complete with Deep Visibility running
- SentinelOne Agent version 2.8 or later

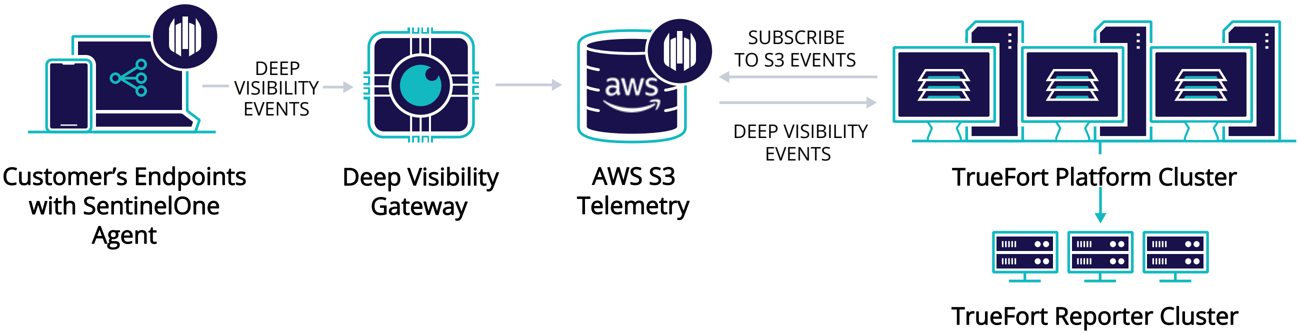

FIGURE 1: TrueFort SentinelOne Integration

ABOUT TRUEFORT
TrueFort is an advanced approach to protecting data center and cloud workloads that makes zero-trust architectures possible. Our platform uses continuous monitoring to deliver real-time detection and response as soon as noisy workload behavior strays from known, understood activity. By absorbing telemetry from multiple agents, we decipher all intra-application communications and trigger suspicious activity alerts. The TrueFort Platform is the only solution instilling the confidence to protect workloads across all production environments. By reducing the impact of security incidents, we increase your overall business resilience, shrink your exploitable attack surface, and enable you to take immediate action against live attacks. We bring the single truth security and application owners need to effectively protect workloads of all forms.

For more information, visit truefort.com and follow us on Twitter and LinkedIn.

TRUEFORT™

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM