TRUEFORT

SOLUTION BRIEF

Microsegmentation on SentinelOne Agents

Zero Trust segmentation and workload protection that understands application behaviour

Executive Overview

Applications can make organizations vulnerable to cyberattacks. While many companies bolster network and endpoint security, data center and cloud protections often lag. Continuous identification of suspicious activities and analysis against trust baselines is vital.

The TrueFort Platform provides an advanced solution for data center and cloud security, supporting zero-trust architectures. The platform's intelligent controls offer real-time detection by analyzing intra-application communication.

TrueFort enhances SentinelOne integrations, offering Zero Trust segmentation and workload protection. It uses telemetry to visualize application flow dependencies, auto-generates policies from behaviors and provides a deep understanding of security incidents for effective risk prevention.

How It Works

The TrueFort Platform offers integrated visualization and analysis for networks, workloads, and applications, streamlining the identification of intricate security links. Leveraging SentinelOne's endpoint data, TrueFort merges behavior analytics with real-time telemetry to craft trusted behavioral profiles for applications, producing actionable insights.

Discover and Map Dependencies

Using SentinelOne telemetry, the TrueFort Platform creates a real-time, unified view of user, network, and process behaviors across various environments. This leads to a dynamic application dependency map, capturing inter-application relationships, which underpins trust profiles and behavioral policies.

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** – Dynamically adapt to irregularities in both on-premises and cloud workloads.
- **File Integrity Monitoring** – Track and verify all file changes to spot malicious activities.
- **Service Account Behavior Analytics** – Monitor trusted connection patterns and block untrusted ones.
- **Workload Hardening** – Adaptively monitor configurations against CIS and specific standards, alerting on deviations.
- **Microsegmenting Environments** – Smartly establish baselines within and between workloads to ensure trusted behavior.
- **Container and Kubernetes Security** – Safeguard containers by monitoring runtime behaviors, detecting anomalies in real-time.

The TrueFort Platform provides an advanced solution for zero-trust protection of data center and cloud workloads.

Automate Policy Generation

TrueFort establishes a trusted profile using its patented behavioral modeling and enforces policies like microsegmentation as applications evolve. By integrating with SentinelOne APIs, there's no need for extra agents for microsegmentation.

Application Control Allow-Listing

TrueFort uses application behavior analytics to identify and automate standard behavior policies. The platform establishes a trusted behavior profile, governing allow-lists for active processes. Any executable not on this allow-list is terminated.

Multi-dimensional Microsegmentation

TrueFort's microsegmentation policies are rooted in the comprehensive behavioral insights of each application. Instead of the trial and error approach seen in other solutions, TrueFort automates the creation and updating of accurate segmentation policies. While many microsegmentation initiatives falter due to insufficient context, TrueFort's intelligent policies leverage application behavior knowledge and auto-update to account for changes in workloads and IP addresses, streamlining the process without manual intervention.

Detect Anomalies

SentinelOne users can utilize TrueFort's anomaly detection to spot unusual behaviors without needing an additional agent. They can also use DVR-style features to review events during incident investigations, determining affected applications, their impact, and the root cause of the anomaly.

Threat Response Management –

TrueFort swiftly directs response teams to an event's source and its potential application impact. The platform provides a real-time security timeline of application changes, enabling teams to promptly contain incidents through automation or manual efforts. TrueFort also offers immediate insights into the scope of an ongoing attack.

Deployment & Integration

TrueFort can be deployed on-premises, in customer clouds, on TrueFort Cloud, or through a hybrid method. It efficiently scales to manage hundreds of thousands of agents without latency issues. It supports existing EDR/EPP agents and security data lakes, but also offers its own lightweight agent for broader OS compatibility and comprehensive application protection.

Customers using SentinelOne can integrate their agents with TrueFort to receive host telemetry and network policies, with TrueFort continuously accessing SentinelOne's Cloud Funnel for telemetry.

REQUIREMENTS

- SentinelOne running Deep Visibility
- SentinelOne Agent version 2.8 (or later)

ABOUT TRUEFORT

TrueFort® puts you in control of lateral movement across the data center and cloud. The TrueFort Cloud extends protection beyond network activity by shutting down the abuse of service accounts. Founded by former IT executives from Bank of America and Goldman Sachs, leading global enterprises trust TrueFort to deliver unmatched application environment discovery and microsegmentation for accounts and activity.

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