TRUEFORT™

SOLUTION BRIEF

TrueFort™ Platform

Zero Trust segmentation and workload protection that adapts to application behavior

Applications are an ever-increasing business risk. They control and manage your most business-critical data assets.

Movement to the cloud and the modernization of applications challenge traditional security tools. Attackers have more ways to get in while they are getting more sophisticated. These threats go undetected for months. Yet workload protection tools do not understand the workload and network activity within applications that attackers prey upon.

Challenges

- Attacks consistently succeed by adapting to new development tools and infrastructure
- Modern applications and the diversity of workloads – cloud, hybrid, virtual, containers & traditional on-premises – challenge existing security tools
- Existing segmentation tools put the burden of understanding users and workloads on the security team
- Threats – lateral movement, ransomware, supply chain attacks, and zero-day threats – easily go undetected
- Too many tools create ongoing alert fatigue with little to no focus on application context

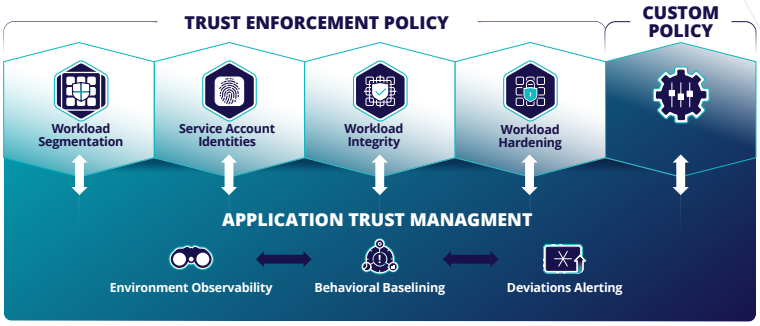
TrueFort™ has pioneered an application intelligent platform built to ensure security teams easily enforce a trusted baseline of workload behavior. The TrueFort Platform uses behavioral analytics with real-time security telemetry to establish a full process, user, and network behavioral profile across data center and cloud environments. TrueFort continuously analyzes workload behavior, in real time, against the baseline to immediately identify risky and anomalous activity. The positive security approach reduces the risk from the evasive attack techniques including compromised credentials, ransomware, supply chain attacks, lateral movement, and insider threats by ensuring workloads only behave as application owners require. For SOC analysts, TrueFort clearly replays all workload events from a few seconds ago to years in the past, making incident investigation and threat hunting effective in environments where it's most challenging.

SOLUTION HIGHLIGHTS

- Real-time anomalous threat detection
- DVR playback provides applications, actions and history to easily investigate
- Alerts on deviations from expected, trusted application behavior
- Automated, continuous monitoring against baselined normal activity
- Quickly identify and alert on untrusted behavior
- Continuous, adaptive trust profiling to limit the threat blast radius
- Baseline and monitor application-specific data, network access and configuration parameters
- Leverage application understanding (trust profile) to generate, maintain and segment policies without guess work
- Ingest existing third-party agent telemetry for instant protection

SOLUTION BRIEF

Consolidated in the TrueFort Platform are six standalone security controls that use workload behavioral baselining to instantly respond to compromise, segment workloads from critical data, spot abusive account usage and enforce optimal system configurations.



Controls

Cloud Workload Protection
TrueFort protects workloads from compromise by dynamically adapting to unusual activity to maintain protection across cloud, hybrid, virtual, containers & traditional on-premises environments.

Microsegmentation
TrueFort discovers and maps applications for intra-application dependencies, workloads and data flows into a trusted baseline of expected activity eliminating the attack surface.

File Integrity Monitoring
TrueFort provides in-depth insight to validate that changes in files, configurations and binaries are not the result of tampering or malicious replacement.

Workload Hardening
TrueFort's adaptive trust profiling enables security teams to shift to continuously validated configurations based on CIS and other standard preventing risks from reoccurring.

Service Account Behavior Analytics
TrueFort detects, monitors, and learns trusted connection patterns of human and non-human accounts, applications, and activity creating allow-listing policies for normal activities.

Container & Kubernetes Security
TrueFort protects containers from compromise by baselining runtime behavior to detect anomalies in real-time.

The TrueFort Platform offers real-time visibility, control, and response. By combining real-time telemetry into a live, fully visualized application intelligent platform, TrueFort enables security teams to quickly understand and implement security controls and policies to protect applications and workloads at the application level.

The only solution that protects applications from and through the application lens.

VISUALIZE + MAP
Clearly see applications, their components, and relationships using real-time and historical data

PROFILE + DETECT
Continuously learn and monitor app behavior, find anomalies & auto-gen policy and microsegmentation

PROTECT + RESPOND
Enforce, investigate and respond to zero-day & application events with unparalleled depth & clarity

ABOUT TRUEFORT
TrueFort is a comprehensive, real-time application and cloud workload protection solution. TrueFort continuously protects your organization's diverse application environment - cloud, hybrid, legacy - by exposing and mitigating hidden security risks to your business. Unlike infrastructure-centric approaches, TrueFort gives security teams an integrated, application-centric solution providing unprecedented visibility, control, and threat response capabilities to reduce the attack surface across an organization's entire application estate. TrueFort provides security teams with a range of powerful controls purpose-built to meet the requirements for comprehensive application environment protection.

TRUEFORT™

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM