WHITEPAPER

TRUEFORT™

TrueFort™ Platform Overview

A Zero Trust segmentation and workload protection platform that understands application behavior to protect it.

TRUEFORT.COM

WHITEPAPER

Ensuring Workload Protection Through the Applications They Serve

Modern businesses rely on a stable and secure foundation of applications and data.

Because applications manage most business-critical data assets, securing them from threats is a high priority for any organization. However, protecting the modern enterprise has become a huge security team challenge given the growing diversity of workload types (cloud, virtual, containers, bare metal), and the shift to DevOps in response to business needs. These challenges include teams having limited, if any, real understanding of how applications and their workloads behave and interoperate. Limited security operation visibility can mean ineffective, fragmented, and poorly implemented security controls as teams cannot protect what they cannot understand. Hidden risks remain hidden, and malicious lateral movement can remain undetected until long after the damage is done.

Infrastructure-centric security tools and approaches, while important to overall operational hygiene, aren't as effective in securing dynamic workloads because they lack the capabilities required to meet these unique, application-specific challenges.

Common challenges to protecting modern enterprise application environments include:

- **Limited operational visibility** into dependencies and interconnections across increasingly dynamic n-tier applications and their component workloads.
- **No unified security team view** of diverse workload deployments that include cloud, virtualized, container-based, and traditional.
- **Incomplete or non-existent application intelligence** for quickly assessing critical security challenges.
- **Inability to enforce valid application behavior** to safely stop attacks and correct for drift.
- **Inability to enable real-time detection and prevention** of unauthorized lateral movement.
- **Catching and correcting application changes** that introduce increased security risks to production environments.
- **On-going alert fatigue** with little, if any, application context for triaging business critical incidents.
- **Time-consuming and fragmented compliance reporting** across the entire application estate.

Adaptive Trust:

The Truefort Approach to Protecting Modern Workloads

TrueFort pioneered a new, advanced approach to protecting data center and cloud workloads that make Zero Trust architectures possible.

Instead of focusing only on securing disconnected infrastructure elements underlying each application (network, server, OS, software components), the TrueFort Platform uses an adaptive application trust approach that combines behavior analytics with real-time security telemetry to create a secure, trusted behavioral profile for each application that includes all component workloads. These adaptive trust profiles are then continuously analyzed using machine learning (ML) to create an environment-wide trust graph as an enforceable security baseline within and between all workloads. As business needs result in new deployments, or drive changes to existing applications, TrueFort automatically adapts its trust graph to maintain control across your entire application landscape.

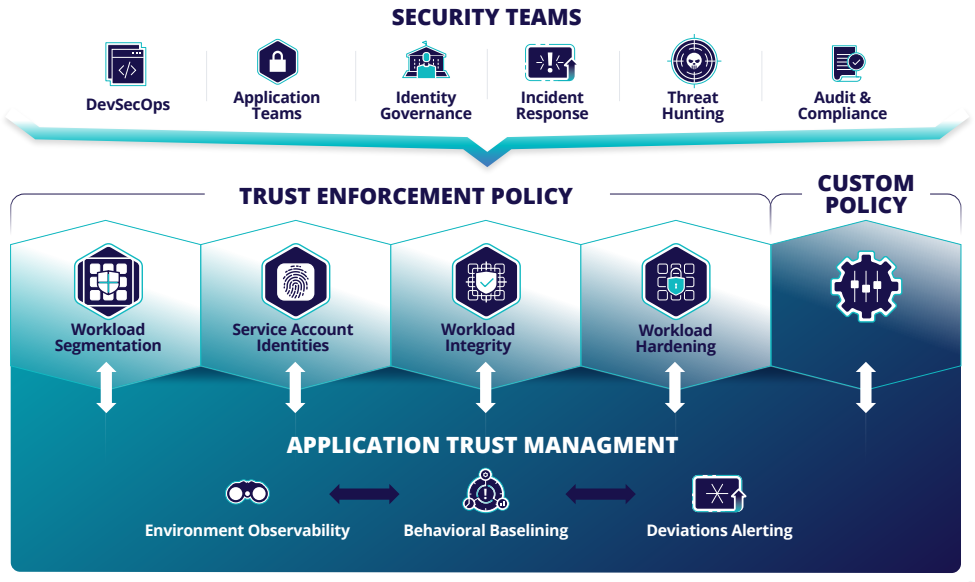

FIGURE 1: The Truefort Platform

The Truefort Platform Protection Features

TrueFort delivers three core modules that align to the requirements for protecting data center and cloud workloads.

These modules leverage the application intelligence and workload behavior analytics as the foundation of the TrueFort Platform. When combined, these capabilities give security teams unprecedented real-time detection, investigation, and response capabilities to dramatically reduce the impact of attempted application attacks.

Security Observability for Applications

TrueFort Platform uniquely combines visualization and analysis across network, workload, and applications in hybrid environments that align application owners and security teams. TrueFort automates discovery and mapping of complex security relationships within and between applications including dependencies and data flows. Security teams immediately see both known, approved relationships between applications, but also unknown and problematic activity. Teams can easily see the inventory of applications under protection, but also drill down into individual applications to assess the security of their underlying workloads and running processes.

By applying real-time behavior analytics to all telemetry to provide a live application behavioral mapping, TrueFort delivers true security observability for data center and cloud.

- **Unified, real-time view of all user, network, and process behavior** within applications across cloud, virtual, container-based, and traditional environments.
- **Detailed security mapping of both intra-application and inter-application relationships** including underlying component workloads and infrastructure.
- **Easily see trusted and untrusted relationships** between applications.
- **A full DVR-like investigation ability** to highlight a point in time and see all behavior that occurred
- **Keep CMDB systems up to date** with latest application dependency information.

Application Intelligent Controls

Workload Protection

Most security teams are burdened by having to use open-source tools and a mix of niche products that focus only on servers or network or containers to protect the application environment. These approaches typically involve scanning occasionally, sending patch requests to operations and waiting for the next scan to see if it improved. The problem with this approach is that security teams have no context for these changes, nor can they ask the application owners about their workloads with the long list of vague results they hold. TrueFort provides application-intelligent security controls designed around the needs of security and application owners to monitor and protect both data center and cloud.

Multi-dimensional Microsegmentation

Like network-based microsegmentation, host-based microsegmentation gives security teams the ability to restrict communications between applications, underlying workloads, and external resources. TrueFort Zero Trust segmentation goes beyond other limited microsegmentation products by leveraging its behavioral understanding of each application, and all dimensions of behavior from network connections, from user to network to the command executed. TrueFort automatically generates, and maintains, accurate segmentation policies without the guesswork or trial and error of competing solutions. Many microsegmentation projects fail for one simple reason: security teams lack application context connections to share with application owners and manage segmentation policies effectively. TrueFort solves that problem by basing its intelligent segmentation policies on what it has learned about how applications actually behave in each environment and automatically updating segmentation rules, without user involvement, when workloads and IP addresses change.

Workload Hardening

Using TrueFort's continuous monitoring for configuration drift, operations and compliance teams find out immediately when a workload violates internal policies and CIS industry standards. Rather than waiting for the next scan and sending patching requests to Operations, TrueFort users are alerted as soon as the secure state of a workload changes. Application-specific context of how the workload is used make corrective actions easily taken without concern of downtime.

Service Account Behavior Analytics

While Privileged Account Management (PAM) are highly effective at managing known privileged accounts, they aren't designed for discovery or behavioral analysis. PAM solutions focus on getting the people side of privileged account management right, but the service, or non-human accounts, are frequently both highly privileged and untracked. As a result, most organizations do not even realize the risk posed by service accounts or if they are orphaned or hardcoded throughout their application environment.

Further, these credentials may be embedded in code or stored procedures, and if compromised, lead to stealthy lateral movement to many workloads and critical data. TrueFort gives security teams real-time visibility into the service identities in everyday use, what their behaviors are, and when they stray from their standard, approved use. Any anomalous service account behavior can be automatically blocked to mitigate potential compromise.

File Integrity Monitoring

File integrity monitoring (FIM) is far from a new concept, but it is required by many regulations for a reason: it is a great indicator that an attack is currently underway, and the attacker may be trying to hide their tracks. Many EDR and SIEM solutions have offered FIM capabilities in recent years, but their alerts are limited to the basics: the following file changed at this time. TrueFort uses application and workload behavioral profiling to add more context to the file, such as where it is currently used and how it changed, to make response to the change easy.

Container and Kubernetes Security

Containers and their orchestration platforms are nearly impossible to secure with legacy tools. Containers are grouped into pods, the basic operational unit for Kubernetes, and any pod can talk to any other pod. Most open source and commercial Kubernetes security solutions focus on the network layer, with limited or no visibility into how these high-scale, ephemeral workloads normally operate.

TrueFort's Kubernetes security capabilities leverage the extensive TrueFort Platform to protect containers, virtual machines, and bare metal servers from a single, unified analytics solution. Just as is done for every other type of workload, TrueFort automatically discovers every how every container is used by applications and maps their relationships to the broader environment. This enables development and security teams to establish trusted behavior and block "out-of-profile" activities.

Detection & Response

TrueFort provides threat response and security operations teams with real-time visibility, alerting into anomalous malicious events, and deep workload forensics for investigation into the application environment. Unlike signature-based detection products, when deviations from expected behavior are detected, TrueFort alerts security teams - in real-time - to the source of these deviations and extensive context to explain suspect behavior.

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.

Application Control Allow-Listing

The TrueFort Platform uses its application behavior analytics to clearly identify normal behavior and automate policy controls around execution permissions down to the individual process-level. In effect, TrueFort creates a learned-trust behavioral profile which governs auto-generated allow list of known running processes and their behavior. Any executable detected that is outside the allow list will be terminated.

Deployment & Integration Options

TrueFort offers an advanced approach to protecting data center and cloud workloads that enhance Zero Trust architectures. 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're able to decipher all intra-application communication including application to application, application to infrastructure, application to Internet, application to corporate network and even learning how workloads leverage unregistered nodes.

The TrueFort Platform 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, such as CrowdStrike Falcon, and SentinelOne, 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 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 to contain attacks in progress. We bring the single truth security and application owners need to effectively protect workloads of all forms.

The TrueFort Platform

- **Provides real-time anomalous threat detection and alerting** based on deviations from trusted application behaviors.
- **Quickly identifies and alerts** to untrusted configuration or file changes that impact application risk posture.
- **Automates policy remediation actions** by stopping attack activity before the damage occurs.
- **Enables fast, guided investigation** into detected incidents to reduce the time to respond (TTR).
- **Provides DVR playback with timeline views** of historical application environment behavioral changes give response teams the full picture of alerts detected within TrueFort or elsewhere.
- **Offers advanced query capabilities** for incident response investigations and threat hunting.
- **Provides detailed forensics** down to process execution level.

CONTACT US TODAY

sales@truefort.com

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