TRUEFORT®

SUCCESS STORY

TrueFort® Platform: Microsegmentation Success Story

TrueFort Platform partnered with a major Fortune 500 Manufacturing company that was going through a divestiture of its two main business units. In preparation for this divestiture, the company was tasked with identifying and logically separating thousands of servers and infrastructure components belonging to the two business units. This infrastructure was connected to a common network environment spanning four data centers and interconnected to hundreds of global locations.

The <Manufacturing Company> initially selected Cisco Secure (formerly Cisco Tetration) to discover and map the applications, servers, and their dependencies across the four data centers. Additionally, they planned to use Cisco Secure to implement policy on the servers segmenting the divested operations.

They faced several significant limitations with Cisco Secure:

1. No Application Perspective

Cisco Secure provided visibility into just the infrastructure components and their dependencies. There was no application context to map infrastructure components to applications. Without the application context, it was difficult for the <manufacturing company> to properly identify the sections of the environment that belong to the specific business unit.

2. Non-Intuitive Views

Cisco Secure required an analyst to dig in and run queries to piece together maps of infrastructure components and their dependencies. Cisco Secure had no out-of-the-box views or reports showing how infrastructure components map together with a few clicks.

3. Course Dependency Mapping and Segmentation

Cisco Secure provided visibility into the processes and network connections that they generate, but there were no facilities to enforce segmentation policies specifically at the process and identity levels. Additionally, applying custom classifiers or labels was not flexible beyond geography and data center. In other words, there was no mechanism to enforce zero trust.

4. No Support for Legacy Environments

The <Manufacturing Company> had thousands of servers running Windows Server 2003 and 2008 that Cisco Secure did not support. This created a significant gap in terms of visibility and segmenting the environments.

The company had been working in this manner for nearly a year, with minimal progress and no segmentation to show for their efforts. Due to these challenges, <Manufacturing Company> was forced to look at other micro-segmentation solutions in the market.

92%

of cybersecurity leaders believe microsegmentation is more practical and efficient than its alternatives.

TrueFort® Platform: Proof of Concept

They reached out to TrueFort for a Proof-Of-Concept of the TrueFort Platform. Because <Manufacturing Company> was running CrowdStrike across their entire server estate, TrueFort enabled visibility within one day and quickly mapped the applications spanning the two business units. TrueFort also classified the relevant infrastructure components by business unit, application, and environment (Development, Test, and Production). Needless to say, the security team was impressed with the quick time-to-value.

During the Proof-of-Concept, <Manufacturing Company> was immediately able to visualize the communication flows at the business unit, applications, and environment. TrueFort Platform provided visibility into the crossed business-unit and environment communication flows that violated the desired policy via real-time alerting and reporting. It was these communication flows that <Manufacturing Company> needed to lock down as part of the divestiture. In one week, TrueFort demonstrated our ability to facilitate the separation of the two business units

Using TrueFort Platform, <Manufacturing Company> achieved the following to advance their divestiture efforts:

1. Immediate Application Visibility

Leveraging TrueFort Platform and CrowdStrike, <Manufacturing Company> was able to identify and categorize infrastructure components along business unit, application, and environment layers and then visualize detailed network flows.

2. Intuitive Views and Reporting

With a few clicks, <Manufacturing Company> was able to understand flows and dependencies at the business unit, application, and environment layers.

3. Granular Dependency Mapping and Microsegmentation

TrueFort Platform mapped every dependency by process, identity/service account, and network connection to enhance discovery and greatly enable fine-grained policy enforcement and segmentation.

4. Support for Legacy Environments

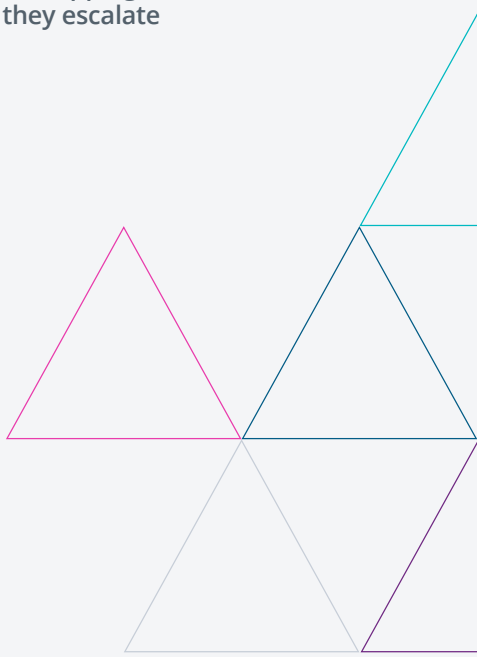
The TrueFort agent was able to support Legacy Operating Systems and completed <Manufacturing Company>'s visibility and control over their application estate across the two business units.

TrueFort® Platform: Additional Value

<Manufacturing Company> understood that they were scratching the surface as far as the full capabilities of TrueFort. Beyond divestiture segmentation, <Manufacturing Company> recognized that TrueFort provided protection of their application ecosystem from Advanced Persistent and Insider Threats that their existing Micro-segmentation, Endpoint, and Network Security products could not provide.

PROTECTING AN ORGANIZATION'S CRITICAL WORKLOADS WITH...

- **Real-time** application behavior mapping. Giving security and application teams get a shared understanding of normal in the application environment
- **Proactive environment attack prevention**, like CIS hardening and file integrity monitoring to greatly reduce the likelihood of lateral movement
- **Deep forensics timelines and event correlation** to fully investigate and properly enact enforcement policies
- **Continuous and immediate behavioral analysis** for real-time detection and automated response capable of stopping attacks before they escalate



Specifically, <Manufacturing Company> saw the following additional benefits from TrueFort:

- **Cloud-based Deployment**
  The manufacturing company was able to install the TrueFort software in their AWS environment and manage the agents in their local datacenters without bulky hardware implementations.
- **Continuously Managed Application Risk Posture**
  TrueFort helps continuously identify risks and vulnerabilities such as cleartext credential usage, unencrypted communications, external remote access (RDP, SSH, SCP), vulnerable runtimes like Java/.NET, PRE-PROD to PROD communications, etc., that attackers can exploit for lateral movement, privilege escalation, data exfiltration, etc. <Manufacturing Company> found more benefits in this approach over traditional vulnerability scanning capabilities.
- **System Integrity Assurance and File Integrity Monitoring**
  Using the CIS Standards for System Hardening, TrueFort can continuously monitor and detect any changes or drift in configuration. TrueFort can also monitor File Integrity on a continuous basis from an application perspective. They saw that they could replace Tripwire with these capabilities.
- **Behavioral Analytics**
  Utilizing machine learning, <Manufacturing Company> can quickly establish a baseline of behavior, alert on change and enforce policies across multiple parameters, including network, process, identity, software packages, file integrity, and process integrity.
- **Incident Response**
  Using machine learning-driven behavioral analytics, real-time alerting, incident replay, and forensics investigation capabilities around applications, TrueFort helps the SOC and Incident Response teams prioritize and work on relevant crown-jewel application-related incidents, dramatically reducing their identification and containment times.
- **Active Enforcement**
  In addition to static micro-segmentation, <Manufacturing Company> found enormous value in active blocking capabilities where they could selectively terminate unauthorized network connections, processes, and identities in the environment using time-based controls.

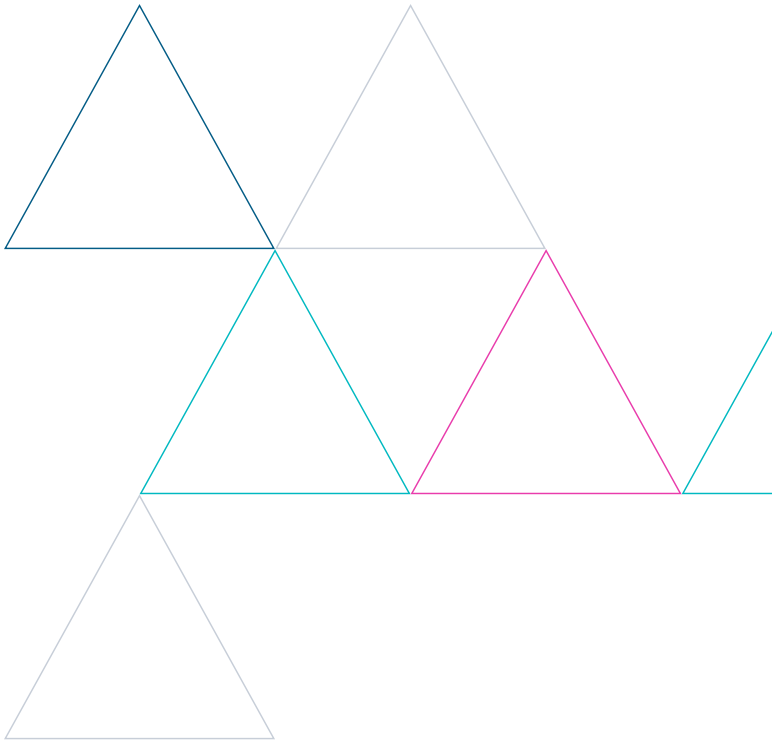
In summary, <Manufacturing Company> selected TrueFort Platform to solve an immediate need around divestiture and provide a long-term, comprehensive Full-Stack Application and Cloud Workload Protection platform that effectively protects their application ecosystems from Advanced Persistent and Insiders Threats.

More simply, the CISO selected TrueFort because "It just works."

TrueFort® Platform: Aligned to Zero Trust Framework

Zero Trust is a conceptual security framework that moves away from a traditional perimeter-centric to a data-centric and identity approach to cybersecurity. Instead of "trust but verify", zero trust assumes a breach is in progress and pushes explicit verification of identities before allowing least privilege access to any resource.

> "It just works."
>
> CISO, Fortune 500 Manufacturing Company.



SUCCESS STORY

How Does TrueFort Platform Support the Zero Trust Framework?

Looking at the sub-domains of zero trust per Forrester Research 1:

Chase Cunningham: "The Zero Trust Extended (ZTX) Ecosystem," Forrester research, 2019, pgs. 5-6.	**TrueFort Platform support**
Zero-Trust Data ▸ Securing, managing data ▸ Categorizing and developing data classification schemes ▸ Encrypting data at rest and in flight	TrueFort can work in tandem with data governance platforms to monitor, detect and respond to anomalous behaviors related to applications and databases hosting data prioritized by criticality and sensitivity.
Zero-Trust Networks ▸ Segmentation and isolation of Networks	Provides application microsegmentation and real-time enforcement capabilities based on Application Behavioral Analytics to prevent unauthorized network connections.
Zero-Trust Users ▸ Authenticating users and continuously monitoring and governing their access and privileges.	Using Application Behavioral Analytics, TrueFort can work in tandem with Identity and Access management systems to detect and take action against user and system identities working outside of their areas of privilege.
Zero-Trust Workloads ▸ Protecting the application stack including the application layer to the container or virtual machine.	TrueFort can monitor and protect workloads across baremetal, virtual machines, and containers down to the specific processes executing under specific identities that connect to other workloads.
Visibility and Analytics ▸ Provide visibility into threats that enable organizations to establish the appropriate policies and defenses against adversaries	TrueFort Platform provides visibility into the inter and intra-application connections and behaviors down to the network, process, and identity to enable organizations to establish the appropriate policies and defenses leveraging machine learning
Automation and Orchestration ▸ Automate and orchestrate policies to reduce manual work while helping stop attacks	TrueFort uses MuleSoft was its workflow engine to kick off external processes (alerts, tickets, SOAR workflows) as well as real-time enforcement at the endpoint (IP block, process termination, user session termination, and 40 other real-time actions.

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.

Learn how TrueFort can enable zero trust application protection for your organization through microsegmentation and other application-centric controls.

Contact us at sales@truefort.com

TRUEFORT®

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM