TRUEFORT™

HOW TO GUIDE

Microsegmentation Made Easy

Entrust TrueFort to Secure your Application Environments

Application and workload communications are exploding with the increased adoption of microservices- and containerized architectures. As a result, protecting critical workloads is more difficult with diverse environments, dynamic applications, and ephemeral workloads.

Microsegmentation is essential to protect data and operations in today's complex IT environments, securing at the application level by using policies to limit traffic and isolate workloads.

- **Security:** While attacks are inevitable, microsegmentation prevents unauthorized lateral movement within your systems and contains ransomware, insider threat, supply chain or other cyberattacks.
- **Compliance:** Microsegmentation is a key capability for maintaining compliance with data and privacy standards that require certain processes to be segmented from general network traffic such as PCI, HIPAA, or CMMC.
- **Business:** Microsegmentation supports a wide array of business projects, such as divestiture and cloud migration through the ability to segment workload communications.

TrueFort puts you in control by offering an easier microsegmentation solution that protects business critical applications through real-time understanding of workload behavior and automating segmentation policy management based on tags around operating system, application type, or other attributes. TrueFort gains valuable intelligence on behavioral characteristics, creating a trusted profile of accepted actions, and automatically pushing rules back to the host firewall for enforcement.

HOW TO GUIDE

The Microsegmentation Journey

TrueFort has the automation and methodology to make it easy to deploy microsegmentation across the enterprise.

STEP #1: Discover and Understand

The TrueFort Platform provides visibility and application context to correctly model application environments by identifying core services, creating applications, mapping workloads to applications, and defining organizational structure. We leverage existing information to ensure a foundation for baselining across heterogenous and complex environments.

Step 2: Profile and Baseline

Using continuous telemetry and advanced machine learning, TrueFort automatically generates granular microsegmentation policies per application, using natural language labels abstracted from network constructs. We discover and map application, workload, and user interactions to profile and baseline acceptable behavior. These policies can be combined with global policies to form comprehensive controls for applications and workloads.

Step 3: Review and Define

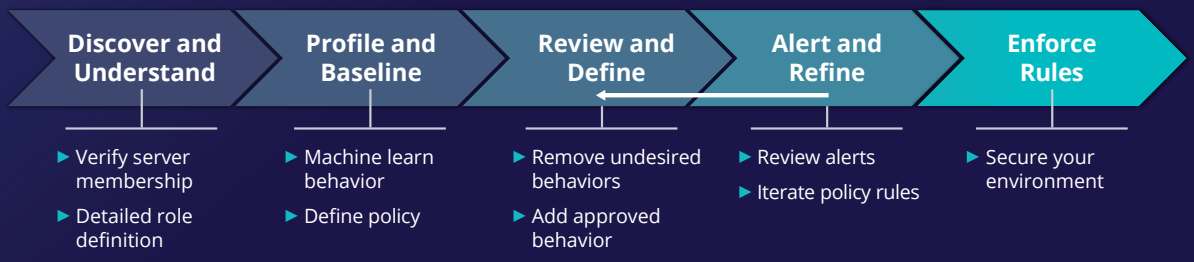
Review and define the policies by inspecting unwanted behaviors and creating policy rules to alert whenever they occur. Create the allow list of approved behavior. By using natural language labels, application teams can understand connectivity with other applications, core services, workstations, and foreign hosts and easily validate policies and interactions.

Step 4: Alert and Refine

Turn on the TrueFort Platform analytics and evaluate behavior against the created policy in real-time. Alerts will be generated for all anomalous behavior, testing the policies. Review alerts to gain confidence that created policies do not break production before moving into enforcement. Regularly review with the application owners as new applications are built and behavior in the environment changes.

Step 5: Enforce Rules

Deploy enforcement with confidence. A single pane of glass combined with advanced automation enables central control of the host-based firewalls on workloads. With the support for OS starting from Windows server 2008 and Linux 6.x, you can be confident that your environment is covered. Change is certain, and TrueFort has the automation in place to easily allow for continuous policy management.



Let TrueFort protect your workloads by intelligently baselining normal, high-volume activities within and between applications, limiting future behavior to only what should be trusted.

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 both identity and activity.

TRUEFORT™

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM