TRUEFORT™

SOLUTION BRIEF

Microsegmentation

Secure environments and efficiently reduce lateral movement by segmenting your applications and workloads

Protecting workloads has become much harder due to the diverse environments, complex architectures, and ephemeral workloads.

Traditional network segmentation solutions have proven difficult to implement and ineffective for controlling East/West traffic. Policies are pushed to network devices that continually inspect traffic but require manual intervention to update and lack any visibility into application behavior and communications – a key path for lateral movement.

Microsegmentation provides a better way to isolate your environment and protect critical assets against unauthorized lateral movement. Network segmentation solutions do not detect lateral movement as abnormal activity because they do not distinguish normal behavior from anomalous behavior. This inability enables attackers to move freely undetected. Commonly they gain access through ransomware, service accounts, insiders, or supply chains. Once in, they easily move undetected.

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 breaches 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 GDPR.
- **Business:**
  Microsegmentation supports a wide array of business projects, such as divestiture and cloud migration through the ability to segment workload communications.

92%

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

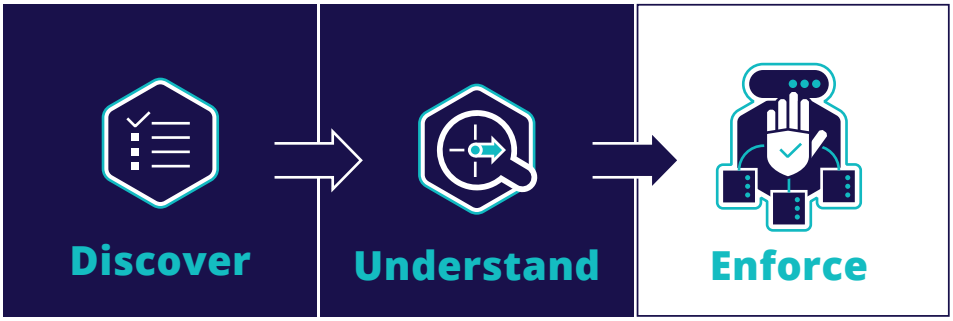
MICROSEGMENTATION CHALLENGES:

1. **Network-based solutions** are application and workload unaware
2. **Lateral movement** isn't detected by network-based segmentation
3. **Network-based solutions** do not understand normal behavior
4. **Supply chain attacks** are application focused and fly under the radar
5. **Dormant or inactive Service Accounts** are easy targets

SOLUTION BRIEF

TrueFort Puts You in Control

TrueFort offers 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 enacts enforcement policies.



TrueFort **discovers** data center and cloud workloads from **existing agents** already installed and determines which **service accounts** execute in each application.

Understand what needs to happen in the applications to block traffic and minimize the chance of lateral movement - the **WHO, WHAT, WHEN,** and **WHERE**. TrueFort uses this to set policies.

Enforce key protection policies against lateral movement by **blocking abnormal connections** between applications and **disabling privileged accounts** that execute in an unusual manner. TrueFort can also **kill anomalous system processes** as they execute.

TrueFort protects workloads and applications by intelligently baselining normal, high-volume activities within and between applications, limiting future behavior to only what should be trusted. Prevent compromise and reduce risk by enabling insight into the application environment and efficiently reduce the threat surface area though microsegmentation.

OUR MICROSEGMENTATION SOLUTION PROTECTS YOUR ORGANIZATION'S CRITICAL WORKLOADS WITH...

- **Live application behavior mapping.** 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

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.

TRUEFORT™

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM