TRUEFORT

BRIEF

MICRO-SEGMENATION MADE EASY
USE FORTRESS TO SECURE YOUR CRITICAL APPLICATIONS

Fortress prevents compromise and reduces risk by enabling organizations to quickly gain insight into their application environment and efficiently reduce the threat surface area though micro-segmentation.

Traditional Segmentation is not enough

Network-based security boundaries are no longer effective in today's dynamic, hybrid environments. Attackers are breaching perimeter defenses and blending into east-west traffic, "living of the land" and taking their time to attack their target. With existing controls, all those workloads, bare metal, VMs and containers generate a huge attack surface.

Micro-segmentation, setting granular security policies on an application basis, reduces the attack surface by implementing a "zero trust" security model. Micro-segmentation policies dictate which applications can communicate with each other and with approved endpoints. Any unauthorized communication attempt is not only blocked, but also triggers an alert that an intruder may be present which would otherwise have gone unnoticed.

It's Not "All or Nothing"

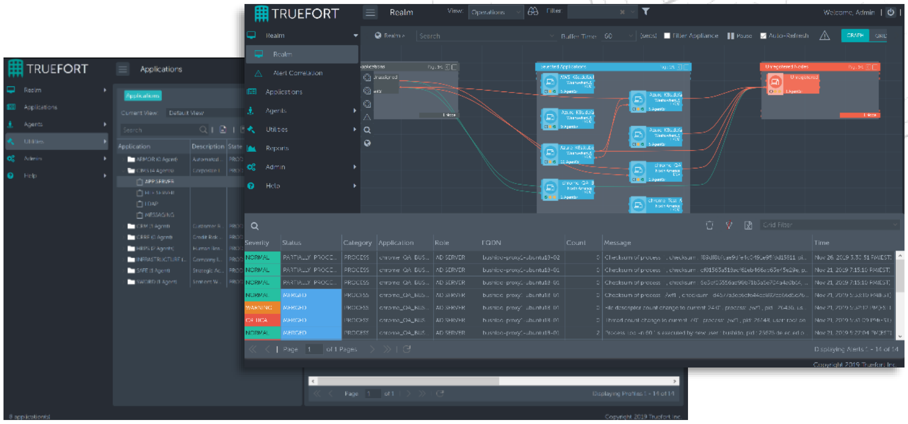
No need to boil the ocean. Use analytics-based virtual segmentation before deploying firewall policies. Successful micro-segmentation projects take a phased approach, starting with priority projects or "crown jewels" and growing out to a more comprehensive program. The application methodology provides a "bite sized" piece of the environment to generate simple app-specific policies that do not need to be all-encompassing.

Micro-Segmentation has traditionally been difficult to implement and maintain.

Fortress has ADVANCED VISIBILITY, MACHINE LEARNING AND AUTOMATION to create, deploy and maintain policies in

Application Focus – Distributed Effort

Security is everyone's responsibility. Fortress provides the tools, automation, and visibility to distribute the effort among DevOps, SecOps and Infrastructure. Involve application teams in the process and ensure their detailed understanding is leveraged to configure policy. Take advantage of tribal knowledge across all disciplines to fine tune policies.



Severity	Status	Category	Application	Role	FQDN	Count	Message	Time
NORMAL	PARTIALLY_PROCE...	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy1-ubuntu18-02	0	Checksum of process : , checksum : f83df8bfcae9d1e4c0491e95fdd15611 pi...	Nov 26, 2019 3:30:51 PM(EST)
NORMAL	PARTIALLY_PROCE...	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy1-ubuntu18-01	0	Checksum of process : , checksum : cf01563a519acf61eb466ae63e45e29e, p...	Nov 21, 2019 7:15:10 PM(EST)
NORMAL	PARTIALLY_PROCE...	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy1-ubuntu18-01	0	Checksum of process : , checksum : 5e3cf03556ad90b71b3a5e704a4d0b14, ...	Nov 21, 2019 7:15:10 PM(EST)
NORMAL	MERGED	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy1-ubuntu18-01	0	Checksum of process : /wf1 , checksum : d457a5e0cfe44cd882cb6db5c76...	Nov 21, 2019 5:33:10 PM(EST)
WARNING	MERGED	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy1-ubuntu18-01	0	File descriptor count change to current 24.0 , process: /wf1 , pid : 26436, us...	Nov 21, 2019 5:32:12 PM(EST)
CRITICAL	MERGED	PROCESS	chrome_QA_BUS	AD SERVER	bushido-proxy1-ubuntu18-01	0	Thread count change to current 7.0 , process: /wf1 , pid: 26148, user: root se...	Nov 21, 2019 5:31:09 PM(EST)
NORMAL	MERGED	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy1-ubuntu18-01	2	Process 'ioc -n 60 ' is executed by new user : bushido, pid : 25676 de ec ed o...	Nov 21, 2019 5:27:04 PM(EST)

Page 1 of 1 Pages — Displaying Alerts 1 - 14 of 14

Copyright 2019 Truefort Inc.

Page 1 of 1 — Displaying Profiles 1 - 14 of 14

Copyright 2019 Truefort Inc.

Top
10

Gartner has identified micro-segmentation as a top 10 priority security project, particularly for organizations "that want visibility and control of traffic flows within data centers,".[1]

SOLUTION HIGHLIGHTS

- **Fastest ROI in the Market**
  Time to value measured in days...not months.
- **From the Cloud to the Ground**
  Span across all environments from a single pane. Bare metal, VMs, Containers, Legacy OS-Windows 2003/2008, AWS, and Azure.
- **Visibility into Critical Applications**
  Gain business context visibility inside your applications. Generate Application Dependency Maps (ADM), understand relationships and flows, update CMDB with live data.
- **Continuous Monitoring and Alert**
  Detect and prevent breaches before they occur. Visualize East/West traffic and lateral movement behind perimeter firewalls and understand anomalies.
- **Simple and Flexible Policies**
  Create simple, highly visual segmentation policies that work consistently across platforms and environments. Apply policy to monitored endpoints, infrastructure and BYOA (VMWare, CrowdStrike)
- **Streamlined Integration and Use**
  Integrate segmentation into your CI/CD process with automated deployment and avoid infrastructure dependencies and downtime for change management.

The Micro-Segmentation Journey

Step 1: Define Applications

Fortress provides the visibility and application context to correctly model application environments. Leverage existing information to ensure a foundation for baselining, even across heterogeneous, complex network environments – From the Cloud to the ground

Step 2: Profiling / Baselining

Using continuous telemetry and advanced machine learning, Fortress automatically generates granular micro-segmentation policy on an application basis, using natural-language labels, abstracted from network constructs. Fortress exposes detailed behavior to App teams on a silver platter. These application specific policies can be combined with global policies to form comprehensive controls for application workloads.

Step 3: Review Whitelist Policy

Review the policy and prune unwanted or unapproved behavior to create a whitelist of behavior for the application. By using natural-language labels, app teams can understand connectivity with other applications, core services, workstation space and foreign hosts and easily validate policy.

Step 4: Virtual Enforcement

This is where the magic begins. Turn on Fortress analytics and evaluate network behavior against the created policy...in real-time. Alerts will be generated for all anomalous behavior, testing the policy. Review alerts in minutes and easily clean and refine. Run with real time alerts on for an appropriate time to ensure confidence in policy and not break production.

Step 5: Micro-Segmentation

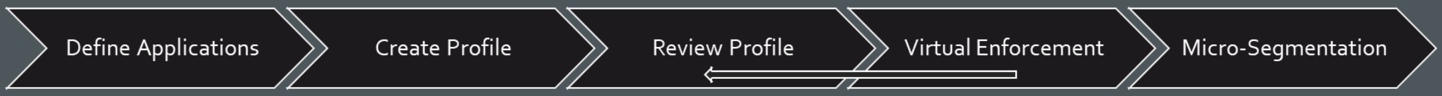
Deploy with confidence! A single pane of glass combined with advanced automation enables central control of the host-based firewalls on servers. With support for OS starting from Windows Server 2008 and Linux 6.x, you can be confident that your environment is covered. Change is certain Fortress has the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

Business Drivers

Micro-segmentation is a security technique that logically divides complex compute environments into distinct security segments down to the individual workloads. This enables IT to deploy flexible security policies deep inside a hybrid cloud instead of installing multiple physical firewalls.

- **Get Going Now**
  Start by focusing on projects that are manageable, easy to complete, and can deliver tangible results.
- **Reduce Your Attack Surface**
  Become a smaller target, making resources invisible and resilient to threat actors.
- **Crown Jewels**
  Protect the most critical applications to the enterprise first and reduce the threat attack surface.
- **Compliance**
  A key driver of micro-segmentation, regulatory standards such as SWIFT, PCI, GDPR, HIPAA or others frequently specify that certain processes must be separated from general network traffic.
- **DevOps.**
  Applications in development, testing or quality assurance environments need to be separated from those in the production environment.
- **IOT**
  Restricted access to compute environments or services from outside users or Internet of Things devices.

STEP BY STEP TOOLS, FOTRESS HAS THE AUTOMATION AND METHODOLOGY TO MAKE IT EASY TO DEPLOY MICRO-SEGMENTATION ACROSS THE ENTERPRISE



- Verify server membership
- Detailed role definition

•Machine Learn Behavior
•Define Policy

•Remove undesired behaviors
•Add Approved Behavior

•Review Alerts
•Refine Policy iteratively to known good state

•Secure your environment

HOW IT WORKS

Fortress delivers value in each step of the journey. Begin by installing our virtual appliance and importing and defining what you know about your business and its apps. Fortress employs the standard appliance-sensor model, offering out-of-box integrations and full REST-API access. Connect your agents, integrations, and feeds. This will provide immediate value and significant insight into the current state and vulnerabilities of your apps before you even start baselining.

Platform appliance. Delivered as software to be deployed anywhere Linux goes including bare-metal, virtual machines, and cloud images. It is fully multi-tenant, scalable and highly available with a load-balanced, highly available and redundant N+1 clustering option.

Reporter Module. For risk posture management, we recommend deploying our optional Reporter module featuring out-of-box preconfigured reports. Ideal for analysts, threat hunters, incident response or executives reviewing results.

Management console. Deploy, configure, protect, report, and investigate all from a single pane of glass that offers configurable, role-based management.

Protect agent. (Optional) Our advanced, proprietary agent offers a light footprint and tracks over 115 parameters to continuously monitor, microsegment and protect. Compatible with legacy servers, virtual machines, cloud instances, PaaS and containerized environments.

> “full visibility into business-critical applications and quick threat detection … enables automated, proactive tuning of existing security policies, blocking malicious activities before they even occur.”
>
> – KuppingerCole

The below chart shows how Fortress supports common security frameworks as well as understanding the application environment and supporting migrations. For more information about how our solution works and supports securing your critical applications, please contact sales@truefort.com .

SOLUTION FEATURES

- Behavioral Analytics
  Uses high - throughput, low - latency based on Wall Street high frequency trading systems .
- XDR with Detailed Telemetry
  Enrich with data you own, and go beyond network with process, identity, and time.
- On Premise and in the Cloud
  Maintain app risk posture across your enterprise.
- Accelerate Investigation/Response
  Reduce forensic investigation costs of cyber-incidents, streamline compliance, and gain historical playback capabilities.
- Integrate in CI/CD Toolchain
  Integrate security into your release process. Good risk posture begins before deployment

FORTRESS
SUPPORTS YOU IN

MICRO-SEGMENTING YOUR APPLICATIONS

AS YOU ASSESS THE LANDSCAPE,

DETERMINE STRATEGY,

… AND EXECUTE YOUR PLAN.

CSA EGREGIOUS 11

- Data breaches
- Misconfig & inadequate change control
- Lack of cloud security architecture and strategy
- Insufficient identity & key management
- Account hijacking
- Insider threat
- Insecure interfaces & APIs
- Weak control plane
- Meta- & applistructure failures
- Limited usage visibility
- Abuse/nefarious use

MITRE ECAF

- Establish security tolerance
- Know threat environment
- Perform risk analysis, select controls
- Know vendor security & privacy capabilities
- Update policies, define architecture
- Develop > assess security & privacy measures
- Perform risk management
- Manage migration security risks

FORTRESS

- Inventory apps with detailed visibility into network relationships tied back to process, and identity,
- Understand outage dependencies, metadata, vulnerabilities, drift and more.
- Migration support - Baseline applications, assess and configure behavior and policy.
- Update configuration and security policy to new environment
- Compare model-driven design to deployment
- Perform continuous monitoring for new operational and security anomalies.

TRUEFORT & THE FORTIFIED" ECOSYSTEM

And remember – good data in, good data out. Power Fortress with the telemetry you already collect, and let our platform fortify the value of security and operational investments you have already made.

Our partnerships span many categories, including network security, infrastructure and leading endpoint protection, detection, and response vendors, so that you can immediately benefit from our bring-your-own-agent option.

We also work with industry standards organizations and offer open access to our fully REST-API driven platform to partners, providers, and our customers through our Fortified program.

kubernetes vmware® Microsoft

Infoblox NEXT LEVEL NETWORKING FORTINET Fabric-Ready

Pivotal CROWDSTRIKE

vmware® Carbon Black CIS. Center for Internet Security®

SUPPORT

Companies offering highly available solutions to protect your business need to be highly available, too.

TrueFort customers receive 24x7 phone and email support, and all maintenance and software upgrades.

RECOGNITION

TAGCYBER 2020 DISTINGUISHED VENDOR

TiE50 2020 WINNER

CROWDSTRIKE Store Partner of the Year

AVAILABILITY

TrueFort Fortress is offered globally as a software subscription. It is licensed per endpoint, workload or containerized environment, whether you choose our TrueFort Protect agent and/or bring-your-own-agent.

To learn more, request a briefing and a demo. Then experience it for yourself with a proof-of-value.

ABOUT TRUEFORT

Applications are the lifeblood of business. TrueFort™ helps organizations align application security policy with operational reality via Fortress, the industry's first application detection and response platform.

Fortress reverses the traditional infrastructure approach to security by comprehensively tracking application behavior to unify cloud workload protection and AppSec in a single console. Using real-time telemetry, patented advanced behavioral analytics and policy automation, enterprises can now visualize, microsegment, protect, hunt, and investigate from the application layer.

Founded in 2015 by former Wall Street senior IT executives, TrueFort offers unparalleled application visibility, control, and protection with the shortest time-to-value through the TrueFort Fortified™ ecosystem and our unique bring-your-own-agent approach.

For more info visit www.truefort.com and follow us on Twitter and LinkedIn.

3 West 18th Street
Weehawken, NJ 07086
United States of America
+1 201 766 2023

sales@truefort.com

TRUEFORT

[1] How to Make Cloud More Secure Than Your Own Data Center | MacDonald & Crow, Gartner, Oct 2019
[2] Four Main Types of Cyberattack That Affect Data Center Uptime | DataCenter Knowledge, June 2019
[3] KuppingerCole Report: Executive Overview -TrueFort Fortress XDR | KuppingerCole, Nov 2019
Feature support varies when in "bring-your-own-agent" mode according to the capabilities of the third- party agent deployed on the workload, and its integration with the Fortress XDR platform.