TRUEFORT

TECH BRIEF

ZERO TRUST WITH FORTRESS

PROTECT YOUR APPLICATIONS from FUTURE ATTACKS

Quickly go beyond network to implement zero trust *application* security. The perimeter no longer exists, and traditional security methods are not enough.

Reduce Risk in the Era Supply Chain Attacks

Zero trust has rapidly overtaken 'trust but verify' since the blind-siding attack on enterprises and governments using trusted third-party software like the SolarWinds Orion software. This attack has highlighted the fact that traditional protection techniques, even the most sophisticated EDR technologies, were ineffective at detecting and mitigating this hack.

As a result, corporate networks are experiencing unprecedented malicious activity as threat actors recognize the opportunity to prey on the weak. There has been a significant increase in DDoS and Ransomware with some organizations reporting a 75% increase in Ransomware attacks alone. All this access has dramatically increased cyber risk from both internal and external sources, and the climate will not be changing any time soon.

The only way to prevent and respond to attacks like SolarWinds, is to truly understand all behaviors in the application environment including those of third-party software. Only the TrueFort Fortress platform addresses this issue with behavior baselining, real-time anomaly detection and response across all applications and workloads.

Zero trust application security goes beyond NETWORK to monitor and control PROCESS, IDENTITY, SOFTWARE AND OS in real-time and create, deploy and maintain policies in dynamic compute environments.

Implement Advanced Zero Trust Today

While the concept of zero trust from the network perspective is not new and is a key component of securing environments, it falls short on its own. For years, network teams have been securing environments by implementing strong perimeter controls. However, threat actors still infiltrate environments, use known good pathways to move East-West between servers and workloads, and "live off the land" until they find their target and execute their attacks. Network security alone is not enough to enable zero trust.

Who is the right team to implement zero trust application security? Our experience shows that relying on one team alone will not be successful. Your network, security and AppSec teams need to work together to protect your most valuable assets, infrastructure, and data. They need to be able to leverage understanding and insight into critical environments and automatically put policy in place. They also need to communicate continuously to implement controls and enforcement and maintain policy going forward. TrueFort can empower your teams to implement zero trust right now, with near-zero risk, and with ease.

Zero Trust Application Security

The TrueFort Fortress platform is purpose built to deliver zero trust security and enable collaboration between security teams. It detects and monitors workloads in real-time, abstracts complexity and automates the creation and validation of fine-grained workload segmentation policy. This streamlines the process of designing, validating, testing, implementing and enforcing zero trust application security. Fortress leverages real-time agent data to visualize telemetry enriching network behavior with related process and identity metrics to correlate user, network, process, and software, in the context of your applications and present it in an easily digestible graphical format.

66%

Forrester found that organizations deploying zero trust are 66% more confident in adopting mobile work models.[1]

SOLUTION HIGHLIGHTS

- **Bring Your Own Agent**
  Leverage existing investment in EDR tools (CrowdStrike, Tanium, etc.) to accelerate your deployment, provide immediate visibility, and support enforcement.
- **Real-Time Network Visibility**
  Identify workloads plus internal/external connections and dependencies from the cloud to the ground.
- **Real-Time Process Visibility**
  Continuously monitor using behavioral baselines to detect and block anomalous behavior in real-time, as a complement to any workload isolation.
- **Identity**
  Identify who logs in, from where, with which credentials and have visibility into what they are doing – now and historically.
- **Auto-Generated Policy**
  Automatically design, validate, version-control and manage fine-grained policies for inter- and intra-workload micro-segmentation and zero trust protection.

It all Starts with Visibility

Simply put, you cannot manage what you do not understand. The journey to zero trust starts with the ability to visualize your critical applications and environments. Most organizations simply do not fully understand their application landscape - the applications they have, the dependencies between them and their related operational controls. Add to that the changing dynamics of hybrid and cloud, and it becomes critical that application maps generate automatically and update dynamically. These maps form the foundation used to categorize and classify the environment and are key to building policy.

It Ends with Zero Trust Application Protection

Whether access is given by accident or sensitive data is maliciously accessed, visibility is the key to security. Without the ability to see what's happening on all workloads and knowing when behavior deviates from a known good state, malicious actors can slip by existing security controls, resulting in a costly or damaging breach. Fortress delivers continuous real-time telemetry across network, process, identity, and software behavior, analyzes it within milliseconds, and generates comprehensive real-time alerts and workflow-driven responses to ensure that bad behavior is immediately seen and stopped.

Fortress sees beyond the network, enabling comprehensive zero trust *application protection*.

Leverage application-centric visibility to:

- Create a closed-loop process to ensure no CMDB drift
- Visualize application relationships, dependencies, and flows
- Baseline behavior across network, process, identity, and software
- Create default policies based on an 'allow list' basis

Verify unusual network activity & data exfiltration attempts, including:

- Anomalous lateral movement
- Access to applications outside of operating windows
- Changes in application flows
- Logins from unknown sources
- New systems joining an application
- Usage of FTP, SSH, SCP, etc., on critical systems

Monitor privileged account abuse and privilege escalation, such as:

- Operator access including time and location
- Interactive usage of service accounts
- Service account usage from unknown source
- Lateral movement with multiple identities
- Unauthorized identities accessing critical applications
- Privileged account activity outside of known or authorized use
- Processes run by different or unauthorized users

Alert on unusual process and system activity, such as:

- New or different processes listening on known ports
- New processes out of context, time, or application profile
- Use of nmap, metasploit and other potentially malicious tools
- New processes spawning connections out of profile
- Process hollowing through changes in runtime hash
- File systems being mounted on unauthorized hosts
- Anomalous service user activity

VISIBILITY AND PROTECTION

Process and Behavior Analytics

Fortress is ready to go out of the box. With pre-built analytics to protect applications, it is the only platform to identify and alert on process checksum and runtime state anomalies.

Forensic Information on the Fly

Click and drag our DVR controls to review an application's behavior down to the network and process levels on individual workloads.

Uncover Critical Threats

Fortress detects advanced threats by leveraging machine intelligence and automated, real-time data analytics. Pre-built event correlation and data-driven threat context automatically generates alerts, allowing you to focus on critical issues.

Never Trust, Always Verify

Real-time telemetry and "virtual enforcement" allow for the automated creation and real-time testing of the right policy, the first time, across all behaviors.

Stop Unauthorized Traffic

Fortress visualizes East/West traffic that would normally be invisible to perimeter firewalls and allows you to detect and block unapproved lateral movement in real-time.

Stop Malware & Bad Behavior

Alert and control in real-time on modified or unapproved process runtime states, identities, or activity.

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. It connects to your existing agents, integrations, and feeds to 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 teams or executives reviewing results.

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

"Without understanding the logic, behavior, and business risks of corporate applications, even the most detailed analysis of network flows between them will never help an analyst to properly assess the risks."[3]

– KuppingerCole

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

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.

TRUEFORT'S UNIQUE APPROACH TO SECURITY

TrueFort was founded in 2015 by former Wall Street senior IT executives who came face-to-face with the inadequacy of network and infrastructure security tools to secure their application environment. They knew they needed something different when they couldn't prevent or confidently determine the blast radius of a breach.

They developed a purpose-built application-centric platform - Fortress – that reverses the traditional infrastructure approach to security. The platform comprehensively tracks 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.

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.

FORTRESS SUPPORTS YOU IN
ZERO TRUST

AS YOU ASSESS THE LANDSCAPE,

DETERMINE STRATEGY,

... AND EXECUTE YOUR PLAN.

CSA EGREGIOUS 11	MITRE ECAF	TRUEFORT FORTRESS
▪ Data breaches	▪ Establish security tolerance	▪ Inventory apps with detailed visibility into network relationships tied back to process, and identity
▪ Misconfiguration & inadequate change control	▪ Know threat environment	▪ Understand outage dependencies, metadata, vulnerabilities, drift and more
▪ Lack of cloud security architecture and strategy	▪ Perform risk analysis, select controls	▪ Migration support - Baseline applications, assess and configure behavior and policy
▪ Insufficient identity & key management	▪ Know vendor security & privacy capabilities	▪ Update configuration and security policy to new environment
▪ Account hijacking	▪ Update policies, define architecture	▪ Compare model-driven design to deployment
▪ Insider threat	▪ Develop > assess security & privacy measures	▪ Perform continuous monitoring for new operational and security anomalies
▪ Insecure interfaces & APIs	▪ Perform risk management	
▪ Weak control plane	▪ Manage migration security risks	
▪ Meta- & applistructure failures		
▪ Limited usage visibility		
▪ Abuse/nefarious use		

TRUEFORT & THE FORTIFIED ECOSYSTEM

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 · Pivotal · Fortinet Fabric-Ready · Infoblox NEXT LEVEL NETWORKING · CIS Center for Internet Security® · CROWDSTRIKE

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.

AVAILABILITY

TrueFort Fortress is available globally as a software subscription licensed per endpoint, workload or containerized environment. For your convenience, TrueFort offers a unique bring-your-own-agent option or you can deploy our proprietary agent.

To learn more, please contact sales@truefort.com to request a briefing and demo. Then experience a zero trust application environment with a proof-of-value.

ABOUT TRUEFORT

TrueFort reduces business risk for security-focused enterprises striving for zero or lean trust application environments. Our innovative and uniquely application-centric Fortress platform delivers comprehensive real-time cloud-to-the-ground insight, protection and automated response with patented machine intelligence and a single or bring-your-own agent.

Fortress overcomes the application security blindspots inherent in legacy infrastructure-centric tools, providing unparalleled visibility and protection for applications in on-prem, hybrid and cloud environments and for security teams across the enterprise. Fortress speeds response times, minimizes the blast radius of compromises, prioritizes resources, and enhances application risk posture.

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

INDUSTRY RECOGNITION

TOP 25 Cybersecurity Company 2020 TSR · computing Security Excellence Awards 2020 Winner Enterprise Threat Detection Award Truefort · TAG CYBER 2020 DISTINGUISHED VENDOR · RED HERRING 100 WINNER N. AMERICA

[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.

TF-1.0-0420

TRUEFORT

3 West 18th Street
Weehawken, NJ 07086
United States of America
+1 201 766 2023
sales@truefort.com

www.truefort.com