TRUEFORT

BRIEF

IMPROVE APPLICATION RISK POSTURE

WITH HYGIENE, HARDENING & CONFIGURATION MONITORING

Fortress prevents compromise and reduces risk by continuously identifying and locking down the most common causes of breach.

RISK POSTURE MANAGEMENT IS MORE IMPORTANT THAN EVER

According to DataCenter Knowledge, **application attacks are one of the four main attack vectors**[2] targeting your data centers, your cloud instances, and your business. Their goal? Gain access to privileged accounts, exfiltrate high-value data, and ransom your crown jewels.

How do you manage this risk?

- **Do you continuously monitor, enforce & adapt configuration policies – in development, your data centers and in the Cloud?**
- **Can you detect and respond to new risks in real-time without delay, operational burden or service outage?**
- **Are you confident you could effectively manage and *do something* about a major incident?**

Vulnerability management, next-gen SIEM, SOAR, pen-testing, and new Cloud Security Posture Management (CSPM) solutions help solve parts of the problem – but disparately and incompletely.

To succeed in preventing breach, you need to **know your apps comprehensively** – with breadth, depth, and at the app level.

FORTRESS IMPROVES POSTURE OF APPS & THEIR WORKLOADS

We can help. Fortress protects enterprise applications everywhere – **whether on-premises, in containers, or in the Cloud.**

It fully visualizes and understands apps in-production, including their dynamic behavior and context. See them in 4k resolution across all aspects including their workloads, processes, scans, connections, configurations, and the time and identities of access and attack.

99%

Gartner – "Through 2023, at least 99% of cloud security failures will be the customer's fault." [1]

SOLUTION HIGHLIGHTS

- **Real-Time Risk Reduction**
  Detect top vulnerabilities like unencrypted traffic, misconfigurations, and **rogue service accounts.**
- **Standards-Based Protection**
  Use XDR-based telemetry to monitor against **CIS** criteria, enable **FIM**, and run ondemand reports and queries.
- **Rapid Value**
  Deploy our agent or **bring-your-own-agent**[4], then get started with a Risk Posture Report.

WWW.TRUEFORT.COM

WHAT IT SOLVES & REPLACES

In general, "Risk Posture Management" includes a broad range of capabilities from threat feeds, to patching, to global policy creation and enforcement – across both development and production environments.

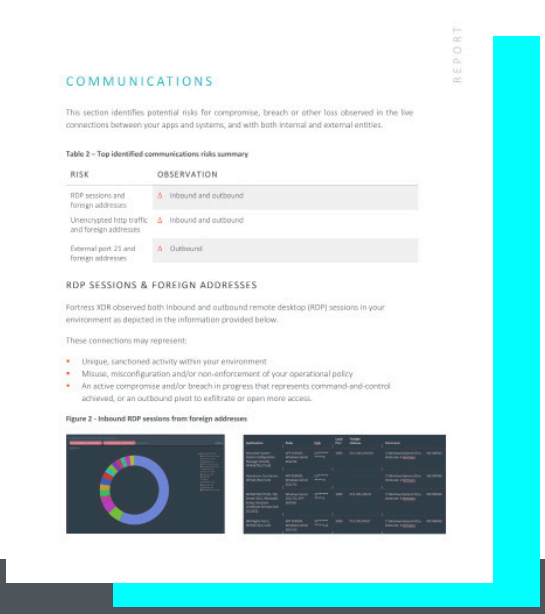
But unlike point solutions, Fortress is *application-**first***, and holistically secures your crown jewels in ways others miss:

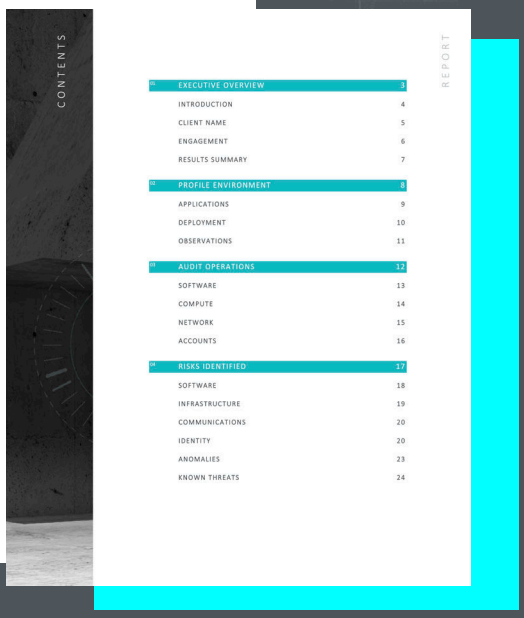
- **Profile, understand and prioritize your enterprise *application* risks within the business context.**
- **Whitelist policy, report, and continuously monitor and respond based on real-time *application* usage patterns.**
- **Get value fast using our bring-your-own-agent (BYOA) option, and assessing *application* risk posture as a first step.**
- **Manage crown jewel risk posture, policy, and cloud workload security from a single, unifed console.**

With Fortress, the industry's first application detection and response platform, you can stay ahead of cyber-adversaries by closing common vulnerabilities, **automating continuous app pen-testing from the "inside-out",** and building your risk posture upon a solid, fortified foundation.

SOLUTION USE CASES

- **Breach Prevention**
  Go proactive with good hygiene, keep pace with ops, and automate anomaly detection.
- **Cloud Migration, M&A & EOL**
  Maintain posture when migrating, merging, or retiring legacy systems.
- **Compliance**
  Ensure and report that regulated data like PII is protected from unauthorized access and exfiltration.





GET THE READ-OUT | APPLICATION RISK POSTURE REPORTS

Profile Your Production Apps within Their Business Logic Context

- App function and component roles
- Deployment characteristics
- Application dependency mapping
- Typical activity hours
- Typical connections

Audit & See the Gap Between Policy, Current State & Behavior

- Processes, executables and commands
- Ports, protocols and traffic
- Accounts and users
- Software and patches

Identify Top Risks in Your Unique Environment

- Vulnerable software and infrastructure
- Unmanaged accounts and unencrypted authentications
- Unencrypted and abnormal connections
- Unusual process execution
- Known attack indicators

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. Then connect agents, integrations and feeds. And before you really start baselining behavior, you get insight into the current state and vulnerabilities of your apps.

Fortress employs the standard appliance-sensor model, offering out-of-box integrations and full REST-API access.

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

Reporter Module. For risk posture management, we recommend deploying our Reporter module featuring preconfigured reports, ideal for analysts 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."[3]

– KuppingerCole

The below chart shows Fortress coverage of the 20 CIS Controls®. For more information about how our solution works and supports CIS criteria[4], please contact sales@truefort.com.

SOLUTION FEATURES

- **Behavioral Analytics**
  Delivers on performance and scale using patented tech based on Wall Street high frequency trading systems.
- **XDR *and* 5-Tuple+ Telemetry**
  Enrich with data you own, and go beyond network with process, identity and time.
- **On-Premises *and* in Cloud**
  Maintain app risk posture across your enterprise.
- **Detect *and* Respond**
  Go beyond a single assessment with continuous monitoring *and* enforcement.
- **Integrate in CI/CD Toolchain**
  Good risk posture begins before deployment.

CONTINUOUSLY MONITOR ON CIS CRITERIA OUT-OF-BOX, OR AS YOU CUSTOMIZE TO WHAT'S IMPORTANT FOR YOUR ENVIRONMENT.

BASIC	FOUNDATIONAL	ORGANIZATIONAL
☐ Inventory & control of hardware assets	☐ Email & web browser protections	☐ Implement a Security Awareness & Training program
☐ Inventory & control of software assets	☐ Malware defenses	☐ Application software security (supporting tools)
☐ Continuous vulnerability management	☐ Limitation & control of network ports, protocols & services	☐ Incident response & management (supporting tools)
☐ Controlled use of administrative privileges	☐ Data recovery capabilities	☐ Pen tests & red team exercises
☐ Secure configuration for hardware & software on [...] servers	☐ Secure configuration for network devices [...]	
☐ Maintenance, monitoring & analysis of audit logs	☐ Boundary defense	
	☐ Data protection	
	☐ Controlled access based on need-to-know	
	☐ Wireless access control	
	☐ Account monitoring & control	

CIS. Center for Internet Security®

BRIEF

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've 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.

AVAILABILITY

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

RECOGNITION

TAG CYBER 2020 DISTINGUISHED VENDOR

TECH 2020 WINNER

CROWDSTRIKE Store Partner of the Year

GET FORTIFIED

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

+1 201 766 2023

sales@truefort.com

WWW.TRUEFORT.COM

[1]Gartner | How to Make Cloud More Secure Than Your Own Data Center | Oct 2019 | Neil MacDonald & Tom Croll | [Gartner subscription required]

[2]DataCenter Knowledge | Four Main Types of Cyberattack That Affect Data Center Uptime | June 2019

[3]KuppingerCole | KuppingerCole Report: Executive Overview -TrueFort Fortress XDR | Nov 2019 | Alexei Balanganski

[4]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-SB-APPPOS-1.2-0520