TRUEFORT

ACCELERATE DIGITAL TRANSFORMATION AND CLOUD MIGRATION
VISIBILITY AND CONTROL WITH FORTRESS

Fortress helps you modernize and securely migrate apps and workloads between on-premises infrastructure, legacy systems, and the Cloud.

SMART MIGRATION – DON'T JUST 'LIFT & SHIFT' TO THE CLOUD

According to the TechRepublic, 2020 is the year of cloud migration and modernization.[2] In fact, despite COVID's impact on data center budgets and a growing trend toward workload repatriation, market numbers show that business investment into hybrid and multicloud environments continues to accelerate. At the same time, this rush to cloud is contributing to increased service loss, data breach and cost due to misconfiguration, incorrect security architecture changes and policy updates. So, to avoid these and other issues, it is important to consider:

- **Do you have the visibility** needed for planning to determine readiness and suitability of migrating or repatriating workloads?
- **Will you be able to accurately assess and report** on the migration outcome - whether success, failure or action required?
- **Can you ensure security posture and policy** requirements will be met with a changing architecture and threat landscape?

Although the cloud provider technologies that help you migrate and secure applications have improved, going hybrid or multicloud requires in depth insight across multiple, disparate providers and proprietary vendor environments - starting with your own. And they won't help you repatriate. Just knowing the infrastructure is not enough - you need to really know your apps.

PROTECTS APPS BY HELPING THEM MIGRATE SECURELY

We can help. Fortress protects enterprise applications everywhere – **whether on premises, in containers, or in the Cloud**. A single pane of glass for your critical applications, wherever they may reside

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, connections, configurations, and the time and identities of access or attack. Map application level relationships to document upstream and downstream dependencies and understand the impact of moving workloads.

93%

Surveyed enterprise organizations have a multi-cloud and provider strategy.[1]

SOLUTION HIGHLIGHTS

- **See & Inventory App DNA**
  Improve migration planning and understanding of legacy Applications. Update CMDBs with visibility into workload roles, configurations, dependencies, relationships, users, and flows.
- **Pre- & Post- Migration Reports**
  Baseline, monitor, report, and assess application behavior before and after migration.
- **Maintain Risk Posture & Policy**
  Detect and block new threat vectors while enforcing consistent hygiene and security standards - wherever your apps may roam.

BRIEF

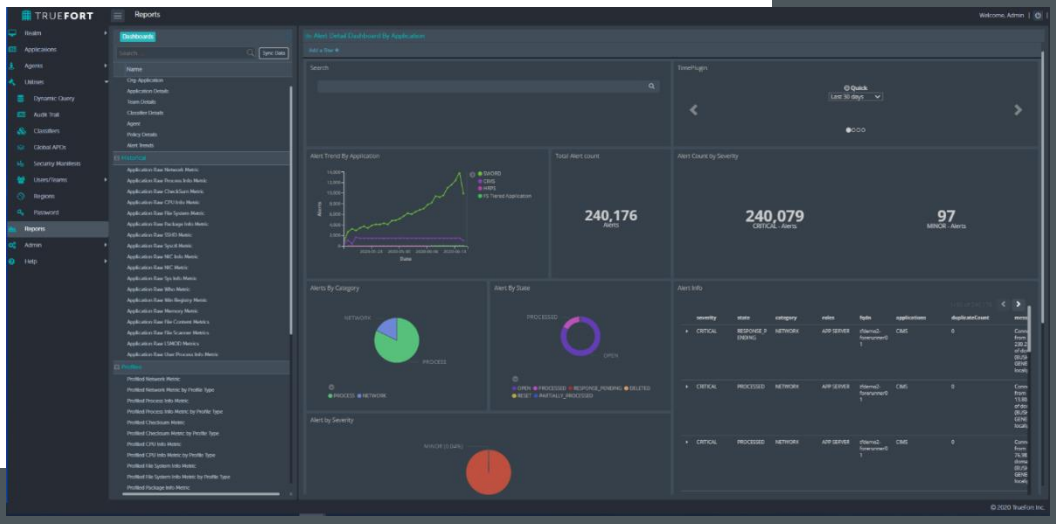
WHAT IT SOLVES & WHAT IT REPLACES

To successfully and securely modernize, migrate or repatriate critical applications and their workloads, the enterprise needs full detail visibility down to the DNA-level of how an app is managed and used by the business. That insight is needed before, during, and after cloud migration. And most importantly, once in place, teams need to ensure the app still works, meets SLAs, is secure, and proves the migration was the right operational decision for the business. Normally this requires a combination of tools, services, skilled staff and a lot of time and effort to succeed. Products often include CMDBs, cloud workload protection, cloud security posture management, and endpoint/server protection solutions for legacy systems. With Fortress you get both app migration support and full app and cloud workload protection in a single console:

- Full visibility and profiling of app configuration, risk posture, security policy, and real-time behavior before and after migration.
- Cross-platform support from bare-metal or legacy environments, to virtual, container and public cloud so you can seamlessly and consistently secure your apps and their workloads.
- Advanced reporting on-demand for comprehensive assessment, documentation, compliance, and audit.
- Centralized, auto-generated security and micro-segmentation policy, monitoring and enforcement.

SOLUTION USE CASES

- **Cloud Migration Readiness**
  Account for virtual, containerized, and physical components and network dependencies during planning to ensure that you avoid service loss and adopt the right cloud controls.
- **Cloud Migration Validation**
  Monitor, report, and evaluate function, upstream and downstream dependencies and security for change management and SLAs.
- **Centralize Security**
  Use a single console to dynamically update, manage and enforce consistent app and workload security policy from the ground-to-the-cloud.
- **Cloud Security is not the Same**
  Enable security teams to rapidly understand, adopt and leverage emerging cloud security capabilities to control cloud applications.



CHANGE WITH VISBILITY | PRE & POST MIGRATION ASSESSMENT REPORTS

Profile Production Apps Within Their Business Logic Context

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

Audit Across Policy, Current State & Behavior

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

Identify Top Risks in Unique & Disparate Environments

- Vulnerable software and infrastructure
- Unmanaged accounts and unencrypted authentication
- Unencrypted and abnormal connections
- Unusual process execution

BRIEF

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 integrations your agents, integrations, and feeds. This will provide immediate values 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.

"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."

–

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.

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 performance and volume tech based on Wall Street high frequency trading systems.
- **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**
  Good risk posture begins before deployment

FORTRESS SUPPORTS YOU IN

CLOUD MIGRATION

AS YOU ASSESS THE LANDSCAPE,

DETERMINE STRATEGY,

... AND EXECUTE YOUR PLAN.

CSA EGREGIOUS 11	MITRE ECAF	FORTRESS
▪ Data breaches	▪ Establish security tolerance	▪ Inventory apps with detailed visibility into network relationships tied back to process, and identity,
▪ Misconfig & 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		

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 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

TAG CYBER 2020 DISTINGUISHED VENDOR

TE 50 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, and whether you choose our TrueFort 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.