TRUEFORT

# VISIBILITY, GOVERNANCE & COMPLIANCE WITH FORTRESS

## *File Integrity Monitoring (FIM)*
## *System Configuration Monitoring & Hardening*

BRIEF

**Fortress** provides critical configuration monitoring to secure applications and meet regulatory compliance - in addition to real-time application detection and response.

### File Integrity Monitoring is Essential

File integrity monitoring (FIM) is a type of change auditing, verifying and validating operating system (OS), database, and application software files by comparing them to a known, trusted "baseline." identifying if they have been tampered with or corrupted. Fortress can generate alerts to enable further investigation or remediation if it detects that files have been altered, updated, or compromised. FIM encompasses both reactive (forensic) auditing as well as proactive, rules-based active monitoring, providing a critical layer of file, data, and application security - alerting to potential risks and aiding in incident response.

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

The primary FIM use cases are:

### Detect Illicit Activity

Altered critical system or application files may be an indicator of a cyber-attack. Even if log files and other detection systems are circumvented, FIM can detect changes to important parts of your IT ecosystem. With FIM in place, you can monitor and protect the security of your files, applications, operating systems, and data.

### Meeting Compliance Mandates

The effort imposed by regulation and compliance requirements is ever increasing and enterprises are hard-pressed to keep up. Fortress provdes the ability to easily audit change monitor and report on activity required for regulatory compliance with GLBA, SOX, HIPAA, and PCI DSS.

### Pinpointing Unintended Changes

Inadvertent file changes can cause problems. Sometimes the ramifications of these changes may be small and go overlooked. Other times, they can create security backdoors, or impact business operations, or continuity. File integrity monitoring simplifies forensics by identifying changes to roll back or take other remediation.

### Verifying Update Status and Monitoring System Health

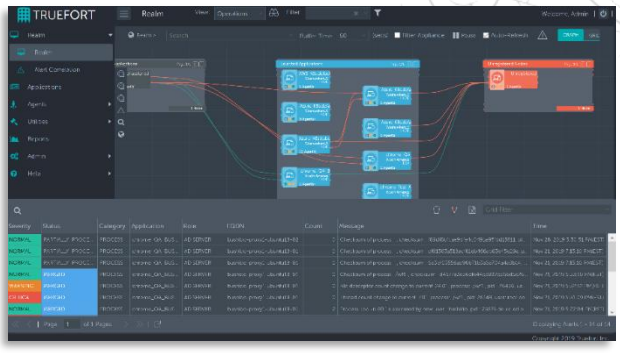
Fortress can ensure if files are patched to the latest version by scanning installed versions across multiple locations and machines with the post-patch checksum.

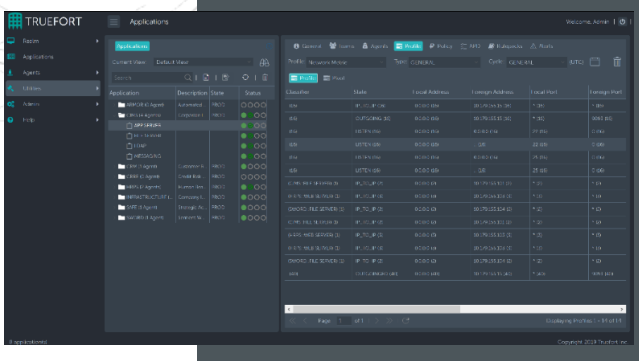
### File Integrity Monitoring Addresses:

- Who modified the file
- When and what changes have been made
- Unusual changes in file size, version, and configuration
- Changes in settings, permissions, and registry keys.
- Unauthorized access of confgs and secrets, system binaries, and directories

## SOLUTION HIGHLIGHTS

- **Fastest ROI in the Market**
  Time to value measured in days...not months. Meet your compliance objectives faster and on-budget.
- **Continuous Compliance Monitoring**
  Comprehensive alerting and reports provide vital evidence to security, management, and auditors of your secure and compliant posture.
- **Support for Hybrid Environments**
  Complete visibility from a single solution for security & compliance for on-prem and cloud
- **File Hash Delta**
  Analyze system file changes. Identify bad changes to critical system and application files.
- **Critical Configuration File Content**
  Monitor changes to the contents of critical configuration files that could lead to the compromise of systems holding valuable data.
- **File and Folder Access Monitoring**
  Protect the critical data that companies process, store, and transmit in order to conduct business.



## Automate System Configuration Monitoring and Hardening

System Hardening is the process of securing system configurations and settings to reduce IT vulnerability and the possibility of compromise. Secure critical applications and environments by reducing the attack surface and attack vectors which threat actors continuously exploit for purpose of malicious activity.

By ensuring a secure and compliant state for applications combined with ongoing, context-based change control and baseline management, Fortress makes streamlining the system configuration processquick and easy.

Removing or disabling unnecessary functions from IT systems is a key security control and a core dimension to any system hardening project. Some controls are obvious to remove or control the use of. For example, FTP and Web services should be removed if not needed. However, now that the Windows Operating Systems ship with over 200 default services, managing drift has become progressively more difficult.

## CIS Benchmarks

As one of a handful of CIS Vendors, TrueFort has a broad range of CIS Benchmark reports which can be used to monitor critical environments for drift from the hardened build standard, to ensure systems stay within compliance 24/7. CIS Benchmarks are the option of choice for auditors when advising organizations on a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, These benchmarks provide out-of-the-box guidelines that immediately enable you to meet compliance standards and safeguard operating systems, software and networks that are most vulnerable to cyber-attacks. The guidelines can also be used a s starting point to configure environment specific controls.

Fortress monitors CIS benchmarks to two levels of security settings:

### Level 1

Essential requirements that cause little or no service interruption or reduced functionality.

### Level 2

For environments requiring greater security that may result in some reduced functionality.

## Broad OS Support

Fortress provides System Configuration Monitoring for a broad base of modern systems including Windows, many Linux variants including RHEL, SuSE, Ubuntu and even specialty OS like AIX and Solaris. You can be confident that your environment is covered

## Ease of Management

Deploy with confidence! A single pane of glass and advanced automation enables central monitoring of your whole environment. CIS Benchmarks can be configured to meet operational requirements for specific environments or applications. Change is certain, and Fortress has automation in place to easily enable continuous policy monitoring .

## Business Drivers

Applying baseline security standards across digital infrastructure should be a foundational practice for every organization.

- **Reduce Your Attack Surface**

  Become a smaller target, making resources invisible or resilient to threat actors. Many services enable ports which an attacker can use to disrupt or gain access to the platform

- **Crown Jewels**

  Protect the most critical applications to the enterprise first and reduce the threat attack surface.

- **Compliance**

  Meet regulatory standards such as SWIFT, PCI, GDPR, HIPAA with ease.

- **Get Going Now**

  Enterprises need System Configuration Monitoring and a process to verify and approve changes to critical systems. This provides a clear capability for breach detection and for cyber defense measures to be maintained.

- **5-Minute Setup**

  Use your existing configuration to establish a baseline and immediately begin monitoring for unauthorized change and misconfiguration.

- **Prioritized Risk Scoring**

  The more functions a platform has, the greater the potential for misuse/abuse. Identify and fix your highest-risk items using prioritized risk scoring for misconfigurations.

CIS Center for Internet Security®

vmware Microsoft

AIX solaris

CROWDSTRIKE

## COMPREHENSIVE APPLICATION PROTECTION

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

## FILE INTEGRITY MONITORING AND SYSTEM CONFIGURATION MANAGEMENT

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 | | |

## 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, 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.



TF-1.0-0420

## 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