TRUEFORT

BRIEF

INCIDENT RESPONSE WITH FORTRESS™
RESPOND IN REAL-TIME, UNDERSTAND IN MINUTES

TrueFort Fortress™ for Threat Hunting and Incident Response allows you to see everything. No more APTs hiding in your environment for days, weeks or months!

Get on Top of Risk.

When it comes to Threat Hunting and Incident Response, most organizations lack the skills, access, tools and most importantly, the resources to do an adequate job. In some cases, MITRE frameworks have been implemented to help integrate Threat Intelligence, but the challenges of empowering and enabling security specialists to perform Threat Hunting and optimizing Incident Response remain.

The team that created Fortress learned their lessons the hard way, responding to incidents while blind to the movement, tactics, and techniques of Advanced Persistent Threat actors. They leveraged their years of experience managing world-class environments and building and deploying monitoring and management systems at scale. The result is a Fortress, a real-time analytics and response platform focused on applications instead of infrastructure. It ingests telemetry and uses patented analytics to present actionable data using an easy to use, searchable graphical model - no data lake or analysis after the fact. Fortress identifies your current exposure to APTs, detects compromises, and alerts on and mitigates risk using automated response.

Threat Hunting and Incident Response enabled by REAL TIME VISIBILITY, ANALYTICS AND RESPONSE to understand and control deviation from baseline behavior in dynamic compute environments.

Secure Your Applications and Manage Your Risk

Fortress - a single platform that provides:

- A unified interface for Threat Hunting and Application Risk Posture *as well as* incident detection, alerting and response.
- The capacity to Threat Hunt in real-time with a rich, graphical interface. Use data from your threat intelligence tools (MITRE etc.) to immediately understand your level of exposure to risk and the impact on your business.
- The information needed to effectively distribute the effort for security. Understand and communicate risk, likelihood & impact across the business, whatever your role – line-of-business, executive or technologist.
- Analytics with an application context for deep insight and understanding.
- Ready-to-use real time alert and response capabilities, powered by out-of-the-box workflows.

Imagine being able to take threat indicators from your intel platform and understand - *in seconds* - where you are at risk across a data set that is 100% up to date. Access reports that articulate risk and impact. Slice and dice the data in seconds to inform and update the organization with context. Understand if exploitation has actually occurred to focus the security team on forensics and mitigation. Go from notification of a threat to understanding the impact in a matter of seconds.

Fortress is always working to protect you. Even before the threat intel process is complete, the platform detects unusual behavior against a baseline across 150 unique pieces of telemetry - not only network, but process, identity, software, configuration, file systems, and more. Any deviation is alerted on and visualized in a map with state and context. Many anomalies can be automatically mitigated using our built-in real-time response capabilities or by integration to your own playbooks.

54

Average number of days it takes to contain a breach in the Financial Services industry.

SOLUTION HIGHLIGHTS

- **Real-Time Network Visibility**
  Identify workloads and internal and external connections and dependencies from the cloud to the ground.
- **Real-Time Process Visibility**
  Continuous monitoring using behavioral baselines to detect and block anomalous behavior in real time, as a compliment to any workload isolation
- **Real-Time Response**
  Workflow-driven, rules-based, real-time response. Block network connections, kill process, disconnect users, API-driven action in 3rd party tools.
- **Identity**
  Identify who logs in, from where, with which credentials and 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 zero-trust, micro-segmentation.
- **Bring Your Own Agent**
  Leverage existing investment in EDR tools (CrowdStrike, Tanium, etc.) to accelerate your deployment, provide immediate visibility, and support enforcement.

BRIEF

Power, Speed, Precision & Control

Threat Hunting and Incident Response are complex activities with many areas that require significant improvement. With Fortress, it's possible to achieve dramatic increases to visibility and understanding of risk across the environment as well as significant reduction of remediation time. To achieve this, Fortress has adopted five principles:

- Deliver comprehensible real-time visibility, with application context – enable your experts to work together.
- One platform for all applications from the Cloud to the Ground – streamline your process and rationalize toolsets.
- A fanatical approach to improving Application Risk Posture – align security, business and development teams and enable collaboration.
- Holistic application protection from the basics through to zero-trust.
- Address Insider Threats, APT's and System and Orphaned Account abuse.

Response When Mitigations Fail

Even the most diligent and best prepared organizations can find themselves exposed, and it is critical to have capabilities in place to understand and respond to these situations when they occur.

Fortress provides rule-based workflows to address most common anomalies, reducing time to action and enabling your teams. Automatically generate policy to isolate an application, block a network connection within milliseconds or disconnect unauthorized or orphaned identities. This capability frees up your experienced resources to be proactive instead of reactive, allowing them to secure the next generation of applications and leverage the benefits of automation.

During the heat of an incident, two specific challenges need to be addressed.

1. Context switching and lack of orchestration and automation causes delays and burns out security and response teams. This contributes to error and increases MTTD and MTTR.
2. When data, analysis and state need to be communicated across different teams, there organizations lose 'flow' – different people need different information at different times.

How it Ususally Happens

The impact of this is probably best illustrated with a concrete example. Let us examine the response to WannaCry, a typical example of incident response gone wrong.

In a traditional Incident Response model, the flow is usually as follows:

1. A user is usually the first responder and identifies that there is a problem.
2. A security specialist is notified and requests permission to access and scan the desktop. Meanwhile many other users begin to report an issue.
3. The network team is drafted to protect the perimeter, which is an exercise in futility.
4. The storage team scrambles to ensure backups are in place and hopefully offline.
5. IT security and business leadership demand minute by minute updates because updating the Service Management tool will have to wait until later.
6. While this is going on everyone 'hopes' that someone is shutting down all critical services to contain the blast radius – but they are too late.

Constant context, tool and team switches slow down the response and allow the problem to spread unchecked. This is compounded by continuous calls, meetings, and the need to communicate extensively - exhausting valuable time and resources!

The New Standard

Let us contrast this with the Incident Response flow with Fortress. Anomaly detection is automated and occurs within seconds. The Incident Response specialist is immediately informed and in control with all events and detail presented in an actionable manner.

1. New process mssecsvc2.0 is detected, alerted, visualized with kill-chain, and killed.
2. SMB V1 – is detected, alerted, visualized, and blocked.
3. The Registry change - detected and alerted
4. File name change – detected, alerted – original contents are preserved.
5. New network traffic on port 445. – detected, alerted, visualized, and blocked.
6. Network connection to untrusted URL – detected & visualized so you can take action.

Fortress detected, alerted, and helped respond to the exploit, even before it was identified through the CVE process. Throughout the entire incident, teams were able to observe the same real-time alerts and dashboards, enabling communication and collaboration with clarity, comprehension, and context.

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 intelligence platform to identify and alert on process checksum and runtime state anomalies.

- **Forensic Information on the Fly**

  Just click and drag our DVR controls to review your application's behavior down to network and process on an individual workload.

- **Uncover Critical Threats**

  Fortress detects advanced threats by leveraging machine learning 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.

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.

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

– KuppingerCole

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

TrueFort 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.

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.

FORTRESS SUPPORTS YOU IN

INCIDENT RESPONSE & THREAT HUNTING

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.

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 · Pivotal · FORTINET Fabric-Ready · Infoblox · 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.

RECOGNITION

Network Products Guide IT World Awards 2019 Silver · computing Security Excellence Awards 2019 · OSPA Finalist · CRN Tech Innovators Finalist 2019 · TAG Cyber 2020 Distinguished Vendor

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 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

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 platform.