TRUEFORT

BRIEF

FORTRESS AND CROWDSTRIKE

VISUALIZE AND SECURE YOUR CRITICAL APPLICATIONS

Fortress and CrowdStrike prevent compromise and reduce risk by continuously identifying and locking down the most common causes of breach.

Leverage your investment in CrowdStrike™ with Fortress

Fortress for CrowdStrike™ is the first Application and Cloud Workload Protection platform to secure Critical Applications in the Enterprise. It provides application focused visibility and proactive detection capabilities to provide deep understanding of applications, automate the identification of orchestrated stealth attacks and alert before data is lost. Visualizing and correlating current and historical event information and alerting on anomalous behavior in near real-time, Fortress can identify indicators of advanced threats that would otherwise go unnoticed.

2019 WINNER

CROWDSTRIKE

2019 CrowdStrike Store™ Partner-of-the-Year

Security and DevOps Are in the Dark

Security teams are challenged to secure increasingly dynamic hybrid and cloud environments, maintain visibility into running applications, monitor for compliance and quickly detect breaches.

When modifying or deploying new security policies, security teams are often in the dark - they cannot see the actual application flows in their environment - leading to slow change processes and inadequate security controls. When sophisticated attackers do get in, traditional security tools and policies fail to detect their movement. This allows them to dwell inside and live off the land for months...or years.

99%

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

SOLUTION HIGHLIGHTS

- **Fastest ROI in the Market**
  Time to value measured in days...not months.
- **Accelerate Investigation/Response**
  Reduce forensic investigation costs of cyber-incidents. Reduce MTTR and streamline efforts with contextual data and historical playback capabilities.
- **Leverage CrowdStrike**
  Leverage existing investment and extend value to provide application visibility and understanding.
- **Stop Potential Attacks and Lateral Movement**
  Detect and prevent breaches before they occur. Visualize East/West traffic behind perimeter firewalls and understand anomalies.
- **Visibility into Critical Applications**
  Gain visibility inside all your applications - generate Application Dependency Maps (ADM), understand relationships and flows, update CMDB with live data.

Visualize & Secure Critical Applications with Fortress

Fortress leverages real time-telemetry to visualize application behavior (network, process, and identity) from an application context in an easily digestible graphical format.

TrueFort is a leader in Application and Cloud Workload Protection. Developed by top cyber security experts, Fortress is changing the way organizations fight cyber attacks in their environment.

Use CrowdStrike and TrueFort to Identify APTs & Insider Threats

- Understand User/Process/Network on each workload
- Create an accurate inventory/CMDB of critical applications
- Visualize application relationships, dependencies, and flows
- Baseline system behavior across network and process
- Identify high-risk threats
- Near real-time behavioral anomaly detection and alerting
- Gain visibility into network, application, and user activity
- Automate micro-segmentation policies

TrueFort-CrowdStrike Solution Summary

Behavioral Analytics

- Uses scalable high-throughput, low-latency technology based on Wall Street trading systems.

Detailed Fortress and CrowdStrike Telemetry

- Go beyond network with process, identity, and time
- From the cloud to the ground
- Improve app risk posture across your enterprise
- Detect, respond, improve, automate
- Continuous monitoring and enforcement

- **Frictionless, Zero Risk Implementation**

  No new agents or infrastructure changes. Just connect to your existing CrowdStrike deployment in AWS and begin analyzing.

- **Application Behavioral Analytics**

  Pre-built analytics for critical applications that would take months of custom development to achieve. The only intelligence platform to identify and alert on application anomalies, helping to mitigate Zero-Day vulnerabilities and Advanced Persistent Threats and Ransomware.

- **Alert on Unauthorized Traffic**

  Visualize east/west traffic invisible to perimeter firewalls and detect Insider lateral movement.

- **Uncover Critical Threats**

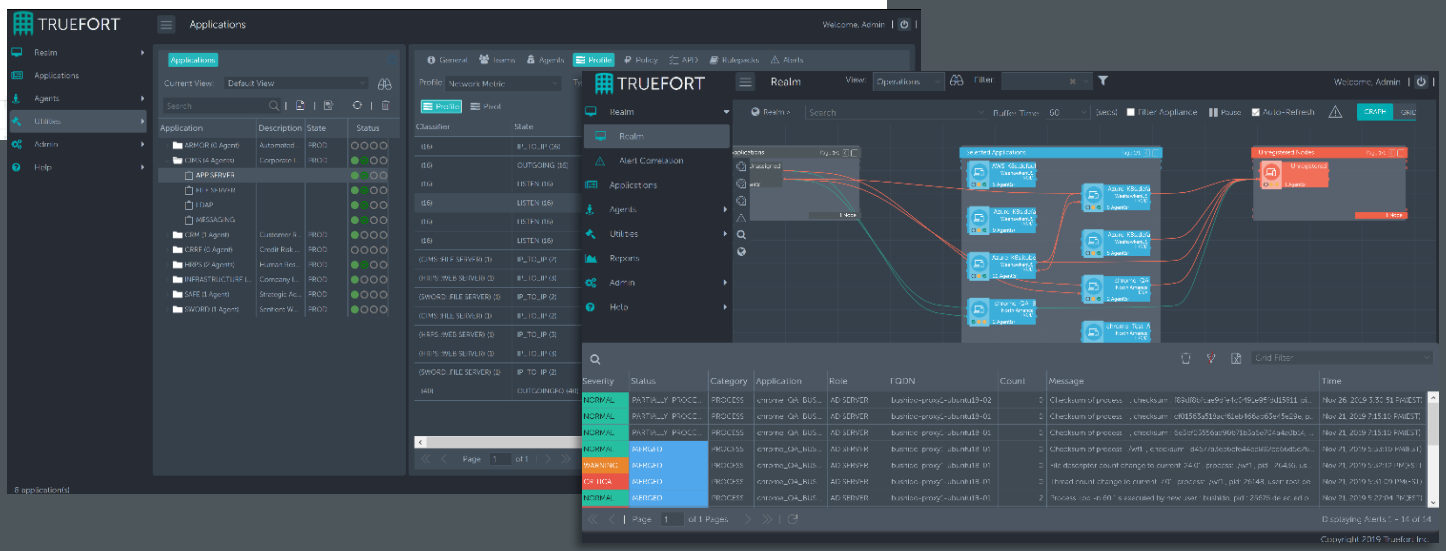
  Detect threats by leveraging machine learning and real-time analytics. Advanced event correlation and application context generates focused alerts allowing you to solve problems quickly.

- **Forensic Information on the Fly**

  Just click and drag our DVR time slider to review your application's network or process behavior down to the individual workload.

- **Threat Intelligence Transformed**

  Fortress transforms cybersecurity operations with automation, visualization and forensic capabilities, enabling teams to become proactive and efficient.



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 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."[3]

– 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 XDR SUPPORTS YOU IN

APPLICATION DETECTION AND RESPONSE

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 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

[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 20194
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.