

Data Sheet

TRUEFORT FORTRESS: ZERO TRUST APPLICATION PROTECTION

Prevent advanced persistent threats, data exfiltration and lateral movement of attacks

CHALLENGES

Applications are the most complex and dynamic element of an organization's security landscape. Yet most organizations lack comprehensive visibility into their constantly evolving application environments, creating problems with security, incident response, compliance, cloud migration and other critical business requirements.

Modern application environments present a sprawling attack surface with many entry points and opportunities for lateral expansion within the environment. Without the ability to dynamically observe application behavior, organizations cannot effectively block or contain ransomware, insider threats, supply chain or other cyberattacks.

Infrastructure-based products, point solutions and snapshot tools compound the problem by providing limited or immediately out-of-date views of the application environment and require deployment and management of multiple agents, delaying time-to-value. Organizations struggle to gain a holistic view across these tools, and security teams suffer alert fatigue and are overburdened with establishing and adapting policies in manual, rule-based frameworks. With all of these challenges, tools are often deployed to only a subset of applications and workloads, increasing risk across the business.

SOLUTION

Using the CrowdStrike Falcon® platform, the TrueFort Fortress platform provides Zero Trust application protection that secures all of your application and cloud workloads, from cloud to ground. You can now power even more visibility, control, detection and response at the application level — no additional agent required. Using TrueFort Fortress with CrowdStrike Falcon, you'll start seeing results within hours, gaining an understanding of your application environment including all of its flows and dependencies.

TrueFort Fortress takes a unique behavior-based approach, first understanding how each of your applications should behave, then applying machine intelligence and automation to continuously assess and learn each application's trusted runtime behaviors. This creates a trusted baseline of authorized behavior that is automatically adapted as needed over time with individual application trust profiles combining to create a dynamic application trust graph for your entire application environment. The TrueFort Fortress platform automatically and intelligently generates policies based on observed behavior, monitors for anomalies, streamlines investigations, enables automated policy enforcement and delivers robust reports — restricting trust to only approved application behaviors.

KEY BENEFITS

Automate Zero Trust application protection with TrueFort and CrowdStrike

Get continuous cloud-to-ground application and workload visibility

Reduce false positives and mean time to respond (MTTR) with behavior-based anomaly detection

Enhance protection and incident response with automated policy creation and enforcement

Secure applications through deep visibility, advanced microsegmentation and safe cloud migration



TRUEFORT FORTRESS: ZERO TRUST APPLICATION PROTECTION

USE CASES/BUSINESS VALUE

Challenge	Solution	Benefits
Enable a Zero Trust application environment	Detect anomalies like lateral movement with behavior-based application trust profiles	Reduce excessive trust and related risks
Get cloud-to-ground application visibility	Combine telemetry from the Falcon platform with a complete runtime application view and drill-down detail	Understand and secure dynamic and complex application environments
Accelerate your cloud migration	Automatically map application connections and dependencies	Securely migrate applications to the cloud and protect them once they are there
Get better microsegmentation	Take advantage of TrueFort's advanced behavior-based segmentation	Easily automate, maintain and enforce microsegmentation policies

TECHNICAL SOLUTION

TrueFort Fortress leverages the event-based telemetry collected by the Falcon platform to deliver immediate application visibility and analytics (on premises, over Kubernetes or in the cloud) powering our advanced behavioral analytics engine. Simply set up the TrueFort virtual appliance on premises or in the cloud, connect to your Falcon deployment, and start seeing your runtime application environment within hours.

Through the TrueFort console or REST API, you can configure, manage, investigate and develop sophisticated workflows for targeted visibility or response to events. You'll be able to understand application relationships, update inventory, detect anomalies, export to your SOAR/SIEM platforms and, of course, send alerts back to your Falcon console. Plus, in the TrueFort Fortress console, a simple opt-in allows you to automatically generate microsegmentation policies that are pushed to the Falcon platform, which uses Falcon Firewall Management™ for enforcement, programming the host firewalls native to the server operating system.

KEY CAPABILITIES

- **Single, lightweight CrowdStrike Falcon agent:** Extend your CrowdStrike investment to automate Zero Trust application protection.
- **Behavior-based application environment protection:** Create an adaptive trust profile for each application and an enforceable trust graph based on known secure behaviors.
- **Cloud-to-ground visibility:** Know and protect all of your applications and workloads with a unified view and granular control across cloud, hybrid, containerized and traditional environments.
- **Automated policy generation:** Auto-generate policies to conform to and enforce known secure behavior, even as applications are added or updated.
- **Safe enforcement:** Place policies in alert-only mode for virtual enforcement or integrate with other tools (e.g., SOAR/SIEM) for active enforcement.
- **Immediate incident playback:** Leverage a DVR-like feature to record and play back events for immediate attack and impact assessment.

“The CrowdStrike and TrueFort solution gave us instant visibility into all the communications between our data center applications, allowing us to see and address unapproved and anomalous communications.”

— Global 1000 Manufacturer

TrueFort is a CrowdStrike Elevate Partner and inaugural solution on the CrowdStrike Store™.

Experience how TrueFort extends your CrowdStrike investment for Zero Trust application protection. Contact TrueFort today to get a demo:
www.truefort.com

ABOUT TRUEFORT

TrueFort Fortress is the real-time zero trust application protection platform that is purpose-built to secure dynamic and complex application environments cloud-to-ground, leveraging CrowdStrike telemetry, advanced behavioral analysis, machine intelligence and automation to reduce excessive trust and related risks.

For more information visit www.truefort.com and follow us on Twitter and LinkedIn.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Learn more www.crowdstrike.com

