TRUEFORT

SOLUTION BRIEF

TrueFort and CrowdStrike: A Strong Partnership

Executive Summary

As an inaugural partner in the CrowdStrike Store, TrueFort integrates with CrowdStrike Falcon EDR to provide application workload visibility, auto-generation of behavioral-based enforcement policies, and microsegmentation. TrueFort does this by leveraging CrowdStrike Falcon EDR agents and Firewall Management module.

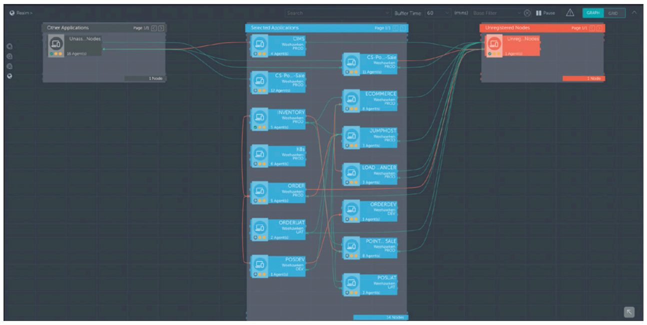
Advanced persistent threats (APTs) and insiders use a combination of tactics and techniques to discover and attack crown-jewel applications in an enterprise environment. CrowdStrike provides a layer of protection of the individual endpoints or servers making up these applications to ensure that these individual nodes are not compromised in an attack. On top of this layer of protection, TrueFort leverages CrowdStrike Falcon agents across the application estate to apply security controls such as microsegmentation as well as detection and alerting capabilities that defend against APTs and insiders that employ "living off the land" and "fileless" tactics that fly under the radar of solutions deploying traditional detection methods.

TrueFort integrates with CrowdStrike EDR to provide application workload visibility, auto-generation of behavioral-based enforcement policies, and microsegmentation to protect against known and zero-day threats.

Extending the Investment

TrueFort extends your CrowdStrike investment to deliver zero trust application protection by consuming CrowdStrike telemetry to visualize application flows and dependencies automatically generating enforcement policies from observed behaviors and anomalies. Understanding the context – the what, who, when and how of the incident – enables smart risk prevention.

Application Visibility – TrueFort automates comprehensive and continuous mapping of complex application relationships including dependencies and data flows down to the process, identity and network detail. This enables security teams to facilitate and accelerate data center consolidation, rationalization and cloud migration planning while establishing zero-trust security controls on application environments.



Behavioral Profiling – TrueFort uses Machine Learning to continually assess and learn the applications behavior and create an Application Trust Profile - a baseline for authorized behavior while monitoring and preventing risk-related behaviors. TrueFort automatically creates granular application trust profiles while enabling you to operationalize your risk posture control across all applications.

Risk Management Prevention – In today's application-centric business, detecting and alerting on anomalous application and user behaviors from APTs and insiders such as zero-day, supply-chain and ransomware attacks put a constant strain on teams to stay one step ahead of the threats. Automated detection and alerting on anomalous behavior, enables quick action on attacks that cause risks to the business.

TrueFort extends your CrowdStrike investment to deliver Zero Trust application protection by using the CrowdStrike Telemetry to visualize application flows and dependencies.

How It Works

TrueFort builds upon CrowdStrike's OS and process inspection with behavior-based application workload protection by creating an application trust profile and an enforceable application trust graph based on known secure behaviors. Actionable deliverables include:

Map Application Dependencies – TrueFort leverages CrowdStrike Falcon telemetry to build a continuous application dependency map in real-time that captures all internal and external application relationships. This application dependency map serves as the foundation for the Application Trust Profile (ATP) or applications behavioral policies.

Automate Policy Generation – TrueFort creates an Application Trust Profile or set of behavior policies based on patented behavioral modeling that can adapt to application changes.

Drive Microsegmentation – Microsegmentation policies are based on the Application Trust Profile sourced from CrowdStrike Falcon network telemetry. Push micro-segmentation policies to CrowdStrike Falcon agents for enforcement.

Detect Anomalies – CrowdStrike customers can leverage TrueFort anomaly detection to identify behaviors that may reflect the activities of an APT or insider, without installing another agent. Additionally, CrowdStrike customers can leverage DVR-like capabilities to play back events during incident response investigations. Such replay capabilities allow incident response teams to answer questions like: Which applications are impacted by this incident and how? What was the underlying cause of the anomaly?

ABOUT TRUEFORT
TrueFort brings zero trust protection to critical business applications. Leveraging unique real-time, adaptive trust, and cloud-to-ground capabilities, the TrueFort platform detects and contains security threats before they become business risks.

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

TRUEFORT

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com