TrueFort® Platform:
Zero Trust Application Protection

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

Challenges

The Complexity of Data Center and Cloud Security

Applications can be an extremely complex and dynamic element within 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. In addition, modern application environments present a sprawling attack surface with many entry points and opportunities for lateral expansion. Without the ability to dynamically observe application behavior, organizations cannot effectively block or contain ransomware, insider threats, supply chain or other cyberattacks.

Legacy 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products, point solutions and snapshot tools compound the problem by providing limited or immediately out-of-date views of the application environment and require deployment and management of multiple agents, delaying time-to-value. Without a holistic view across these tools, security teams suffer from alert fatigue and are overburdened with establishing and adapting policies in manual, rule-based frameworks.

Solution

The TrueFort® Platform integration with the CrowdStrike Falcon® platform provides Zero Trust application protection that secures 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 Platform with Falcon, you'll start seeing results within hours, gaining an understanding of your application environment, including all of its flows and dependencies.

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 Platform takes a unique behavior-based approach, first understanding how your applications should behave, then applying machine intelligence and automation to assess and learn each application's trusted runtime behaviors continuously. This creates a trusted baseline of authorized behavior that is automatically adapted as needed over time with individual application trust profiles combined to create a dynamic application trust graph for your entire application environment. TrueFort 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.

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

> **"The CrowdStrike and TrueFort solution gave us instant visibility into all of the communications between our data center applications, allowing us to see and address unapproved and anomalous communications."**
>
> **- Global 1000 Manufacturer**

Key capabilities

TrueFort Platform leverages the event-based telemetry collected by the Falcon platform to deliver immediate application visibility and analytics (on-premises, over Kubernetes and in the cloud), powering TrueFort's 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 and response to events. You'll be able to understand application relationships, update inventory, detect anomalies, export to your SOAR/SIEM platforms and send alerts back to your Falcon console. Plus, in the TrueFort Platform console, a simple opt-in allows you to automatically generate microsegmentation policies that are pushed to the Falcon platform, which uses CrowdStrike Falcon® Firewall Management for enforcement, programming the host firewalls native to the server operating system.

This solution delivers the following 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.

TrueFort is a trusted CrowdStrike Marketplace partner providing Zero Trust application protection, leveraging the Falcon platform's telemetry and policy capabilities, to secure your applications and cloud workloads, from cloud to ground.

About TrueFort

TrueFort® Platform puts you in control of lateral movement across the data center and cloud. The TrueFort Cloud extends protection beyond network activity by shutting down the abuse of service accounts. Founded by former IT executives from Bank of America and Goldman Sachs, leading global enterprises trust TrueFort to deliver unmatched application environment discovery and microsegmentation for accounts and activity.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Try it in the
CrowdStrike Marketplace →

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/