TRUEFORT

BRIEF

PROACTIVELY PROTECT AGAINST SOLARWINDS & OTHER ATTACKS

A zero trust application environment is your best defense

The SolarWinds hack has now affected hundreds of businesses and federal agencies, and many are at a loss to understand their exposure.

TrueFort customers have been able to quickly determine where SolarWinds software is running in their environment and what it is connecting to so that they can take immediate mitigation action. And, importantly, TrueFort can detect and stop the exact types of anomalous behavior used by the SolarWinds hackers to find and exfiltrate critical data.

FORTRESS: PURPOSE-BUILT TO PROTECT CRITICAL APPLICATIONS AND DATA

TrueFort designed the Fortress enterprise security platform to prevent and mitigate just these types of attacks. Fortress is purpose-built to ensure zero trust application environments. Real-time application infrastructure telemetry combines with machine intelligence to give each application in your environment a behavioral security identity. This makes it possible to identify anomalous behavior in real-time and stop a hack in its tracks, preventing unauthorized lateral movement and malicious data access.

The SolarWinds attack has highlighted the fact that traditional security tools don't provide sufficient information about, or protection from, threats to enterprises.

START PROTECTING YOUR APPS & DATA TODAY

You can evaluate Fortress for 30 days at no charge and with no commitment. You can get visibility into your exposure and get true application protection in just 1 week using our proprietary agent or your CrowdStrike Falcon agent.
Contact sales@truefort.com to get started.

ABOUT TRUEFORT

TrueFort reduces business risk for security-focused enterprises striving for zero or lean trust application environments. Our innovative and uniquely application- centric Fortress platform delivers comprehensive real-time cloud-to-the-ground application insight, protection and automated response with patented machine intelligence and a single agent.

sales@truefort.com | +1 201 766 2023 | LinkedIn | Twitter | truefort.com

7 KEY FORTRESS CAPABILITIES THAT DEFEND AGAINST SOLARWINDS

1. Identify and control compromised SolarWinds service identities being used by the hackers.
2. Continuously monitor and alert on behavioral changes coming from SolarWinds accounts.
3. Alert and block all attack traffic to specific IPs and domains.
4. Quickly introspect SolarWinds connected systems to determine attack blast radius.
5. Apply and enforce application (micro) segmentation to restrict attacker access.
6. Detect new malicious binaries and processes being planted by hackers into customer app environments even if those binaries are being left for later activation.
7. Play back suspicious incidents and review application behavior at the network and process levels on individual workloads with DVR-like controls.

Zero Trust for Your App Environment

Immediately reduce your risk with zero trust application security.

> **READ THE BRIEF**

SolarWinds | Indicators of Compromise

A guide to how the SolarWinds attack is executed, indicators of compromise, and TrueFort queries for the relevant insight reports.

> **GET THE GUIDE**

1. to determine attack blast radius.

5. A