TRUEFORT®

SOLUTION BRIEF

# TrueFort® Platform: Mitigating Insider Risk

## Revolutionizing Cybersecurity for a Zero-Trust Future

Insider threats pose a significant risk to organizations worldwide. Without adequate detection and mitigation measures, these threats can lead to substantial financial and reputational damage, plus regulatory non-compliance. It is the responsibility of experienced CISOs, CTOs, and cybersecurity practitioners, to minimize this risk by implementing an effective cybersecurity solution.

## Insider Risk: The Invisible Threat

Insider threats emerge from individuals who have authorized access to an organization's critical systems and data. These individuals may be employees, contractors, or partners who, intentionally or unintentionally, can cause significant harm.

Examples range from data theft by a disgruntled employee to an innocent administrator clicking on a phishing link, granting unauthorized access to secure systems.

## Why Prioritize Insider Risk Mitigation?

Insider risk is a substantial threat as it is often overlooked.

The 2023 Insider Threat Report [Cybersecurity Insiders] indicates that 74% of organizations believe that they are at least moderately vulnerable (or worse) to insider threats.

More than half of organizations surveys had experienced an insider threat in the last year, with 8% having experienced more than 20.

## TrueFort Platform: A Comprehensive Solution

TrueFort offers an advanced cybersecurity platform that ensures maximum protection against insider threats, providing increased visibility, zero trust, and the ability to detect, monitor, and learn trusted connection patterns of users, applications, and service accounts.

TrueFort Platform can significantly bolster defenses against insider risks, employing a zero-trust model, and ensuring visibility and control over users, applications, and service accounts.

- **74%** of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials, or Social Engineering.

  c/o 2023 Verizon Data Breach Investigation Report

- **74%** of organizations say insider attacks are becoming more frequent
- **More than half** of organizations have experienced an insider threat in the last year, and **8%** have experienced more than **20**
- **53%** say detecting insider attacks is harder in the cloud

  c/o 2023 Cybersecurity Insiders Threat Report

SOLUTION BRIEF

# The Zero-Trust Security Model

A zero-trust (or least-privilege) security model assumes no user or device is trusted by default, regardless of its location relative to the network perimeter. With TrueFort Platform, every access request is baselined and validated, with unapproved activity triggering alerts to ensure optimal protection at a granular level across the environment.

# Full-Spectrum Visibility

TrueFort Platform's real-time visibility allows for continuous surveillance of an organization's security state. With comprehensive monitoring tools, security teams can easily oversee file integrity, validate account relationships, and ensure least-privileged access and cybersecurity best practices.

# Anomaly Detection and Behavioral Analytics

TrueFort's machine learning algorithms intelligently identify anomalous behavior, minimizing false positives while maximizing threat detection.

# Future-Proofing Your Cybersecurity

TrueFort's solution capabilities are essential for securing the modern enterprise. Integrating TrueFort into any business cybersecurity strategy can significantly enhance an organization's resilience against insider threats and help them to confidently navigate the cyber-threat landscape.

Mitigate insider risk, enforce zero trust, and protect your organization with TrueFort.

## MITIGATING RISKS WITH TRUEFORT PLATFORM

- **Automating Least Privilege Access:** TrueFort automates least-privilege access, ensuring users only have the necessary privileges for their roles.
- **Enforcing a Zero-Trust Model:** TrueFort Platform helps enforce zero-trust security principles, meaning legitimate verification for every user, device, application, and service, at a granular level.
- **Regulatory Standards:** TrueFort meets and exceeds industry standards, such as CIS benchmarking, NIST, PCI-DSS 4, HIPAA, and more.
- **Validating Account Relationships:** With TrueFort, organizations can verify the trustworthiness of account relationships, ensuring the legitimacy of access rights.
- **Monitoring Service Accounts:** Service accounts often have high-level access but lack stringent security controls. TrueFort's monitoring helps detect anomalies and prevents misuse.
- **Revealing Forgotten Accounts:** TrueFort Platform discovers and monitors inactive accounts, reducing the risk of unmonitored access points within an organization.
- **Beyond Network Segmentation:** TrueFort Platform offers optimum lateral movement protection with best-in-class microsegmentation.

**ABOUT TRUEFORT**

TrueFort 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.

**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



TRUEFORT.COM