TRUEFORT™

SOLUTION BRIEF

Service Account Protection

Contain Lateral Movement by Protecting Service Accounts

Challenges

Regulators have recognized that service accounts, or non-human privileged accounts, are high-value targets for attackers. They fall through monitoring gaps because of their high-volume daily usage. They run in the background of applications and are allowed to execute system commands, yet they're rarely rotated. They may have been set up to manage a software installation or a system provisioning process and left active after the action occurred. This enables them to go unnoticed and unmanaged for extended periods of time.

While access management solutions or password vaults sound like a great way to manage service accounts, this assumes visibility into where and how your service accounts are used. In most organizations, old, orphaned, and unmanaged service accounts have been introduced by developers or operations without realizing they neglected to properly document them in inventory, leaving a high-risk, privileged identity completely unmonitored.

Once compromised, service accounts grant attackers full access to the infrastructure, applications, systems, and critical data stores. This unfettered access enables dangerous lateral movement with a long shelf-life within your data center or cloud environments.

Top 5 Risks

- **Inadequate inventory and visibility of service accounts** restricts compliance and policy mandates
- **Access management and vaulting solutions** are not designed to discover and baseline behavior
- **Passwords not easily rotated** without breaking existing application dependencies
- **Often hardcoded during development or embedded** in supply chain code
- **Locally managed or orphaned accounts**, with no central logging of their activity

74%

Of Data Breaches Start with Privileged Credential Abuse[1]

SOLUTION HIGHLIGHTS

Discover & Inventory

- Automatically identify, report, and monitor known and orphaned account usage across data center and cloud applications
- Build list of active accounts logging on or executing commands
- Analyze commands being executed

Baseline & Manage

- Adhere to the principle of least-privilege-access and apply microsegmentation by account to prevent lateral movement
- Ensure accounts execute only allowed commands to block unwanted changes in account behavior
- Control and disable anomalous service account activity

Alert & Enforce

- Alert on suspicious executions or automatically kill actions outside of established baselines
- Alert if dormant(inactive) accounts become active
- Push logs and telemetry to systems to enable SOC teams to remediate
- Ease investigation and remediation with "DVR-like" playback details around the event to pinpoint what, when and by whom

1 - https://www.forbes.com/sites/louiscolumbus/2019/02/26/74-of-data-breaches-start-with-privileged-credentialabuse/?sh=442448063ce4

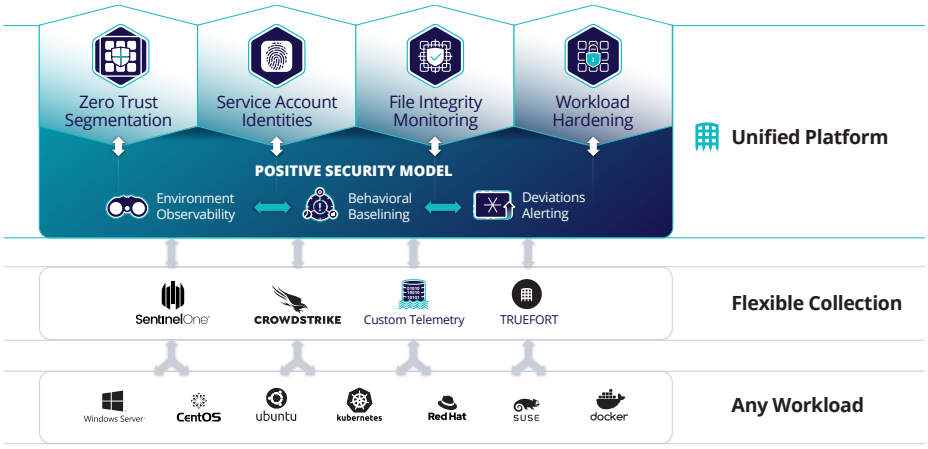
Solution

TrueFort enables you to understand and protect your business from service account abuse, reducing your attack surface.

TrueFort automatically detects, reports, and tracks all account usage across servers, workloads, and applications to prevent unauthorized behavior. By working in conjunction with existing access management and HR solutions, TrueFort profiles active accounts by recording every command executed by the account to validate ownership and need within the organization. TrueFort maps dependencies and visualizes application operations, including their dynamic behavior, their corresponding workloads, processes, network connections, and configurations. In less than a day, the TrueFort Platform absorbs telemetry from existing CrowdStrike, SentinelOne, or TrueFort agents and immediately applies machine learning. Connections outside of the approved behavioral profile can be controlled in real-time through the existing agents or host-based firewalls.

TrueFort enables security teams to take a different approach to service account management by:

- **Identifying active and dormant service accounts** used by Windows and Unix applications and building a record of compliant active accounts.
- **Profiling accounts using advanced behavioral analytics** that determine normal versus anomalous or rogue behavior
- **Controlling anomalous or rogue accounts** by stopping an action in real-time
- **Detect hard-coded accounts** in supply chain software to disable access
- **Recording executed commands and password rotations** to ensure only approved (allow-listed) activity occurs using verified application trusted profiles
- **Immediately alert the SOC or log out interactive accounts** that deviate from the approved behavior or policy.
- **Validate account relationships** to safely retire service accounts or change passwords without causing downtime
- **Automate least privilege access** to strengthen your security posture and minimize lateral movement
- **Demonstrate compliance** by profiling service account usage and changes in production applications



TrueFort makes it easy to detect, adapt, and enforce service account policies based on what accounts do within your applications and systems. It baselines behavior by learning what is normal activity, automatically establishing allow-list policies, and generating alerts on suspicious behavior.

ABOUT TRUEFORT

TrueFort is an advanced approach to protecting data center and cloud workloads that makes zero-trust architectures possible. Our platform uses continuous monitoring to deliver real-time detection and response as soon as noisy workload behavior strays from known, understood activity. By absorbing telemetry from multiple agents, we decipher all intra-application communications and trigger suspicious activity alerts. The TrueFort Platform is the only solution instilling the confidence to protect workloads across all production environments. By reducing the impact of security incidents, we increase your overall business resilience, shrink your exploitable attack surface, and enable you to take immediate action against live attacks. We bring the single truth security and application owners need to effectively protect workloads of all forms.

TRUEFORT™

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM