TRUEFORT

SOLUTION BRIEF

Service Account Analytics

Prevent Lateral Movement by Understanding Privileged Service Account Usage

Challenges

Service accounts, or non-human privileged accounts, are easy 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.

Once compromised, service accounts grant attackers full access to the infrastructure, applications, systems, and critical data stores. This unfettered access enables dangerous attack vectors with long shelf-lives within your organization.

Top 5 Risks

- **Inadequate inventory and visibility of service accounts**
- **IAM/PAM solutions unable to adequately 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, with no central logging**

Solution

TrueFort protects applications by identifying service account abuse, reducing your attack surface, and enhancing workload security.

TrueFort automatically detects, reports, and tracks privileged and service account usage across servers, workloads, and applications to prevent unauthorized behavior. TrueFort visualizes and explains application operations, including their dynamic behavior, their corresponding workloads, processes, network connections, and configurations.

Adversaries had decreased breakout time to under thirty minutes, over an hour faster than the previous year's average speed.[2]

74%

Of Data Breaches Start with Privileged Credential Abuse[1]

SOLUTION HIGHLIGHTS

- **Discover & Inventory**
  Automatically find, report, and monitor known and orphaned account usage across applications, containers and other workloads.
- **Baseline & Enforce**
  Adhere to the principle of least-privilege-access and allow-listed, application-centric microsegmentation to prevent lateral movement.
- **Alert & Evict**
  Use advanced behavioral profiling and real-time notifications to alert on suspicious executions or automatically kill unwanted actions outside of established baselines.

1 - https://www.forbes.com/sites/louiscolumbus/2019/02/26/74-of-data-breaches-start-with-privileged-credentialabuse/?sh=442448063ce4
2 - https://www.infosecurity-magazine.com/news/attacker-breakout-time-now-less/

SOLUTION BRIEF

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

TrueFort brings application context to service accounts.

- **Identify and track** privileged accounts using advanced behavioral analytics that determine normal versus anomalous or rogue behavior.
- **Ensure** only allow-listed activity using automatically generated security policy.
- **Investigate**, hunt, and report on account activity using behavior continuously analyzed over recent seconds, weeks, or years.
- **Validate** account relationships by understating applications and workload interactions to safely retire service accounts without 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 to demonstrate a baseline for accepted behavior

> Its advantage over existing detection & response tools is the fundamental focus on high-level application behavior analysis and automatic remediation of IT problems regardless of underlying infrastructures.
>
> KUPPINGERCOLE

TRUEFORT STARTS WITH INDUSTRY BEST PRACTICES AND THEN LETS YOU CUSTOMIZE MONITORING & POLICY ACCORDING TO YOUR UNIQUE REQUIREMENTS

20 CIS CONTROLS®

- Continuous vulnerability management
- Controlled use of administrative privileges
- Secure configuration for hardware & software on [...] servers
- Maintenance, monitoring & analysis of audit logs
- Controlled access based on need-to-know
- Account monitoring & control

MITRE ATT&CK®

- T1068 - Exploitation for Privilege Escalation
- T1078 - Valid Accounts
- T1088 - Bypass User Account Control
- T1098 - Account Manipulation
- T1108 - Redundant Access
- T1131 - Authentication Package
- T1136 - Account Creation
- T1177 - LSASS Driver
- T1182 - AppCert DLLs
- T1199 - Trusted Connections

NIST 800-53 [REV 4]

- AC-1 - Access Control Policy & Procedures
- AC-2 - Account Management
- AC 3 - Access Enforcement
- AC-5 - Separation of Duties
- AC-6 - Least Privilege
- AC-24 - Access Control Decisions

ABOUT TRUEFORT

TrueFort has created a new, game-changing approach to application and workload protection: Adaptive Application Trust (AAT). Based on trusted behavioral profiles, AAT unifies application protection across all your interconnected data flows, architectures, and deployment methods. Now overburdened security teams are empowered to easily create and enforce security policies across their entire application landscape, on containers, virtual machines, bare metals and Kubernetes...on premises and in the cloud...from a single pane of glass. TrueFort powers zero trust application environments with Fortress, the only real-time, behavior based, cloud-to-ground security platform. Founded by cybersecurity visionaries who have led security and IT teams at global banking leaders including Goldman Sachs, Bear Stearns and Bank of America, TrueFort protects some of the world's largest enterprises.

TRUEFORT

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM