WHITEPAPER

TRUEFORT™

Service Account Analytics

TRUEFORT.COM

The Business Problem

The Potential for Compromised Credentials

Managing the risks of uncontrolled Service Accounts

The compromise of credentials that have trusted, privileged access to 'Crown Jewel Resources' such as Service Accounts and Administrative Accounts is increasingly becoming one of the leading enterprise security threat vectors.

Service Accounts have a long shelf life as they are typically deployed to support administrative or infrastructure processes in support of the application environment. Typically, passwords are embedded into the legacy applications, making updating these account passwords for proper security hygiene, both difficult and time consuming.

Because of this, Service Accounts are often poorly managed with passwords for these accounts changing less often than User Accounts. So, while organizational security policy may state that passwords need to be changed at least once a year, this is rarely achieved due to the volume of service accounts within the organization and the large volume of services running.

Compounding this problem, access for application support is broad and privilege controls are often not enforced. This enables bad actor tactics such as 'Living off the Land' which enable hackers to move laterally and with impunity once the Service Account credentials have been accessed. In short, this type of breach provides bad actors access to a large range of datacenter and cloud workloads, thereby allowing them to monitor, access, and potentially harvest critical data stores.

> Any company that does not adequately manage Service Accounts — addressing old and orphaned accounts, restricting access and managing the integration with applications — is at a high-risk of compromise.

Technology & Risk Challenges

As an example, imagine a single Service Account running 800 different processes spanning hundreds of applications. Each time a password change is required for just this one Service Account, a significant amount of time and security team manpower is required to avoid creating outages and negative business impacts. While a password vault sounds like a great way to manage your Service Accounts in a centralized manner, this approach assumes visibility into where and how your Service Accounts are utilized. These risks are further compounded by old or orphaned Service Accounts that predate any identity governance controls.

For all these reasons, any company that does not identify unmanaged Service Accounts, correctly inventory their entitlements, and ultimately bring the Service Accounts under the control of existing identity governance systems, is at a high-risk of compromise.

Top 5 Risks
Related to Service Accounts

1. **INADEQUATE VISIBILITY AND INVENTORY** OF SERVICE ACCOUNTS – WHERE AND HOW THEY ARE USED.
2. **IAM/PAM SOLUTIONS** UNABLE TO ADEQUATELY DISCOVER AND BASELINE BEHAVIOR.
3. **PASSWORDS** NOT EASILY ROTATED WITHOUT BREAKING EXISTING APPLICATION DEPENDENCIES.
4. **HARDCODED** DURING DEVELOPMENT OR EMBEDDED IN SUPPLY CHAIN CODE.
5. **LOCALLY MANAGED OR ORPHANED**, WITH NO CENTRAL LOGGING.

Truefort's Application-Centric Approach

Security teams must take a different approach to unmanaged Service Accounts

TrueFort utilizes a unique application-centric approach to controlling Service Account risks to enterprise data.

TrueFort controls deliver:

1 **ENHANCED VISIBILITY**
Establish an inventory of where and how Service Accounts are used across the estate of applications.

2 **IMPROVED RISK POSTURE**
Identify the risks associated with Service Accounts and know where and how they are used across the application environment.

3 **NORMAL APPLICATION BEHAVIORAL PROFILES**
Profile the behavior of Service Accounts across the application environment using machine learning technologies to automatically establish allow-listed policies based on normal behavior.

4 **REAL-TIME DETECTION AND RESPONSE**
Detect anomalous Service Account behaviors baselined to a 'normal' activity profile, generate automated alerts on suspicious behavior, and respond in real-time to a potentially compromised Service Accounts.

Visibility

Before you can control your Service Accounts, you first need to understand where and how they are being used and what applications they're associated with. Unlike logging and configuration-centric products, TrueFort captures and correlates — in real-time — the execution behavior of every process, its associated identity, and all network connections using a lightweight agent that runs in the server (no instrumentation, no changes to applications required).

1. **Process** – Command and Arguments
2. **Identity**
3. **Network** – Source/Target IP and Port

This approach means that responses can be prioritized for your most critical applications and can happen in real-time, well before a compromise takes root and creates negative impacts on the business.

Risk Posture

If your environment has been compromised, TrueFort can proactively assess the risks that Service Accounts pose based on where and how the accounts are used across your entire diverse application environment. TrueFort allows you to answer these questions:

- **Which Service Accounts enable adversaries to laterally move across the application environment based on application relationships?**
- **Which Service Accounts can enable adversaries to compromise business-critical applications and data?**

Additionally, TrueFort can help clean up any inactive or unwanted Service Accounts to help reduce the attack surface. It can also provide input into the policies required to control and limit Service Account behaviors.

Profile

After visibility, policy is one of the most challenging pieces to get right as far as permitting and disallowing certain identities from performing certain tasks. TrueFort distinguishes itself from other solutions in its use of machine learning and classifiers to profile and baseline normal Service Account behavior within an application context. This approach not only accelerates the profiling and learning process, but is also highly maintainable compared to other approaches that require longer learning and re-learning cycles.

Behavioral Detection And Response

Once a behavioral profile is established, TrueFort can detect Service Account behavioral anomalies. The detection of these anomalies can not only generate alerts at a minimum, but also deliver automated response capabilities that immediately prevent the use of Service Accounts that are behaving anomalously or maliciously.

Top 5 Truefort Benefits

BENEFIT #1 – VISIBILITY

TrueFort enables an effective application and data protection strategy with real- time visibility into your environment and controls that can help correlate and respond to threats and vulnerabilities. The more you know, the more you can control.

BENEFIT #2 – IDENTITY INTERACTIONS

TrueFort helps you see and understand the interaction between identities, usage patterns (including software executed) and applications. By profiling Users, Developers, System Accounts, and System Admin interactions in your environment on a per application basis, it can spot and alert your team to unusual activity.

BENEFIT #3 – PROCESS VISIBILITY

TrueFort exposes software and processes installed or executing in the application environment, giving your team real-time feedback on changes as well as correlations with potential malicious code or software. You'll gain an understanding of the performance dynamics and be able to identify unusual process events, all with the added ability to examine what identities link to the malicious software/code or processing events.

BENEFIT #4 – RELATIONSHIPS

TrueFort reveals the relationships between applications and the ways that data transfers between them. It also recognizes unusual patterns and relationships that pose business or confidentiality risks.

BENEFIT #5 – ALLOW-LISTING

TrueFort profiles and allow-list application states, including understanding network and protocol connections in and out of applications and databases. It can also profile network activity and connections, and understand the amount of data transferred during normal patterns (with periodicity) so that any abnormal activity can be defined and detected for each application.

Response

Detecting and alerting is foundational, but effective response capabilities are transformational. The speed with which either a malicious human or bot can move through your environment along with the damage they can do 'Living off the Land' cannot be under-estimated. Chances are, your SOC team is already overloaded and may be suffering alert-fatigue, leaving them reactive, struggling to contain, let alone remediate.

In order to minimize potential damage from breaches, you need to both quickly and safely automate your mitigation response to prevent malicious damage. TrueFort can respond in real-time with mitigation precision across the most demanding environments. TrueFort provides a library of automated response options to best meet your requirements, including:

- **Users (legitimate or APT) moving between business units or from development to production; TrueFort knows where machines live and can block a port or IP address immediately, simply upon seeing a developer logging in.**
- **A user or administrator authenticated locally or via AD logging in from a new location (desktop or country), or you observe a new user.** In each case, TrueFort can terminate the session before the user even gets to the shell or into Windows.
- **A legitimate Service Account logging in but performing tasks outside of the approved process.** TrueFort can terminate the session while preserving the forensic trail, enabling you to understand everything the user did.
- **If someone hijacks a process or runs a process out of the normal profile,** TrueFort captures the account and terminates the process.

Truefort Value

- **Password vaults and password rotations** won't give you the visibility and control of your Service Accounts that TrueFort's application-centric approach can deliver.
- **The only way to change developer use of Service Accounts** is via visibility, detection, and response to unwanted behavior.
- **TrueFort complements IAM/PAM solutions** by identifying orphaned Service Accounts that may still be executing long after being deactivated.

> TrueFort proactively responds to a wide variety of Service Account abuses, reducing your attack surface and enhancing data security.

About TrueFort

TrueFort is a comprehensive, real-time application and cloud workload protection solution. TrueFort continuously protects your organization's diverse application environment - cloud, hybrid, legacy - by exposing and mitigating hidden security risks to your business. Unlike infrastructure-centric approaches, TrueFort gives security teams an integrated, application-centric solution providing unprecedented visibility, control, and threat response capabilities to reduce the attack surface across an organization's entire application estate.

TrueFort provides security teams with a range of powerful controls purpose-built to meet the requirements for comprehensive application environment protection.

▶ CONTACT US TODAY

sales@truefort.com

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.

TRUE**FORT**™

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM