Service ID Management

TRUEFORT FORTRESS™

Service ID Management

CONFIDENTIAL

www.truefort.com

TRUEFORT

TRUEFORT FORTRESS

SERVICE ID MANAGEMENT

The TrueFort Fortress Service ID Management capability has been deployed by multiple entities over the last five years, including the TrueFort executive Team (+25 Years Wall Street experience), current reference customers of various verticals, and prospective TrueFort customers via on-going Proofs of Concept. All of these entities are solving real world business problems with these capabilities of TrueFort Fortress.

This document serves as reference material to provide potential customers the insight and awareness into the Service ID Management capabilities of the TrueFort Fortress platform.

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

THE BUSINESS PROBLEM

The Potential for Compromised Credentials

Management of Service ID's

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

Service ID 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. Such updates may require changing software code and/or the use of a password vault solution.

Because of this, Service ID's are often poorly managed with passwords for these ID's changing less often than User ID's. So, while organizational security policy may state that passwords need to be changed once or twice a year, this is rarely achieved due to the volume of ID's within the organization and the large volume of services running on a single ID.

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

Technology & Risk Challenges

As an example, imagine a single Service ID running 800 different processes spanning hundreds of applications. Each time a password change is required for just *this one Service ID*, 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 ID's in a centralized

manner, this approach assumes visibility into where and how your Service ID's are utilized. Not all Service ID's can be managed via an IAM, especially Linux Service ID's. Developers take advantage of this fact and use Service ID's interactively to perform certain tasks, in the same way as adversaries who use "Living off the Land".

For all of these reasons, any company that does not adequately manage Service ID's, including addressing old and orphaned accounts, restricting access and managing the integration with applications, is at a high-risk of compromise.

Top 5 Risks Related to Service ID's

1. Inadequate visibility and inventory of Service ID's – where and how they are used.
2. IAM/PAM Solutions unable to adequately track where and how Service ID's are utilized.
3. Service ID passwords are not easily rotated without careful planning and risk of breaking applications, thus ID's are hardcoded to applications.
4. Developers using Services ID's as backdoors out of convenience.
5. Service ID's that are locally managed (Linux) or become "orphaned".

TRUEFORT'S APP-CENTRIC APPROACH

Security teams must take a different approach to managing Service ID's

TrueFort applies a unique application-centric approach to Service ID Management because apps are the gateway to enterprise data. Cybersecurity measures to protect data centers and cloud environments must be able to protect the applications that keep businesses running.

We've designed the Truefort Fortress platform with Service ID Management to do just that. The platform delivers:

1. ENHANCED VISIBILITY - Establish an inventory of where and how Service ID's are used across the estate of applications.
2. IMPROVED RISK POSTURE – Identify the risks associated with Service ID's and know where and how they are used across the application environment.
3. NORMAL APP BEHAVIORAL PROFILES – Profile the behavior of Service ID's across the application environment using machine learning technologies to automatically establish policies on normal Service ID behavior.
4. REAL-TIME DETECTION and RESPONSE – Detect anomalous Service ID behaviors comparing to a 'normal' profile, alert on suspicious behavior, and respond in real-time to the potentially compromised Service ID.

VISIBILITY

Before you can manage your Service ID's, you first need to understand where and how they are used within an application-context. **Unlike other logging and configuration-centric solutions, TrueFort Fortress 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 apps 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 apps and can happen in real-time, well before a compromise has a chance to take root and create negative impacts on the your business.

RISK POSTURE

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

- Which ID's enable adversaries to laterally move across the application environment based on application relationships?
- Which ID's can enable adversaries to compromise a Crown Jewel Application?

Additionally, TrueFort Fortress can help clean up any inactive or unwanted Service ID's to help reduce the attack surface. It can also provide input into the policies required to manage and limit Service ID 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 Fortress distinguishes itself from other solutions in its use of machine learning and classifiers to profile and baseline normal Service ID behavior *within an application context*.** This approach not only accelerates the profiling and learning process (two weeks), 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 Fortress can detect Service ID behavioral anomalies. The detection of these anomalies can generate alerts at a minimum. However, alerts are the bare minimum to help take action. For full protection, **TrueFort Fortress goes further to deliver an automated response capability that immediately prevents the use of Service ID's that are behaving anomalously or maliciously**.

TRUEFORT FORTRESS | TOP 5 SOLUTION BENEFITS

Benefit #1 - Visibility

TrueFort Fortress 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 Fortress helps you see and understand the interaction between identities, usage patterns (including software executed) and applications. By profiling Users, Developers, System Accounts, and Sys 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 Fortress 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 Fortress 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 - Whitelisting

TrueFort Fortress can profile and white 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 Response is transformational. The speed with which either a human or bot can move and 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. This leaves them reactive, struggling to contain, let alone remediate.

You need to automate your response to prevent damage and you know you must do so safely. TrueFort Fortress can respond with precision in some of the most demanding environments. It leverages a library of automations to meet your requirements, including:

- Users (legitimate or APT) moving between business units or from development to production; Fortress 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, Fortress can terminate the session before the user even gets to the shell or into Windows
- A legitimate service ID logging in but performing tasks outside of the approved change process. Fortress can terminate the session but the forensic trail remains, enabling you to understand everything the user did
- If someone hijacks a process or runs a process out of the normal profile; Fortress captures the ID and terminates the process

TrueFort Fortress is able to respond to a wide variety of Service ID abuses, reducing your attack surface and enhancing data security.

TRUEFORT VALUE

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

TrueFort™ helps organizations align application security policy with operational reality via Fortress™, the application and cloud workload protection platform. Fortress reverses the traditional infrastructure approach to security by taking an application-centric approach: comprehensively tracking application behavior to unify cloud workload protection and AppSec in a single console. Using real-time telemetry, that leverages your existing security investments, patented advanced behavioral analytics and policy automation, your enterprise can now visualize, microsegment, protect, threat-hunt and investigate from the application layer.

Founded in 2015 by former Wall Street senior IT executives, TrueFort offers unparalleled application visibility, control, and detection with the shortest time-to-value through the TrueFort Fortified™ ecosystem and our unique bring-your-own-agent approach.

Contact Us Today
www.truefort.com
Tel: +1 201.766.2023
Email: sales@truefort.com