TRUEFORT FORTRESS™

Service ID Control

www.truefort.com

TRUEFORT

ABOUT TRUEFORT FORTRESS

TrueFort Fortress is a comprehensive, real-time application and cloud workload protection solution. Fortress 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, Fortress 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.

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

Any company that does not adequately manage Service IDs — 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

Managing the risks of uncontrolled Service IDs

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.

Because of this, Service IDs are often poorly managed with passwords for these IDs changing less often than User IDs. 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 IDs within the organization and the large volume of services running on a single ID.

Compounding this problem, access to IDs 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 IDs in a centralized manner, this approach assumes visibility into where and how your Service IDs are utilized. These risks are further compounded by old or orphaned IDs that predate any identity governance controls.

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

Top 5 Risks Related to Service IDs

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

TRUEFORT'S
APPLICATION-CENTRIC APPROACH

Security teams must take a different approach to unmanaged Service IDs

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

Fortress Service ID controls deliver:

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

VISIBILITY

Before you can control your Service IDs, 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 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 applications and can happen in real-time, well before a compromise has a chance to take root and create negative impacts on the business.

RISK POSTURE

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

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

Additionally, Fortress can help clean up any inactive or unwanted Service IDs to help reduce the attack surface. It can also provide input into the policies required to control 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. **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, 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, Fortress can detect Service ID 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 IDs that are behaving anomalously or maliciously**.

TOP 5 FORTRESS BENEFITS

Benefit #1 - Visibility

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

Fortress 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

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

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 – Allow-listing

Fortress can profile 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. Fortress can respond in real-time with mitigation precision across the most demanding environments. Fortress 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; 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 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, 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 FORTRESS VALUE

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