TRUEFORT

BRIEF

IMPROVE APPLICATION RISK POSTURE

BY LOCKING DOWN PRIVILEGED ADMIN & SERVICE ACCOUNTS

Fortress XDR™ helps reduce risk and uncover APTs by identifying, monitoring and enforcing access policy on privileged admin and service accounts.

PRIVILEGED ACCOUNT COMPROMISE IS THE GATEWAY TO BIG BREACH HEADLINES

It isn't news that privileged account compromise is a top insider threat and clear inroad for APTs 'living off the land'. But as illustrated by CSO Online[2] and the recent Marriott and GoDaddy breaches, the value of this target is higher than ever. Attackers are evolving their tactics by combining efforts like APTs with ransomware and theft of managed service provider credentials to increase their success rates - to the tune of $billions in damage.

So, what are you doing to secure these top compromise targets?

- **Do you know *how and where* your admin and service accounts are being used?**
- **Can you *ensure* these privileged accounts are not misused and exploited for other purposes?**
- **Can your Identity and Access Management (IAM) solution effectively *and efficiently* monitor and control these accounts?**

By their nature, trusted admin and service accounts should be secure as they are purpose-built and deployed with highly predetermined and predictable behavior.

Yet, despite millions invested in pen-testing, and complex cloud workload protection, application security and IAM platforms – control over them has remained elusive.

FORTRESS XDR PROTECTS APPS BY CONTROLLING ROGUE ACCOUNTS

We can help. Fortress XDR protects enterprise applications everywhere – **whether on-premises, in containers, or in the Cloud.**

It fully visualizes and understands apps in-production, including their dynamic behavior and context. See them in 4k resolution across all aspects, including their workloads, processes, scans, connections, configurations, and the time and **identities** of access and attack.

74%

Surveyed IT organizations claim breach due to privileged account abuse[1]

SOLUTION HIGHLIGHTS

- **Monitor & Inventory Accounts**
  Automatically find, report, and track account access, actions, and times, across app servers, containers and workloads.
- **Easily Create & Enforce Policy**
  Implement Zero Trust using the **principle-of-least-privilege** and whitelisted, app-level microsegmentation.[5]
- **Evict attackers 'off-the-land'**
  Use advanced behavioral analytics to alert on permitted, yet suspicious, executions outside of established norms.

WWW.TRUEFORT.COM

WHAT IT SOLVES & REPLACES

Once compromised, privileged accounts grant attackers full access to lateral movement, apps, systems, and critical data stores. They are dangerous threat vectors with long shelf-lives, poorly managed due to their proliferation, SLA-considerations, and tendency to fall through operational and technology gaps.

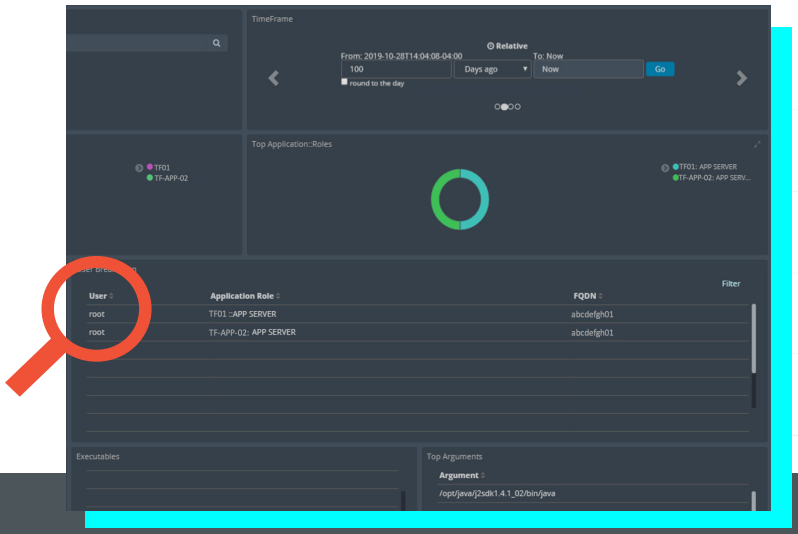
For example, IAM/PAM platforms focus on human accounts while InfraSec solutions lack the logical app context to effectively monitor them. As a result, attackers use these privileged accounts by stepping around basic policy triggers, reaching their targets.

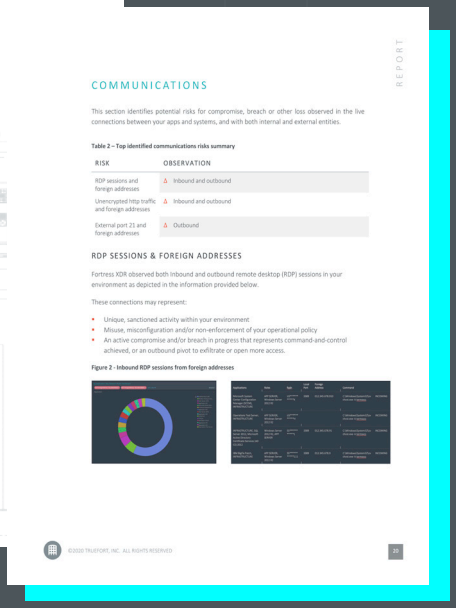
Fortress XDR uniquely closes the gap by **making it easy** to baseline, detect, monitor, create and enforce policy based on **what these accounts *do with your apps and systems***:

- **Clearly identify and track privileged accounts using XDR-based telemetry and advanced behavioral analytics that determine normal versus anomalous or rogue behavior.**
- **Control and ensure only whitelisted activity and access using automatically generated security and microsegmentation policy.**
- **Investigate, hunt, audit and report on account activity using data continuously collected over seconds, weeks, or years.**
- **Use a single pane-of-glass to monitor and control account policies at dramatically reduced operational time, effort, and cost.**

SOLUTION USE CASES

- **Improve Visibility & Posture**
  Support compliance and prevention by enforcing policy and stopping misuse, shadow IT, and clear text authentications.
- **Detect Compromise**
  Continuously monitor privileged accounts to block attacks *before* they breach.
- **Report & Remediate Breach**
  Use DVR playback across months or years to locate origin and avoid future account violations or compromise.





GET THE READ-OUT | APPLICATION RISK POSTURE REPORTS

Profile Your Production Apps within Their Business Logic Context

- App function and component roles
- Deployment characteristics
- Application dependency mapping
- Typical activity hours
- Typical connections

Audit & See the Gap Between Policy, Current State & Behavior

- Processes, executables and commands
- Ports, protocols and traffic
- Accounts and users
- Software and patches

Identify Top Risks in Your Unique Environment

- Vulnerable software and infrastructure
- Unmanaged accounts and unencrypted authentications
- Unencrypted and abnormal connections
- Unusual process execution
- Known attack indicators

HOW IT WORKS

Fortress XDR delivers value in each step of the journey. Begin by installing our virtual appliance, and importing and defining what you know about your business and its apps. Then connect agents, integrations and feeds. And within days or just hours, you **get insight into your admin and service accounts, whether default, local, or domain-based.**

Fortress XDR employs the standard appliance-sensor model, offering out-of-box integrations and full REST-API access.

Platform appliance. Delivered as software to be deployed anywhere Linux goes, including baremetal, virtual machines and cloud images. It is fully multi-tenant, scalable and highly available with a load-balancing, N+1 clustering option.

Reporter Module. For reporting on service accounts, we recommend deploying our Reporter module featuring preconfigured reports, ideal for admins, analysts, audits, or executives reviewing results.

Management console. Deploy, configure, protect, report and investigate all from a single pane of glass that offers configurable, role-based management.

Protect agent. (Optional) Our advanced, proprietary agent offers a light footprint and tracks over 150 parameters to continuously monitor, microsegment and protect. Compatible with legacy servers, virtual machines, cloud instances, PaaS and containerized environments.[5]

"advantange 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."[3]

– KuppingerCole

The below chart depicts TrueFort alignment with CIS, MITRE, and NIST. For more details about our solution and its support of industry frameworks, please contact **sales@truefort.com.**

SOLUTION FEATURES

- **Behavioral Analytics**
  Uses high performance tech based on Wall Street high frequency trading systems.
- **XDR *and* 5-Tuple+ Telemetry**
  Track account activity in full context across network, system, process, and time.
- **On-Premises *and* in Cloud**
  Monitor account activities and find orphans across your environments.
- **Detect *and* Respond**
  Go beyond a single assessment with continuous monitoring *and* enforcement.
- **Integrate in CI/CD Toolchain**
  Good risk posture begins before deployment.

FORTRESS XDR STARTS WITH INDUSTRY BEST PRACTICES AND THEN LETS YOU CUSTOMIZE MONITORING & POLICY ACCORDING TO YOUR UNIQUE REQUIREMENTS[5]

20 CIS CONTROLS®	MITRE ATT&CK®	NIST 800-53 [REV 4]
Continuous vulnerability management	T1068 - Exploitation for Privilege Escalation	AC-1 - Access Control Policy & Procedures
Controlled use of administrative privileges	T1078 - Valid Accounts	AC-2 - Account Management
Secure configuration for hardware & software on [...] servers	T1088 - Bypass User Account Control	AC-3 - Access Enforcement
Maintenance, monitoring & analysis of audit logs	T1098 - Account Manipulation	AC-5 - Separation of Duties
Controlled access based on need-to-know	T1108 - Redundant Access	AC-6 - Least Privilege
Account monitoring & control	T1131 - Authentication Package	AC-24 - Access Control Decisions
	T1136 - Account Creation	
	T1177 - LSASS Driver	
	T1182 - AppCert DLLs	
	T1199 - Trusted Connections	

BRIEF

TRUEFORT & THE FORTIFIED™ ECOSYSTEM

And remember – good data in, good data out. Power Fortress XDR with the telemetry you already collect, and let our platform fortify the value of security and operational investments you've already made.

Our partnerships span many categories, including network security, infrastructure and leading endpoint protection, detection and response vendors, so that you can immediately benefit from our bring-your-own-agent option.

We also work with industry standards organizations and offer open access to our fully REST-API driven platform to partners, providers and our customers through our Fortified program.

kubernetes · vmware · Microsoft · Pivotal · Fortinet Fabric-Ready · Infoblox NEXT LEVEL NETWORKING · vmware Carbon Black · CROWDSTRIKE · CIS Center for Internet Security®

SUPPORT

Companies offering highly available solutions to protect your business need to be highly available, too.

TrueFort customers receive 24x7 phone and email support, and all maintenance and software upgrades.

AVAILABILITY

TrueFort Fortress XDR is offered globally as a software subscription. It is licensed per endpoint, workload or containerized environment, and whether you choose our TrueFort Protect agent or bring-your-own-agent.

To learn more, request a briefing and a demo. Then experience it for yourself with a proof-of-value.

ABOUT TRUEFORT

Applications are the lifeblood of business. TrueFort™ helps organizations align application security policy with operational reality via Fortress™ XDR, the industry's first application detection and response platform.

Fortress XDR reverses the traditional infrastructure approach to security by comprehensively tracking application behavior to unify cloud workload protection and AppSec in a single console. Using real-time telemetry, patented advanced behavioral analytics and policy automation, enterprises can now visualize, microsegment, protect, hunt and investigate from the application layer.

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

For more info visit www.truefort.com and follow us on Twitter and LinkedIn.

RECOGNITION

Network Products Guide IT World Awards 2019 SILVER · computing Security Excellence Awards 2019 · OSPA FINALIST 2019 · The Channel Co. CRN TECH INNOVATORS FINALIST 2019 · TAG CYBER 2020 DISTINGUISHED VENDOR

GET FORTIFIED

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

+1 201 766 2023

sales@truefort.com

WWW.TRUEFORT.COM

[1]Forbes | 74% of Data Breaches Start With Privileged Credential Abuse | Feb 2019 | Louis Columbus

[2]CSO Online | More targeted, sophisticated, and costly: Why ransomware might be your biggest threat | June 2019 | Lucian Constantin

[3]KuppingerCole | KuppingerCole Report: Executive View -TrueFort Fortress XDR | Nov 2019 | Alexei Balanganski

[4]Center for Internet Security | The 20 CIS Controls & Resources, MITRE | Enterprise Techniques NIST | NIST Special Publication 800-53 (Rev. 4)

[5]Feature support varies when in "bring-your-own-agent" mode according to the capabilities of the third-party agent deployed on the workload, and its integration with the Fortress XDR platform.

TF-SB-SVCACCTS-1.1-0520