TRUEFORT

TRUEFORT FORTRESS XDR™

APPLICATION DETECTION & RESPONSE PLATFORM

Industry-first platform unlocks the unparalleled insight, control, and protection needed to secure what matters most

ARE YOUR BUSINESS-CRITICAL APPLICATIONS SECURE?

Each year enterprise IT and security organizations spend millions trying to effectively manage and secure their applications and data. Yet breaches still succeed from evasive attacks and insider threats.

And when asked, most security teams can't answer basic questions:

? **Are your applications a target, vulnerable, under attack or already compromised?**

? **Do you know where your apps are running and is your CMDB accurate?**

? **Does your security policy align with your business operational policy and could you deliver a GDPR notice within just 72 hours?**

Today, most organizations go to a collection of tools and siloed teams in attempt to close these gaps. They scan code, secure workload connections and reverse-engineer the app-map using 'app-centric' solutions they've implemented. And even when a war room is assembled, it is impeded through volumes of disconnected data.

So, many tools and agent-installations later, organizations still fail to secure their apps and answer rudimentary questions.

FORTRESS XDR SECURES APPLICATIONS & THEIR CLOUD WORKLOADS

We can help. Fortress XDR protects enterprise applications everywhere – whether on-premises or in the Cloud. It helps you fully visualize and understand them in-production – their dynamic behavior and context across all aspects including code, infrastructure, connections, configuration and the time and identities of access and attack.

SOLUTIONS

🔒 SECURITY

- Continuously monitor apps and detect anomalies & vulnerabilities
- Protect, alert & respond in real-time with automation
- Hunt threats & investigate incidents forensically
- Automate security policies & microsegmentation

👁 OPERATIONS

- Visualize applications, dependencies & flows
- Update CMDBs with live insight
- Integrate security into the entire SDLC and CI/CD toolchain

☢ RISK & COMPLIANCE

- Report state-of-union
- Capture and analyze forensic data
- Enable regulatory compliance
- Support hardening, configuration and vulnerability assessment with CIS™ benchmarks and FIM

WWW.TRUEFORT.COM

FORTRESS XDR IS THE NEW APPROACH TO CLOUD WORKLOAD PROTECTION

Our XDR approach pulls static and real-time operational, AppSec and InfraSec data into a single console for analysis by our advanced behavioral analytics engine, helping you:

- Understand the full application environment whether in the data center, Cloud or containers.
- Detect anomalies and execution events other solutions miss while dramatically reducing time-to-detection and response.
- Benefit from the shortest time-to-value through our policy automation and a unique 'bring-your-own-agent' option.
- Be prepared to provide real answers to questions about the life and health of your apps.

The only solution that protects applications from and through the application lens.

VISUALIZE + MAP
Clearly see applications, their components, and relationships using real-time and historical data

PROFILE + DETECT
Continuously learn and monitor app behavior, find anomalies & auto-gen policy and microsegmentation

PROTECT + RESPOND
Enforce, investigate and respond to zero-day & application events with unparalleled depth & clarity

WHAT'S NEW IN 3.X

Version 3.x introduces our new XDR platform approach and the following features:

- **Secure containerized applications via Kubernetes and the Istio standard**. Deploy the TrueFort Protect agent as a DaemonSet to a Kubernetes node to continuously collect telemetry, visualize, monitor and secure orchestrated environments.
- **Forensics-on-the-fly with the new Reporter module.** Deploy appliances dedicated to storing and managing the same level of breadth, depth and DVR-playback across weeks, months or even years – to dashboard, report, conduct investigations or serve up evidentiary support on-demand.
- **Secure apps on legacy hosts**. Version 3.x extends support for applications running on older systems, including Microsoft Windows® 2003.

FEATURES

VISIBILITY
- **Seven-Tuple Telemetry**
  Profile and baseline at app, workload, operating system, network, process, identity and time levels.

POLICY
- **Security & Microsegmentation**
  Auto-generate app-oriented policies that are centrally managed and locally enforced.

DETECTION
- **Block Lateral Attacks**
  See what's invisible to perimeter firewalls and other infrasec solutions.
- **Breach & Anomaly Detection**
  Pre-built analytics identify deviations including unauthorized software, process checksums and runtime states.

RESPONSE
- **Active Protection**
  Stop Zero-Day, APTs & exfiltration in real-time with workflow-driven response to unauthorized connections, processes, users, and software.
- **Forensics-on-the-Fly**
  Real-time data stored at your fingertips for review, reporting and historical playback – your own flight recorder.

FORTRESS XDR FORTIFIES DETECTION RATES

Prevent unusual network activity and exfiltration attempts
- Lateral movement.
- App access outside of operating windows.
- Change in application flows.
- Logins from unknown sources and malicious networks.
- New systems joining an application.
- Unexpected interactive sessions like FTP, SSH, SCP, etc.

Stop privileged account abuse and escalation
- Interactive or unknown source usage of service accounts.
- Lateral movement with multiple identities.
- Unauthorized identities.
- Privileged account activity outside of known or authorized use.
- Processes run by unauthorized users.

Find unusual process and system activity
- New/different processes on known ports.
- New processes outside of expected behavior.
- Nmap, Metasploit and other malicious tools.
- New processes spawning connections out of application profile.
- Process hollowing via runtime changes to hash file systems mounted on unauthorized host.

PLATFORM

The TrueFort Fortress XDR platform employs the standard appliance-sensor model and is designed for enterprise-grade flexibility in deployment and modularity.

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. (Optional) Featuring out-of-box preconfigured reports, ideal for analysts conducting investigations 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 115 parameters to continuously monitor, microsegment and protect. Compatible with legacy servers, virtual machines, cloud instances, PaaS and containerized environments, TrueFort Protect goes anywhere your apps go.
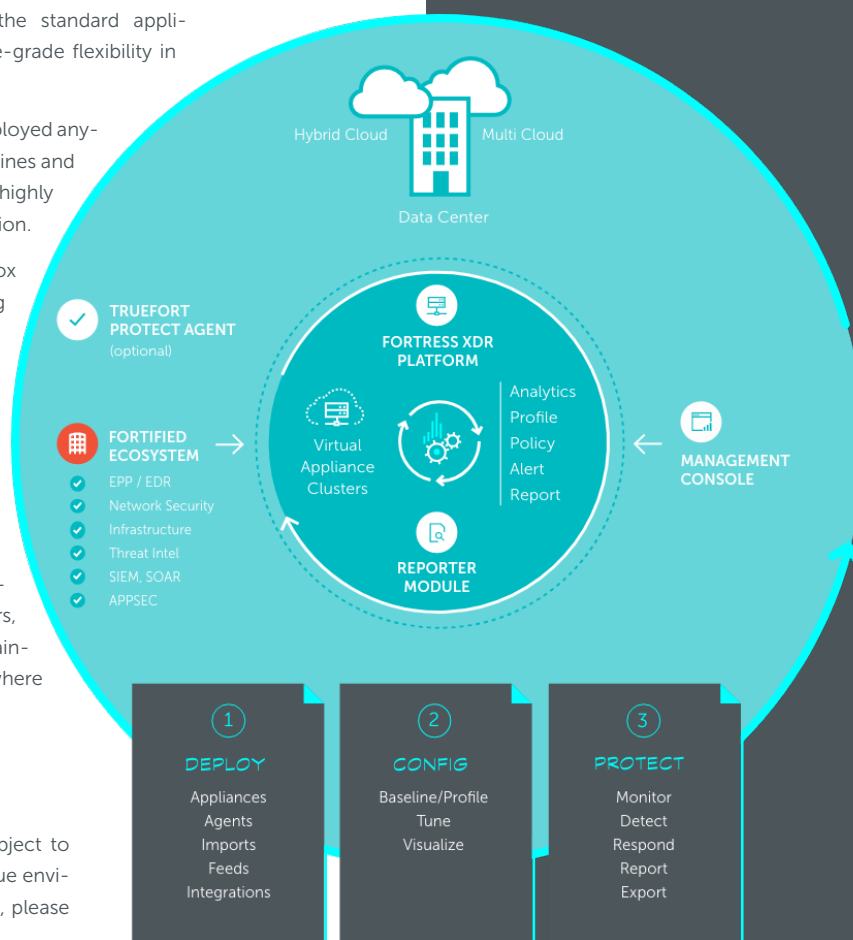
SPECIFICATIONS

The below minimum configuration details are subject to change. Your configuration depends on your unique environment and requirements. For more information, please consult our documentation or **sales@truefort.com**

Hybrid Cloud   Multi Cloud

Data Center

TRUEFORT PROTECT AGENT (optional)

FORTIFIED ECOSYSTEM
- EPP / EDR
- Network Security
- Infrastructure
- Threat Intel
- SIEM, SOAR
- APPSEC

FORTRESS XDR PLATFORM

Virtual Appliance Clusters

Analytics
Profile
Policy
Alert
Report

REPORTER MODULE

MANAGEMENT CONSOLE

1 DEPLOY
Appliances
Agents
Imports
Feeds
Integrations

2 CONFIG
Baseline/Profile
Tune
Visualize

3 PROTECT
Monitor
Detect
Respond
Report
Export

	COMPUTE	STORAGE	SOFTWARE
PLATFORM APPLIANCE	■ Dual Intel® Xeon® E5-2687W v4 3Ghz ■ 12 cores ■ 8x 16GB RDIMM@128 GB	■ 7 X 50GB SSD ■ 6Gbps 2.5" @ 1 drive/partition each	■ RedHat® RHEL 7.2 + ■ CentOS 7.2 +
REPORTER APPLIANCE (Optional)	■ Intel® Xeon® CPU E5-2663 v3 @ 2.80GHz ■ 8 Cores ■ 96GB RAM	50GB SSD	■ RedHat® RHEL 7.2 + ■ CentOS 7.2 +
PROTECT AGENT (Optional)		**Windows** Java: 350MB Go: 100MB **Linux** 100MB	■ Kubernetes & Istio ■ Microsoft® Windows® Server 2003 + ■ Ubuntu® 16 + ■ SUSE® 11 + ■ RedHat RHEL & CentOS 6 + ■ Oracle Linux 6+
WEB CONSOLE			■ Google Chrome® ■ Mozilla Firefox™

TRUEFORT FORTIFIED ECOSYSTEM

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

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

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

SUPPORT

Companies offering highly available solutions to protect your business need to be highly available, too. TrueFort customers automatically 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 and/or bring-your-own.

Contact us and let us prove it. Request a briefing and a demo. Then experience it for yourself with a proof-of-value.

RECOGNITION

GET FORTIFIED

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 information visit www.truefort.com and follow us on Twitter and LinkedIn.

HEADQUARTERS

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

+1 201 766 2023

sales@truefort.com

WWW.TRUEFORT.COM