TRUEFORT

BRIEF

SECURITY AND COMPLIANCE FOR CLOUD-NATIVE APPLICATIONS

USE FORTRESS TO SECURE CLOUD (KUBERNETES,CAAS & PAAS)

Fortress and Kubernetes – secure the assets and applications that are transforming your digital business.

Kubernetes (K8s) environments have become an important platform for building critical applications and it is impossible to secure using traditional methods and tools. The speed at which change occurs in these applications is part of the challenge, further complicated because they are operated by DevOps engineers who are busy rewriting change management controls.

Securing cloud-native applications and achieving compliance demands that security teams look at their role through a new lens, modernize their processes and tooling to deliver engaging user experience at digital-velocity while mitigating different risks.

Don't Allow Kubernetes Security to Become the Next Silo

Even cloud-native applications do not run entirely on K8s; they integrate with your existing data services, authentication, and more - leaving a new attack surface for perpetrators to sneak through. WAF and RASP may be a good first line of defense, but are leaky and once breached, threat actors have the keys to your data, intellectual property - your business.

K8s introduces complexity at the same time that security is being forced to accelerate and modernize controls. ITIL hinders your digital transformation and cloud journey – DevSecOps removes friction!

You Need Security That Will Work at the Speed of Dev Ops

K8s, the cloud, or any CaaS/PaaS demands that your security solution monitors both the control-plane and the data-plane. 'Real-time' is essential since applications change dynamically and anyone, or anything, with the access keys can make a change (human, robot, hacker).

The Kubernetes ecosystem is immature and security is evolving rapidly.

Fortress has the REAL-TIME ADVANCED VISIBILITY, ANALYTICS AUTOMATION AND CONTROL to create, deploy and maintain policies in dynamic compute environments.

TrueFort is platform agnostic, ensuring you are protected. You will find K8s in your environment, either in the data center or from a host of public cloud providers. Your public cloud provider may assure you that their deployment is up to date, but they do not insure you for vulnerabilities in your code, network configuration or any of the many management offerings that exist (AKE,GKE, EKS, OpenShift, Tanzu). And you cannot insert a firewall in a public cloud, so access & egress must be software-defined. This is a security nightmare for all organizations.

84%

Percentage of organizations running containers in their environment.
Over 50% have more than 250 containers.

SOLUTION HIGHLIGHTS

- **From the Cloud to the Ground**
  Comprehensive Security, visualizations, and automation across the entire application – not just K8s, but all services that comprise the application, whether running on bare metal, VM, container, in the data center or cloud.
- **Not in the Container & not a Sidecar**
  Fortress uses a DaemonSet to ensure 100% application and infrastructure coverage without slowing deployment, degrading performance, or impacting developers.
- **Deploy Controls with Workloads**
  Leverage development artefacts as policy; security-as-code.
- **Closed-loop policy automation (Plan, Do, Check, Act)**
  Deploy policy, controls, and automation as an integral part of product release. API-enabled security protecting the application the toolchain, orchestrator, runtime, and container.
- **Integrated Service Mesh (Istio) Controls and Traffic Management**
  Visualize traffic flows & compliance for automated policy generation & deployment.

WWW.TRUEFORT.COM

SHIFT-LEFT with Fortress + Kubernetes

The ability to deploy and refactor cloud-native applications has turbocharged developers and business. Security used to be able to keep up - when deployments took months and when security was the gatekeeper. Now, with development powered by K8s, changes take seconds to deploy and security is unfamiliar with this new release process. They need help keeping up.

To maintain posture, security tooling must be frictionless and automatically deployed with the application and changes, so that security is ON the instant the application comes online. Security must also shift-left by enabling good practices to be implemented and measured without downstream effort; compliant by design, enforced by policy.

Kubernetes is often used as a front end for existing systems to deliver the UI or present an API. These new 'apps' connect to traditional services for state, data, authentication and pretty much everything else that makes them useful. This presents opportunities for threat actors to find vulnerabilities and 'Live off the land'.

Using agents or monitoring net flow within a closed K8s ecosystem is not the way to go. Application behavior is the only effective approach to detecting an attack. TrueFort presents a simple method to enforce policy, integrated with the Service Mesh. Fortress works in real-time to respond to a detected anomaly in order to control traffic, processes, and other behaviors . This is the only way to stop the attackers.

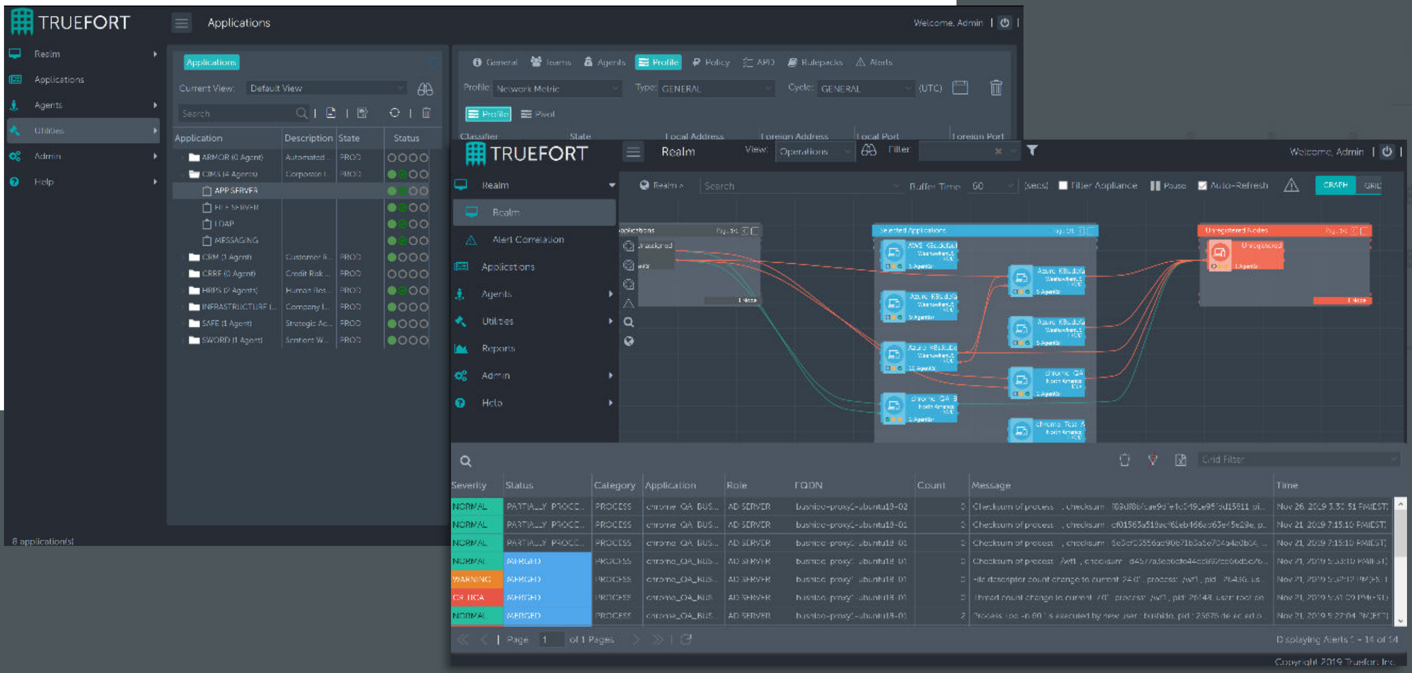
Teams now have THE ULTIMATE DEVSECOPS PLATFORM for making operational decisions. A single source of truth with out-of-the-box automation and granular policy creation.

Even with extensive dynamic (DAST) and static code analysis (SAST), applications remain vulnerable. These are critical components to reduce the attack surface, but the application security posture will grow stale (technical debt). Applications now include OSS, images from public repos and container registries, all contributing to riskier security posture. Monitoring anomalous activity and having the real-time controls in-place to prevent deviant behavior is essential

Even if you only use public cloud, you are working in a shared responsibility model. Your public cloud provider does not assure your application. If you consume K8s as a service; you must protect yourself.

FORTRESS CAPABILITIES

- The power to visualize the entire app and data flows is critical – you can't manage what you can't measure.
- New applications are automatically identified, visualized, and monitored as they are provisioned, and auto-protected for scale-out, scale down & deprecation, without process overhead, security as code.
- Fortress learns complex network and process behavior and codifies it so security can define policy & development can deploy it through the CICD pipeline. Continuous improvement through iteration.
- DAST/SAST and IDS do not guarantee security. You must be able to detect ransomware, illicit service account use and many other behavioral anomalies.
- Containers are designed to run a single process and be immutable. Guarantee your image is safe, secure, and unchanged from the moment it was provisioned.
- Fortress enables collaboration and greatly accelerates incident response and threat hunting with high-fidelity alerting and forensics including DVR replay capabilities.
- Security teams can immediately respond to policy violations and configure response workflows for different anomalous activity.
- Fortress provides out-of-the-box policy for compliance standards including CIS/PCI.



Current View: Default View

Application	Description	State	Status
ARMOR (0 Agent)	Automated ...	PROD	○○○○
CIMS (4 Agents)	Corporate I...	PROD	●●○○
APP SERVER			●●○○
FILE SERVER			●●○○
LDAP			●●○○
MESSAGING			●●○○
CRM (1 Agent)	Customer R...	PROD	●○○○
CRRF (0 Agent)	Credit Risk ...	PROD	○○○○
HRPS (2 Agents)	Human Res...	PROD	●●○○
INFRASTRUCTURE (...	Company I...	PROD	●○○○
SAFE (1 Agent)	Strategic Ac...	PROD	●○○○
SWORD (1 Agent)	Sentient W...	PROD	●○○○

8 application(s)

Profile: Network Metric   Type: GENERAL   Cycle: GENERAL   (UTC)

View: Operations   Filter   Buffer Time: 60 (secs)   Filter Appliance   Pause   Auto-Refresh

Severity	Status	Category	Application	Role	FQDN	Count	Message	Time
NORMAL	PARTIALLY_PROCE...	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy2-ubuntu19-02	0	Checksum of process , checksum : f83df8b/cae9d'efc049ce95'dd15811 pi...	Nov 26, 2019 3:30:51 PM(EST)
NORMAL	PARTIALLY_PROCE...	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy2-ubuntu19-01	0	Checksum of process , checksum : cf01563a519ac61eb166ab63e45e29e, p...	Nov 21, 2019 7:15:10 PM(EST)
NORMAL	PARTIALLY_PROCE...	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy2-ubuntu18-01	0	Checksum of process , checksum : 5e3cf03556ad90b71b3a5e704a4e0b04, ...	Nov 21, 2019 7:15:10 PM(EST)
NORMAL	MERGED	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy1-ubuntu18-01	0	Checksum of process /wf1 , checksum : d4577a5eb0cfe44ad892cc6dbc26...	Nov 21, 2019 5:53:10 PM(EST)
WARNING	MERGED	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy1-ubuntu18-01	0	File descriptor count change to current 24.0 , process /wf1 , pid : 26430, us...	Nov 21, 2019 5:32:12 PM(EST)
CRITICAL	MERGED	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy1-ubuntu18-01	0	Thread count change to current 7.0 , process /wf1 , pid 26148, user root se...	Nov 21, 2019 5:31:09 PM(EST)
NORMAL	MERGED	PROCESS	chrome_QA_BUS...	AD SERVER	bushido-proxy1-ubuntu18-01	2	Process /os -n 60 is executed by new user : bushido, pid : 25676 detected o...	Nov 21, 2019 5:27:04 PM(EST)

Page 1 of 1 Pages

Displaying Alerts 1 - 14 of 14

Copyright 2019 Truefort Inc.

HOW IT WORKS

Fortress :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. Fortress employs the standard appliance-sensor model, offering out-of-box integrations and full REST-API access. Connect integrations your agents, integrations, and feeds. This will provide immediate values and significant insight into the current state and vulnerabilities of your apps before you even start baselining.

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

Reporter Module. For risk posture management, we recommend deploying our optional Reporter module featuring out-of-box preconfigured reports. Ideal for analysts, threat hunters, incident response 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.

> "full visibility into business-critical applications and quick threat detection … enables automated, proactive tuning of existing security policies, blocking malicious activities before they even occur."
>
> – KuppingerCole

The below chart shows how Fortress supports common security frameworks as well as understanding the application environment and supporting migrations. For more information about how our solution works and supports securing your critical applications, please contact sales@truefort.com.

SOLUTION FEATURES

- Behavioral Analytics
  Uses high performance and volume tech based on Wall Street high frequency trading systems.
- XDR and with Detailed Telemetry
  Enrich with data you own, and go beyond network with process, identity, and time.
- On Premise and in the Cloud
  Maintain app risk posture across your enterprise.
- Accelerate Investigation/Response
  Reduce forensic investigation costs of cyber-incidents, streamline compliance and gain historical playback capabilities.
- Integrate in CI/CD Toolchain
  Good risk posture begins before deployment

FORTRESS SUPPORTS YOU IN

CLOUD MIGRATION

AS YOU ASSESS THE LANDSCAPE,

DETERMINE STRATEGY,

... AND EXECUTE YOUR PLAN.

CSA EGREGIOUS 11

- Data breaches
- Misconfig & inadequate change control
- Lack of cloud security architecture and strategy
- Insufficient identity & key management
- Account hijacking
- Insider threat
- Insecure interfaces & APIs
- Weak control plane
- Meta- & applistructure failures
- Limited usage visibility
- Abuse/nefarious use

MITRE ECAF

- Establish security tolerance
- Know threat environment
- Perform risk analysis, select controls
- Know vendor security & privacy capabilities
- Update policies, define architecture
- Develop > assess security & privacy measures
- Perform risk management
- Manage migration security risks

FORTRESS

- Inventory apps with detailed visibility into network relationships tied back to process, and identity,
- Understand outage dependencies, metadata, vulnerabilities, drift and more.
- Migration support - Baseline applications, assess and configure behavior and policy.
- Update configuration and security policy to new environment
- Compare model-driven design to deployment
- Perform continuous monitoring for new operational and security anomalies.

TRUEFORT & THE FORTIFIED™ ECOSYSTEM

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

Infoblox NEXT LEVEL NETWORKING FORTINET Fabric-Ready

Pivotal CROWDSTRIKE

vmware Carbon Black 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.

RECOGNITION

TAG CYBER 2020 DISTINGUISHED VENDOR

TE 50 2020 WINNER

CROWDSTRIKE Store Partner of the Year

AVAILABILITY

TrueFort Fortress 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-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™, the industry's first application detection and response platform.

Fortress 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.

3 West 18th Street
Weehawken, NJ 07086
United States of America
+1 201 766 2023

sales@truefort.com

TRUEFORT