TRUEFORT

CLOUD WORKLOADS & FORTRESS
FULL-STACK CLOUD WORKLOAD PROTECTION

Fortress for Cloud Workload Protection

Workload-centric security, world-class, real time visibility and analytics target the unique requirements of workloads across multi-cloud, hybrid, and data centers.

Key Application and Data Protection Requirements for CWPP

Workloads (any unit of back-end computational work - bare metal, VM, container) today are increasingly diverse and distributed with services running on-premises and in the public cloud. The percentage of workloads running on-premises is shrinking. By design, enterprises are using multiple IaaS and PaaS providers. Most enterprises now have new-build, migration and refactoring projects in development, pilot, or production. The workloads are moving to microservices and with the adoption of containers and functions, continuous delivery infrastructure becomes ephemeral and immutable. This means shorter life spans for these workloads. As a result, overall complexity is compounding at an unmanageable rate as enterprises adopt this hybrid, multi-cloud architecture. Security just cannot keep up.

The increasing shift to DevOps development patterns for organizations creates a need for solutions that can meet the requirements of dynamic, hybrid, multi-cloud workloads. Cloud-native applications utilize a combination of virtual machines (VMs), containers, and serverless PaaS to deliver an application service – often connecting to legacy systems and environments. The cloud-native containers and serverless workloads that run these applications come and go quickly and need to be secure from the moment of instantiation.

Cloud workload risk demands a solution that:

- Provides consistent visibility and control of all workloads, regardless of location or size.
- Replaces antivirus-centric strategies with a "zero-trust execution" real-time application control approach, even if used only in detection mode.
- Exposes all functions via API.
- Extends workload scanning and compliance into development (DevSecOps) especially with container-based and serverless function PaaS-based deployments.
- Requires CWPP vendors to support containers or serverless architectures. .
- Architect for scenarios where runtime CWPP agents cannot be used or no longer make sense.
- Start securing workloads proactively in development , so that they are "born" protected.

Fortress provides consistent visibility and control for all workloads, regardless of location , including physical machines, virtual machines, containers and serverless workloads. It assesses system configuration, compliance, and vulnerability status from the "inside out", and supports creating application control/whitelisting models in development, before the workloads are deployed into production. Additionally, it can control application and lockdown containers at runtime (zero trust). Specific policy recommendations are provided for workload hardening based on the workload's role.

70%

Gartner – Through 2020, due to the immaturity of incumbent CWPP offerings, 70% of organizations will use a different CWPP offering for container and serverless protection than they use for virtual machine protection.[1]

The Cloud Workload Landscape

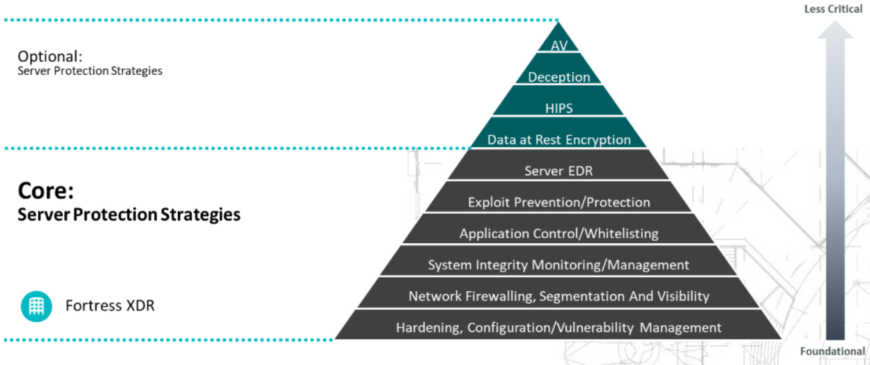
- Requirements for securing virtual machine, container and serverless workloads in public and private clouds are evolving rapidly, your security platform must evolve as well to maintain protection and reduce risk.
- Cloud workloads change frequently and are often reprovisioned, scaled and deprecated through CICD automation. Your CWPP solution must be integrated into the toolchain and updated dynamically.

CWPP Controls, Layer by Layer

- Hardening, configuration, and vulnerability management
- Network firewalling, Visibility and Micro-segmentation
- System Integrity Assurance
- Application control/Whitelisting
- Exploitation prevention/Memory protection
- Server workload EDR, behavioral monitoring, and threat detection/response
- Host-based IPS with vulnerability shielding
- Anti-malware scanning

Unprecedented Cloud Work Protection

Only Fortress provides comprehensive, real-time cloud workload protection out of the box. It can provide all of the Core server protection strategies, and leverage TrueFort Ecosystem partners to extend capabilities to cover the Optional strategies as well.


Less Critical
Optional:
Server Protection Strategies
AV
Deception
HIPS
Data at Rest Encryption
Core:
Server Protection Strategies
Server EDR
Exploit Prevention/Protection
Application Control/Whitelisting
System Integrity Monitoring/Management
Fortress XDR
Network Firewalling, Segmentation And Visibility
Hardening, Configuration/Vulnerability Management
Foundational

Source: Gartner, Market Guide for Cloud Workload Protection Platforms, Neil MacDonald, March 26th, 2018

Hardening, Configuration, and Vulnerability Management – Evaluate workloads against CIS or custom Linux, Windows, AIX, and Solaris benchmarks. Fortress protects your system utilities, secrets, and configurations to ensure optimal security and guard against drift.

Network Firewalling, Visibility and Micro- Segmentation - Leverage machine learning to understand network behavior for every workload and intelligently generate segmentation policies. Fortress utilizes a cryptographic reference – not IP – to identify each workload, allowing for real-time management in dynamic environments. The Fortress platform supports two types of segmentation controls:

- Static Policy: A machine-learned or user-defined policy creates a whitelist for network relationships. Apply policies to a workload's native firewall via the TrueFort Agent or a supported third-party agent (CrowdStrike, etc.), or push them to SDN for enforcement (VMware NSX or Fortinet Fabric).
- Dynamic Segmentation: Fortress evaluates every connection in real-time and actively controls access. Connections can be managed granularly to ensure that the right relationships between network, process, and identity are maintained at the approved times.

System Integrity Assurance - Monitor critical system files, registry, and configuration at runtime to ensure workload integrity in real time. Address anomalous behavior related to misconfiguration when it happens by terminating it at the network or process layer, protecting the workload.

Application Control/Whitelisting – Use Fortress core real-time detection and response capabilities to build behavioral whitelists and define what is normal. This is in-line with the micro-services model. Leverage automation or integration with the CI/CD pipeline to generate whitelists for the following behaviors:

- Network - connections, protocols, data transfers all with context of source and destination, identity, software processes, inter-process, and inter-application.
- Software - installed and executed with context of location, checksum values, inter-process relationship, arguments passed and identity.
- Identity - with context of authentication (centralized or local), software usage, timings, location, data transferred and access patterns.
- Systems - hardware, OS, network address and routes, systems performance, and usage.

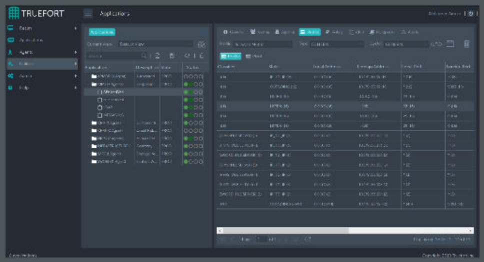
This quickly moves applications toward a zero-trust framework. Any execution outside the whitelist is detected in real-time and the rules-based response can block the anomalous behavior. Fully API enabled both upstream and downstream, Fortress readily integrates with existing tools and process.

Exploit Prevention/Memory Protection – With Fortress comprehensive process data is acquired and baselined to guarantee that only the 'expected' code is executed. All software is inspected and baselined enabling identification of CVE's and obsolete software from one authoritative source. Any change in the software will alert, including the renaming of binaries. This enables the ability to block malicious code, even trojans or code which has been hijacked to prevent the execution of vulnerable software.

Server Workload ADR – Understand behavior across your entire application environment – from legacy to cloud platforms. Fortress accomplishes this by machine learning good known behaviors, establishing a whitelist, and comparing telemetry against it – even pulling data from multiple sources outside the TrueFort Agent, including third-party agents (CrowdStrike, Tanium, etc.), network devices, AD/LDAP sources, load balancers, and PaaS orchestration layers. This enables the monitoring of network, processes, identities, log entries, and file access for behavior patterns that indicate malicious activity in the context of your applications.

Adoption of CWPP Strategies

- A Single Platform for container, serverless, virtual machine and legacy environment is essential to protect the environment and reduce risk.
- Workloads are being moved from on-premises to the public cloud due to the shift to cloud-native development using container-based application architecture, microservices - based applications and the adoption of serverless PaaS.
- In public cloud IaaS, workload-centric host-based CWPP solutions provide an easier architectural option for enforcing security policy than in traditional in-line network-based security controls.
- Workload-based offerings automatically scale out and back as the number of workloads increase and decrease.
- Using a DaemonSet or agentless approach to monitoring ensures limits the impact and reduces bottlenecking on cloud-based applications. This is especially true for inspecting traffic that moves laterally east/west from service to service in microservices-based architectures.
- This level of security requires new CWPP capabilities both in development and at runtime. Cloud-native apps require solutions designed to address the protection requirements of cloud-based systems.



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.

> "without understanding the logic, behavior, and business risks of corporate applications, even the most detailed analysis of network flows between them will never help an analyst to properly assess the risks."

TrueFort 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.

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.

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.

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

[1] How to Make Cloud More Secure Than Your Own Data Center | MacDonald & Crow, Gartner, Oct 2019
[2] Four Main Types of Cyberattack That Affect Data Center Uptime | DataCenter Knowledge, June 2019
[3] KuppingerCole Report: Executive Overview -TrueFort Fortress XDR | KuppingerCole, Nov 2019
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.