TRUEFORT

BRIEF

CLOUD SECURITY WITH FORTRESS
CLOUD VISIBILITY DELIVERED

Even though “Cloud” means someone else’s computer, it is still your security problem. Get control with Fortress .

Security is in the Dark when it Comes to Cloud.

Cloud-based applications and services are riddled with opportunities for Shadow IT to run rampant. It is not uncommon to hear of departments hiring their own IT staff, purchasing their own servers, or even developing software themselves without knowledge, buy in, or supervision from the IT department – building up independent IT resources to meet specific or urgent requirements. The security implications of these activities are significant, and the damage can be seen in the news every day. This cannot be allowed to continue!

Fortress has been designed to help security teams rapidly come up to speed with the complexities of enterprise hybrid and multi-cloud deployments, to improve security posture, and securely deploy to the cloud. With agentless support for AWS, Azure and GCP, TrueFort makes it simple to connect and go!

Speed and Complexity

Many enterprises leverage the cloud to quickly grow and scale. However, organizations are now starting to realize that moving to the cloud comes with a price - it adds a significant amount of risk and complexity. The cloud adds a whole operational methodology and widens the divide between developers, the business, & security. New concepts from an AWS perspective alone range from AMI’s to Security Groups, Direct Connect, EC2, and Lambda. Hundreds of unique services and overlays are constantly being added and implemented, making it difficult for even the most informed and diligent security teams to keep up.

> Cloud Visibility in a dynamic and multi-cloud environment is easy with Fortress Agentless Telemetry quickly enables visibility across all your environments.

To add to that, the cloud moves fast ,giving business many advantages, but also creating many security challenges. Developers push code whenever they want, without a change window. Applications scale unchecked based on workload and consumption requirements. User experience testing happens in production. Most importantly - no one is consults with the security teams, who may be viewed as overly cautious.

Hackers are well aware of the opportunities that these behaviors create, and the evidence is that AWS S3 buckets are being compromised, ransomware is taking down businesses, and personal data is being stolen en masse.”. To combat against these challenges, your security and visualization platform needs to be immediate and intelligent. It must be able to provide valuable telemetry from all your environments, from the cloud to the ground, and it must provide the tools and automation to make it easy to enable security and reduce risk.

Collaboration is the Key

Fortress enables the kind of collaboration needed to unify SecOps, DevOps, and Infrastructure. It leverages real-time data from multiple sources (including native cloud telemetry) automation and analytics to provide simple visualizations to easily gain understand and insight into the environment and simplify communication between the teams. Visualize your workloads enriched with contextual information about region, application, time, network overlay, consumed services, and normal behavior. Create policies that not only secure, but support portability and migration. Understand network, process, identity, software, and configuration in the context of application and time. . With Fortress Security can now provide increased value by acting as consultants and advisors - supporting digital transformation efforts and increasing their ability to protect.

70%

The percentage of businesses using public cloud services. Cloud security has passed the tipping point.

SOLUTION HIGHLIGHTS

- AGENTLESS

  Native Cloud Telemetry

  Plug-in and go to your Clouds network telemetry from AWS, Azure and GCP.

- BYOA - EDR

  Leverage Existing Tools

  Leverage existing investment in EDR tools (CrowdStrike, Tanium, etc.) to accelerate your deployment, provide immediate visibility, and support enforcement.

- TRUEFORT AGENT

  Real-Time Network Visibility

  Identify workloads and internal and external connections and dependencies from the cloud to the ground. Close the gaps across host, security group and VPC. Gain full historical visibility with DVR replay capabilities.

  Real-Time Process Visibility

  Continuous monitoring using behavioral baselines to detect and block anomalous behavior in real time.

  Identity

  Identify who logged in, from where, using which credentials and what they are doing – now and historically.

Securing the Whole Environment

The cloud presents its own set of challenges. Everything is abstracted, often multiple times. Being able to recognize an obsolete AMI, a poorly configured Security Group, unexpected consumption in a foreign region or zone, or the use of a cloud database such as RDS or a serverless function is essential. These are the building blocks of modern applications. Being able to reconcile this with the relationship and risk back to your on-premises systems demands considerable expertise and skill. To make matters worse, this list of challenges is changing all the time.

The Right Insight to Help Security

Fortress ingests and analyzes native cloud telemetry, automatically building an application-centric behavioral profile that spans network, process, and identity metrics in the context of time and location. This contextual information is critical to policy creation and application risk reduction – allowing genuine insight into real application behavior. For example, when you scale back infrastructure to reduce consumption and cost, Fortress evaluates whether this is normal behavior based on the time that this occurred, If not, XDR can alert on or block behaviors in real time if they are evaluated as out-of-profile.

While leveraging native cloud telemetry removes barriers and provides visibility without effort, it is only the start. For more advanced use cases such as automated response and workload controls, you have the option to deploy the TrueFort agent directly to your EC2 instances. This model ensures 100% application coverage from the start and can even broaden and deepen support as you progress. In addition, since applications are pushed at-will by developers, it is important to integrate into the toolchain to understand when thing s are happening, and ease adoption and application on-boarding.

Leverage application-centric visibility to:

- Visibility across all cloud and data center – a single control plane
- Security as Code; with tight CICD integration
- VM (ec2), container (ECS), platform (EKS), function (Lambda), service (S3), network abstraction (VPC) etc. visualization
- Recognize and assess application relationships, dependencies and flows
- Baseline behavior across network, process, identity and software
- Policies for portability; one policy engine supporting any cloud

Verify unusual network activity & data exfiltration attempts, including:

- Anomalous lateral movement
- Access to applications outside of operating windows
- Change in application flows and application scale
- Logins from unknown sources
- Access to services such as S3

Monitor privileged account abuse and privilege escalation, such as:

- Operator access including time, location
- Interactive usage of service accounts
- Service account usage from unknown source
- Unauthorized identities accessing critical apps
- Privileged account activity outside of known or authorized use
- Processes run by different or unauthorized users

Alert on unusual process and system activity, such as:

- Incorrect Security Group configuration
- New processes out of context, time, or application profile
- Compromise in a specific region or zone
- New processes spawning connections out of profile
- Anomalous service user activity

VISIBILITY AND PROTECTION

Process and Behavior Analytics

Fortress XDR is ready to go out of the box, with pre-built analytics to protect application workloads from the Cloud to the Ground

Forensic Information on the Fly

Just click and drag our DVR controls to review your application's behavior down to network and process on an individual workload.

Bridge the Teams

Help Cloud Admins and DevOps collaborate; common language, visualizations, and a cloud agnostic policy engine.

Developer Friendly

Automated discovery, ingested telemetry and analytics which do not get in the way let the developers and the business do their thing.

Federated into Process and Tools

No need to reinvent the wheel. RESTful APIs integrate to leverage existing process and tools. Simply push policy through a plug in the toolchain

Auto-Generated Policy

A Policy engine that traverses any Cloud supporting simple visibility, enhancing understanding, and supporting cloud portability

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.

> "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."
>
> –

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 VISIBILITY

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

TAGCYBER 2020 DISTINGUISHED VENDOR

TIE50 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.

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 platform.

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.

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

sales@truefort.com

TRUEFORT