

ZERO TRUST WITH FORTRESS

PROTECT YOUR APPLICATIONS

Fortress – Quickly go beyond network to implement zero-trust **application** security. The perimeter no longer exists, and traditional security methods are not enough.

Reduce Risk in the Era of Working Remotely

Zero-trust has rapidly overtaken 'trust but verify' since COVID-19 changed our world. With offices closed and most employees working from home, we have opened network access to our critical environments like never before to allow our users to work remotely and to enable operations teams to support the business.

As a result, corporate networks are experiencing unprecedented malicious activity as threat actors recognize the opportunity to prey on the weak. There has been a significant increase in DDoS and Ransomware with some organizations reporting a 75% increase in Ransomware attacks alone. All this access has dramatically increased cyber risk from both internal and external sources, and the climate will not be changing any time soon. The time is now to implement zero-trust to protect your business!

Implement Zero-Trust Today

The concept of zero-trust from the network perspective is not new and although it is a key component of securing environments, it falls short on its own. For years, network teams have been securing environments by implementing strong perimeter controls. However, threat actors still infiltrate environments, use known good pathways to move east-west between servers and workloads, and "live off the land" until they find their target and execute their attack. Network alone is not enough for Zero Trust.

Who is the right team to implement zero-trust application security? Our experience shows that relying on one team alone will not be successful. Your network, security and AppSec teams need to work together to protect your most valuable assets, infrastructure, and data. They need to be able to leverage understanding and insight into critical environments and automatically put policy in place. They need to communicate continuously to implement controls and enforcement and maintain policy going forward. Your teams can be empowered to implement zero-trust, with near-zero risk, with ease, and they can do it right now.

Zero Trust Application Security

The Fortress platform is built from the ground-up to deliver zero-trust security and enable collaboration between your teams. It detects and monitors workloads in real-time, abstracts complexity and automates the creation and validation of fine-grained workload segmentation policy - streamlining the process to design, validate, test, implement and enforce zero-trust application security.

Fortress leverages real-time agent data to visualize telemetry - enriching network behavior with related process and identity metrics. This correlates user, network, process, software, in the context of your applications and presents it in an easily digestible graphical format.

Zero-Trust application security goes beyond **NETWORK** to monitor and control **PROCESS, IDENTITY, SOFTWARE AND OS** in real-time to create, deploy and maintain policies in dynamic compute environments.

66%

Forrester found that organizations deploying zero-trust are 66% more confident in adopting mobile work models.¹

SOLUTION HIGHLIGHTS

- **Bring Your Own Agent**
Leverage existing investment in EDR tools (CrowdStrike, Tanium, etc.) to accelerate your deployment, provide immediate visibility, and support enforcement.
- **Real-Time Network Visibility**
Identify workloads and internal and external connections and dependencies from the cloud to the ground.
- **Real-Time Process Visibility**
Continuous monitoring using behavioral baselines to detect and block anomalous behavior in real time, as a complement to any workload isolation.
- **Identity**
Identify who logs in, from where, with which credentials and what they are doing - now and historically.
- **Auto-Generated Policy**
Automatically design, validate, version-control and manage fine-grained policies, for inter and intra workload zero-trust, micro-segmentation.

It all Starts with Visibility

Simply put, you cannot manage what you do not understand. The journey to zero-trust starts with the ability to visualize your critical applications and environments. Most organizations just do not know what makes up their applications, the dependencies between them and operational controls in place. Add to that the changing dynamics of hybrid and cloud, and it becomes critical that application maps generate automatically and update dynamically. These maps form the foundation used to categorize and classify the environment and are key to building policy.

It ends with Zero-Trust Application Protection

Whether an employee lets the bad guys in by accident, or intentionally steals sensitive data, visibility is the key to security. Without the ability to see what is happening on all workloads and knowing when behavior deviates from a known good state, malicious actors can slip by existing security controls, resulting in a costly or damaging breach. Fortress delivers continuous real-time telemetry across network, process, identity, and software behavior, analyzes it within milliseconds, and generates comprehensive real-time alerts and workflow-driven responses to ensure that bad behavior is immediately seen and stopped.

Not just zero-trust network, but comprehensive, zero-trust application protection.

Leverage application-centric visibility to:

- Create a closed-loop process to ensure no CMDB drift
- Visualize application relationships, dependencies, and flows
- Baseline behavior across network, process, identity, and software
- Default policies are created on a whitelist basis

Verify unusual network activity & data exfiltration attempts, including:

- Anomalous lateral movement
- Access to applications outside of operating windows
- Change in application flows
- Logins from unknown sources
- New systems joining an application
- Usage of FTP, SSH, SCP, etc., on critical systems

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
- Lateral movement with multiple identities
- 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:

- New or different processes listening on known ports
- New processes out of context, time, or application profile
- Use of nmap, metasploit and other potentially malicious tools
- New processes spawning connections out of profile
- Process hollowing through changes in runtime hash
- File systems being mounted on unauthorized hosts
- Anomalous service user activity

VISIBILITY AND PROTECTION

■ Process and Behavior Analytics

Fortress is ready to go out of the box. With pre-built analytics to protect applications, it is the only intelligence platform to identify and alert on process checksum and runtime state anomalies.

■ 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.

■ Uncover Critical Threats

Fortress detects advanced threats by leveraging machine learning and automated, real-time data analytics. Pre-built event correlation and data-driven threat context automatically generates alerts, allowing you to focus on critical issues.

■ Never Trust, Always Verify

Real-time telemetry and "virtual enforcement" allow for the automated creation and real-time testing of the right policy, the first time, across all behaviors.

■ Stop Unauthorized Traffic

Fortress visualizes east/west traffic that would normally be invisible to perimeter firewalls and allows you to detect and block unapproved lateral movement in real-time.

■ Stop Malware & Bad Behavior

Alert and control in real-time on modified or unapproved process runtime states, identities, or activity.



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 XDR 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.

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.

“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.”

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

ZERO TRUST

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- & applitructure 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.



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



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 Protectagent 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



¹How to Make Cloud More Secure Than Your Own Data Center | MacDonald & Crow, Gartner, Oct 2019

²Four Main Types of Cyberattack That Affect Data Center Uptime | DataCenter Knowledge, June 2019

³KuppingerCole 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.