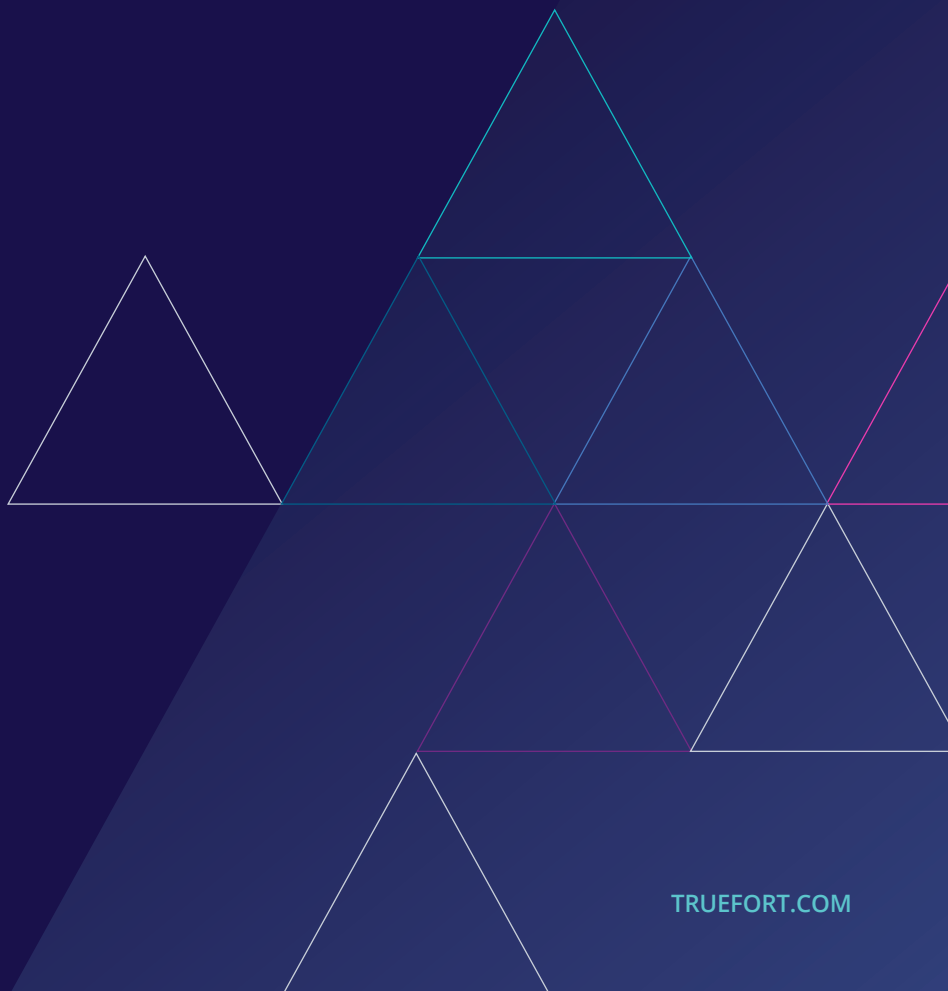
GUIDE

TRUEFORT

Application Environment

Security Readiness Guide

How well are you securing your application environment?



TRUEFORT.COM

Introduction

How well are you securing your application environment?

Properly securing the application environment is one of the most daunting challenges facing any enterprise security team.

These environments are a complex and dynamic collection of legacy, hybrid, and cloud-native applications, each with myriad network and data path interactions within and between them. Application workloads are a distributed collection of virtual machines, containers, container orchestration platforms, cloud-native services, and legacy bare metal deployments. And, DevOps teams are frequently updating and changing application components in response to business needs but without security review.

These characteristics make the application environment uniquely variable and can leave security teams overwhelmed as they attempt to assess environment risk and implement protection strategies.

This guide is intended to help security leaders gauge the readiness of their organizations to secure their application environment. The guide uses a series of scorecard questions divided into four categories:

1. UNDERSTANDING YOUR APPLICATION ENVIRONMENT
2. SECURING YOUR APPLICATION ENVIRONMENT
3. APPLICATION-CENTRIC DETECTION & RESPONSE CAPABILITIES
4. CONTINUOUS APPLICATION RISK POSTURE ASSESSMENT AND VISIBILITY

Readiness Scorecard

Answer the questions in the following four sections, then **total the "No" responses.**

1 UNDERSTANDING YOUR APPLICATION ENVIRONMENT

How well do you understand your application environment?

Do you have a continuously up-to-date inventory of all your applications, whether cloud, hybrid, or legacy?	Y / N
Can you see and make sense of the complex security interactions within and between applications?	Y / N
Do you know what normal security behavior is for each of the applications in your environment?	Y / N
Can you identify application risks that could be exploited at execution?	Y / N
Do you know which applications you need to monitor for data privacy compliance?	Y / N
Do you know which developer changes impact the security of your applications?	Y / N
Can you identify application behaviors that changed when moving from on-premise to the cloud?	Y / N
TOTAL "NO" RESPONSES:	

2 SECURING YOUR APPLICATION ENVIRONMENT

How well can you secure your application environment?

Do you track and continuously update baselined normal security behavior for your application workloads?	Y / N
Are you able to automatically generate and set policy controls based on normal baseline application behavior?	Y / N
Are you able to track changes to your application environment in real time?	Y / N
Do you have application-aware security controls you can deploy to enforce enterprise, regulatory, or industry frameworks (NIST, CIS, PCI, etc.)?	Y / N
Do you use baseline application behaviors when evaluating security impacts across your application lifecycle(development/pre-production/production)?	Y / N
Do you continuously monitor and enforce application environment-secure configuration policies across your application lifecycle (development/pre-production/ production)?	Y / N
Do your operational security processes take into account the dynamic and continuous changes that are happening in your application environment?	Y / N
TOTAL "NO" RESPONSES:	

3 APPLICATION-CENTRIC DETECTION & RESPONSE

How well can you detect and respond to threats in your application environment?

Is your security team alerted in real-time to anomalous application environment security behavior?	Y / N
Would you be able to easily and quickly identify the applications impacted in a 'low and slow' data exfiltration attack?	Y / N
Can you respond automatically and in real-time to limit the blast radius of an application environment compromise?	Y / N
Would you have to build custom tools to identify which application-layer components demonstrated suspicious behavior in a security event?	Y / N
Could you quickly assess the epicenter and impact of an application environment compromise?	Y / N
Can your team view, introspect, and playback application-centric security telemetry around a security event?	Y / N
TOTAL "NO" RESPONSES:	

4 CONTINUOUS APPLICATION RISK POSTURE ASSESSMENT

How well can you can you assess your overall application risk posture?

Do you currently measure your application risk posture?	Y / N
Do you know the variables that impact your application risk posture?	Y / N
Can you measure, monitor, and remediate issues that impact your application risk posture?	Y / N
Do you know how to prioritize activities to improve your application risk posture?	Y / N
Do you know how your application risk posture is impacting your business risk?	Y / N
Do you know how your risk levels are changing over time?	Y / N
TOTAL "NO" RESPONSES:	

Scoring

Totaling Your Responses

Total up the "**No**" responses in each section:

1 UNDERSTANDING

2 SECURING

3 DETECTION & RESPONSE

4 RISK POSTURE

TOTAL NO RESPONSES:

If you answered "**Yes" to all of the questions**, congratulations! You have a strong handle on securing your application environment.

If you answered "**No**" **to 2 or more questions** in any section, your application environment is creating security risks for your business that should be addressed as soon as possible, but certainly in your next security planning cycle.

If you answered "**No**" **to ALL of the questions**, securing your application environment should be considered an immediate priority for your security teams. We recommend adding a solution with an application-centric approach to your security stack in order to give your security teams application-specific visibility, control, and response capabilities.

CONTACT US TO SECURE YOUR APPLICATION ENVIRONMENT!

About TrueFort Fortress

TRUEFORT FORTRESS is a comprehensive, real-time application and cloud workload protection platform that understands and protects the application environment in real-time and at scale.

FORTRESS is purpose-built to secure your application environment from the cloud to the ground. It leverages and integrates telemetry from your existing agents to enhance the value of the information already being generated in your security environment, adding an application-centric perspective to your security.

FORTRESS is a single console, policy, and reporting system from which to measure, control and immediately improve your application risk posture. It secures the largest, most targeted and most dynamic, part of the enterprise attack surface … the application environment.

ABOUT TRUEFORT

TrueFort reduces business risk for security-focused enterprises striving for zero or lean trust application environments. Our innovative and uniquely application-centric Fortress platform delivers comprehensive realtime cloud-to-the-ground insight, protection and automated response with patented machine intelligence and a single or bring-your-own agent. Fortress overcomes the application security blindspots inherent in legacy infrastructure-centric tools, providing unparalleled visibility and protection for applications in on-prem, hybrid and cloud environments and for security teams across the enterprise. Fortress speeds response times, minimizes the blast radius of compromises, prioritizes resources, and enhances application risk posture.

TRUEFORT

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM