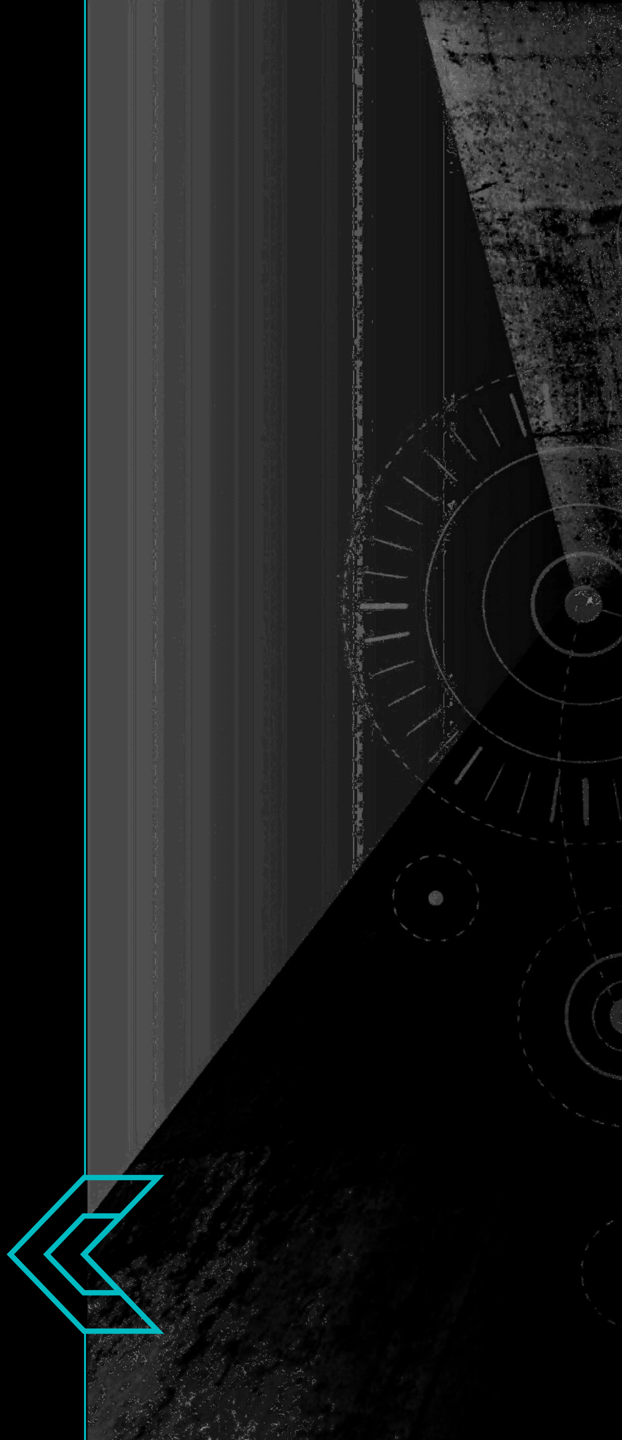
TRUEFORT

WHEN IT COMES TO YOUR **APPLICATION ENVIRONMENT** ...

HOW CAN YOU PROTECT WHAT YOU CAN'T SEE?

END **SECURITY BLINDSPOTS** WITH AN APPLICATION-CENTRIC APPROACH



TRUEFORT.COM

SALES@TRUEFORT.COM | +1 201 766 2023

NOT UNDERSTANDING YOUR APPLICATION ENVIRONMENT CREATES BUSINESS RISK

Your business runs on data, controlled by applications

Attackers target data, making applications high value threat targets

Security strategies that don't fully protect the application environment, leave a large attack surface and increase security risks to the business

APPLICATION ENVIRONMENTS ARE COMPLEX & CONSTANTLY CHANGING

The application environment in any modern enterprise is now a diverse and dynamic collection of legacy, hybrid, and more modern cloud-native applications with myriad network and data path interactions within and between applications.

Application workloads, too, have become a complex and distributed collection of virtual machines, containers, container orchestration platforms, cloud-native services, and legacy bare metal deployments.

DevOps application teams frequently update and change application components in response to business needs but without security approval.

All this leaves security teams overwhelmed as they try to understand the application environment they are trying to protect.

Digital transformation and the move to the cloud have expanded the boundaries of business beyond the enterprise network and introduced new applications and workloads that must also be secured.

CAN YOU PROTECT WHAT YOU CAN'T SEE?

YOUR APPLICATION ENVIRONMENT IS A BLINDSPOT

1/ The application environment is a prominent attack surface with unique security requirements

Agile teams are making frequent changes without security team review, new applications are being added, and compliance requirements change frequently. It's hard for security teams to keep an up-to-date view of the constantly changing, interconnected, and complex application environment, let alone make sound security assessments or policy decisions.

2/ The application-layer of the IT stack is often the most opaque across the security organization

Adding to the problem, the typical infrastructure-centric security stack is designed to protect component layers of the stack like endpoints, VMs, containers, networks, and servers. But **these systems lack observability and a contextual understanding of security-relevant behavior in the application layer**.

For example, network security tools don't understand whether certain applications should be using specific ports when interacting with other applications. They also can't see which apps have recently changed and what changes have been made.

3/ Infrastructure-centric security tools are not designed to and cannot fully protect the application environment

Security teams need observability at the application layer, and to be able to set and apply policy at the application level.

Infrastructure tools lack application understanding and application-aware controls, making their controls less effective for securing applications.

Less effective controls mean hidden risks, compliance violations, & active threats that go undetected for long periods of time.

Threat detection and response teams need to be alerted to application environment risks, violations, and threats before they can become full blown breaches with a huge, business impactful, blast radius.

AN APPLICATION-CENTRIC APPROACH IS A MODERN SECURITY REQUIREMENT

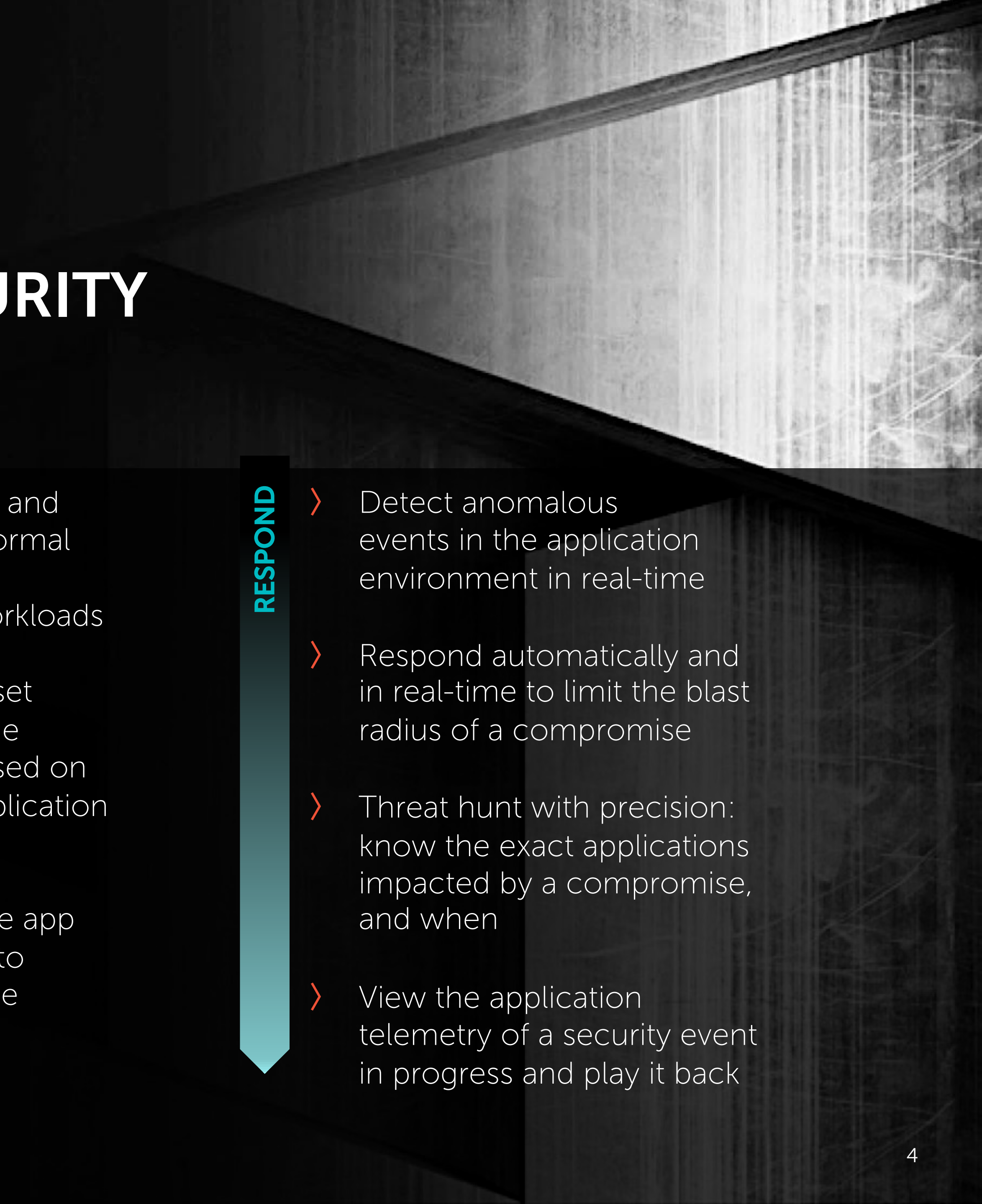
INFRASTRUCTURE-CENTRIC SECURITY ALONE ...

leaves blindspots that can lead to breaches, operational disruption and data exfiltration.

ADDING APPLICATION-CENTRIC SECURITY ...

gives security teams better insight, better response capabilities, and more time to be proactive.

WHAT YOU'RE MISSING *WITH* INFRASTRUCTURE-CENTRIC SECURITY



CAN YOU … ?

SEE

- Identify all the applications in your environment
- Visualize all the security-related interactions and dependencies within and among applications, systems and data
- See real-time status on your app risk posture

CONTROL

- Continuously refine and update baselined normal behaviors for your applications and workloads
- Auto generate and set policy controls at the application level based on normal baseline application behavior
- Enforce policy at the app and workload level to maintain compliance

RESPOND

- Detect anomalous events in the application environment in real-time
- Respond automatically and in real-time to limit the blast radius of a compromise
- Threat hunt with precision: know the exact applications impacted by a compromise, and when
- View the application telemetry of a security event in progress and play it back

TRUEFORT

APPLICATIONS & DATA ARE CENTRAL TO YOUR BUSINESS …
SO WE DESIGNED A PLATFORM TO SECURE THEM

TRUEFORT was founded by two financial services security professionals who faced a major breach exposing their application environment and business critical data.

In the weeks that followed, they found they didn't have the information they needed to fully understand and respond to the attack, or prevent a similar attack in the future.

Their 'infrastructure-centric' security methods and tools were a poor fit for protecting the critical business applications on which some of the largest financial institutions in the world relied.

They realized that their business — and all businesses, really — needed an innovative approach that wouldn't just promise security but would deliver with a solution that could understand and protect the application environment in real-time and at scale.

TRUEFORT FORTRESS is that solution.

> "TRUEFORT FORTRESS gives us security visibility into our application environment that has radically improved our threat detection and response."
>
> *-- Top Global Healthcare Company*

WHAT IS APPLICATION-CENTRIC SECURITY?

- An innovative approach to security designed to specifically address the unique needs of the application environment and add a layer of additional security capabilities with application context
- Complements your existing infrastructure security tools
- Gives application-specific observability, control, and response to security teams across the enterprise

TRUEFORT

FORTRESS

PROTECT YOUR APPLICATION ENVIRONMENT IN REAL-TIME

TRUEFORT FORTRESS is a **comprehensive, real-time application and cloud workload protection** solution.

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.

Best of all, FORTRESS is **a single console**, policy, and reporting system from which to measure, control and immediately improve your overall application environment risk posture.

TRUEFORT FORTRESS **secures the largest, most targeted and most dynamic, part of the enterprise attack surface …**

its application environment

GO BEYOND INFRASTRUCTURE SECURITY

1/ Reduce your attack surface

2/ Uncover hidden risks

3/ Enable real-time detection and response

REQUEST A DEMO & SEE WHAT YOU'VE BEEN MISSING

TRUEFORT

Protect your complex application environment in real-time, at scale

4 WAYS **FORTRESS** APPLICATION-CENTRIC SECURITY DELIVERS BETTER SECURITY

1/ True visibility into and understanding of your complex and dynamic application environment

2/ Security controls that apply to workloads with application-level context, insight and policies

3/ Significantly reduced mean-time to detection *and* response with real-time alerting and actionable information about impacted applications and workloads

4/ Improved app risk posture with continuous monitoring, assessment and reporting for security, ops and executive teams

understand
tame
assess
detect
control
respond
monitor
improve
protect

harden
segment
secure service IDs
ensure integrity
allow/deny
prevent exploits

TRUEFORT

WWW.TRUEFORT.COM

SALES@TRUEFORT.COM
+1 201 766 2023

REQUEST A DEMO &
SEE WHAT YOU'VE
BEEN MISSING