TRUEFORT™

Application Runtime Segmentation

that Understands Application Behavior to Protect It

Innovative technologies create incredible capabilities but leave your applications and workloads exposed.

As each organization's digital footprint expands to include greater capabilities and broader locations, their risk also concurrently grows.

The previous security measures that included perimeter firewalls and network segmentation as protective shields from supply chain attacks, ransomware, and nation-state attacks are no longer reliable. With so many companies running production applications on cloud infrastructures, the ability to bypass and comprise controls have become much less complicated.

With applications constantly changing, it can be very difficult for security solutions to keep pace, leaving organizations vulnerable and under a near constant attack at levels never previously imagined. In 2021, corporate ransomware attacks occurred every 11 seconds, with 30,000 websites attacked everyday worldwide.

Corporate ransomware attacks occur every 11 seconds, with 30,000 websites attacked everyday worldwide.

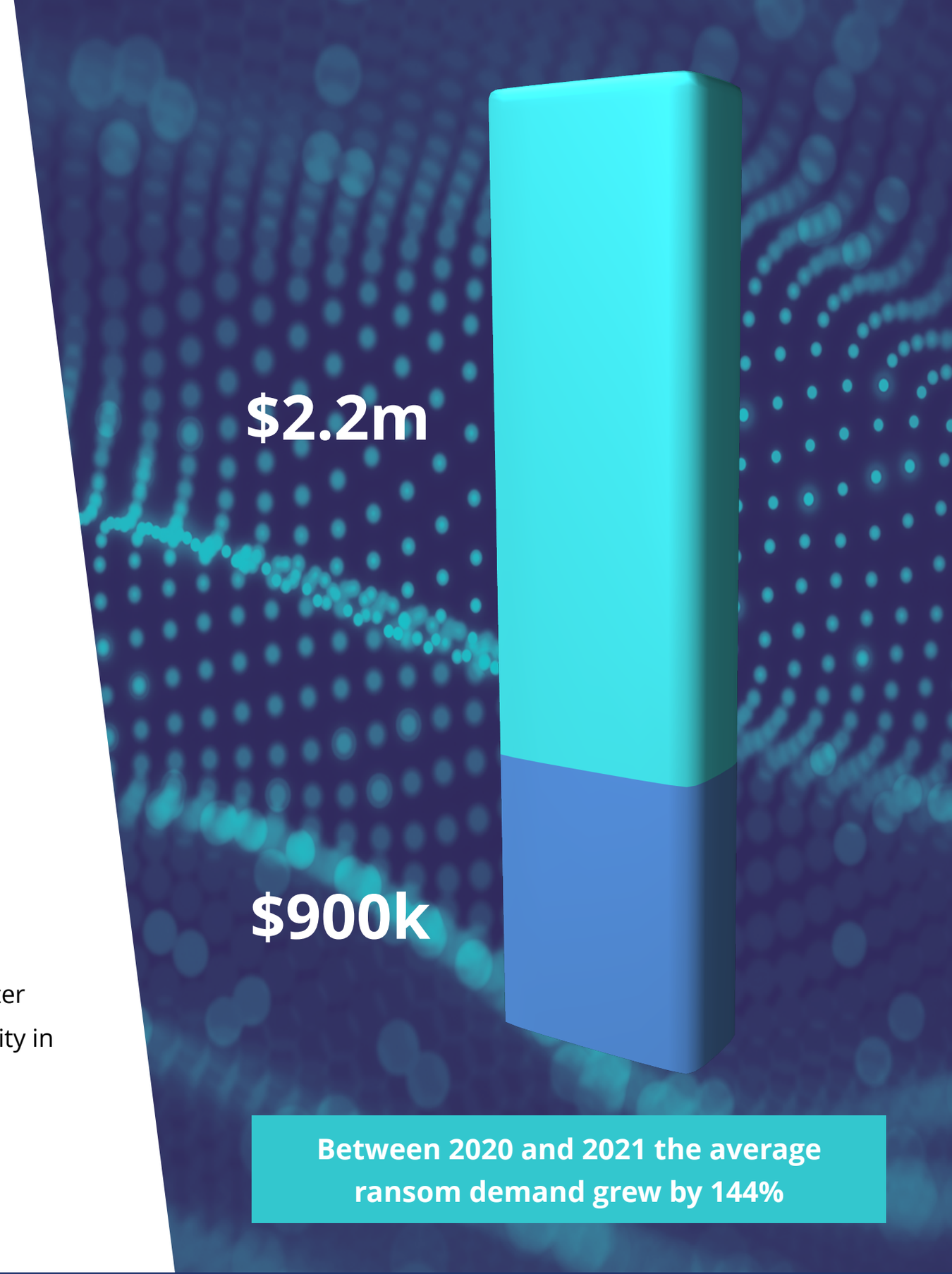
What can you do?

Most organizations focus security efforts in a few key areas.

But if you only protect your infrastructure and fail to invest in securing the data center and cloud workloads, you're leaving yourself incredibly exposed to ransomware attacks. Between 2020 and 2021 the average ransom demand grew by 144% from $900,000 to $2.2 million. Can you afford to take your chances?

You need to establish a zero-trust architecture that monitors and exposes what's actually happening.

Using this to guide your zero-trust implementation you can better protect workloads and applications while maintaining full visibility in real-time.



How did we get here?

Obviously cyberattacks are not a new phenomenon, but they've grown exponentially since the first known attacks beginning in the 1980s and they're not expected to stop anytime soon. By 2031 it's estimated that the frequency of ransomware attacks on governments, businesses, consumers, and devices will occur every 2 seconds – or about three attacks in the time it took to read this sentence.

Choosing to ignore this trend leaves your entire business in peril. From 2009 to 2019 the number of cyber-attack incidents resulting in over $1 million in reported losses grew by over 500%.

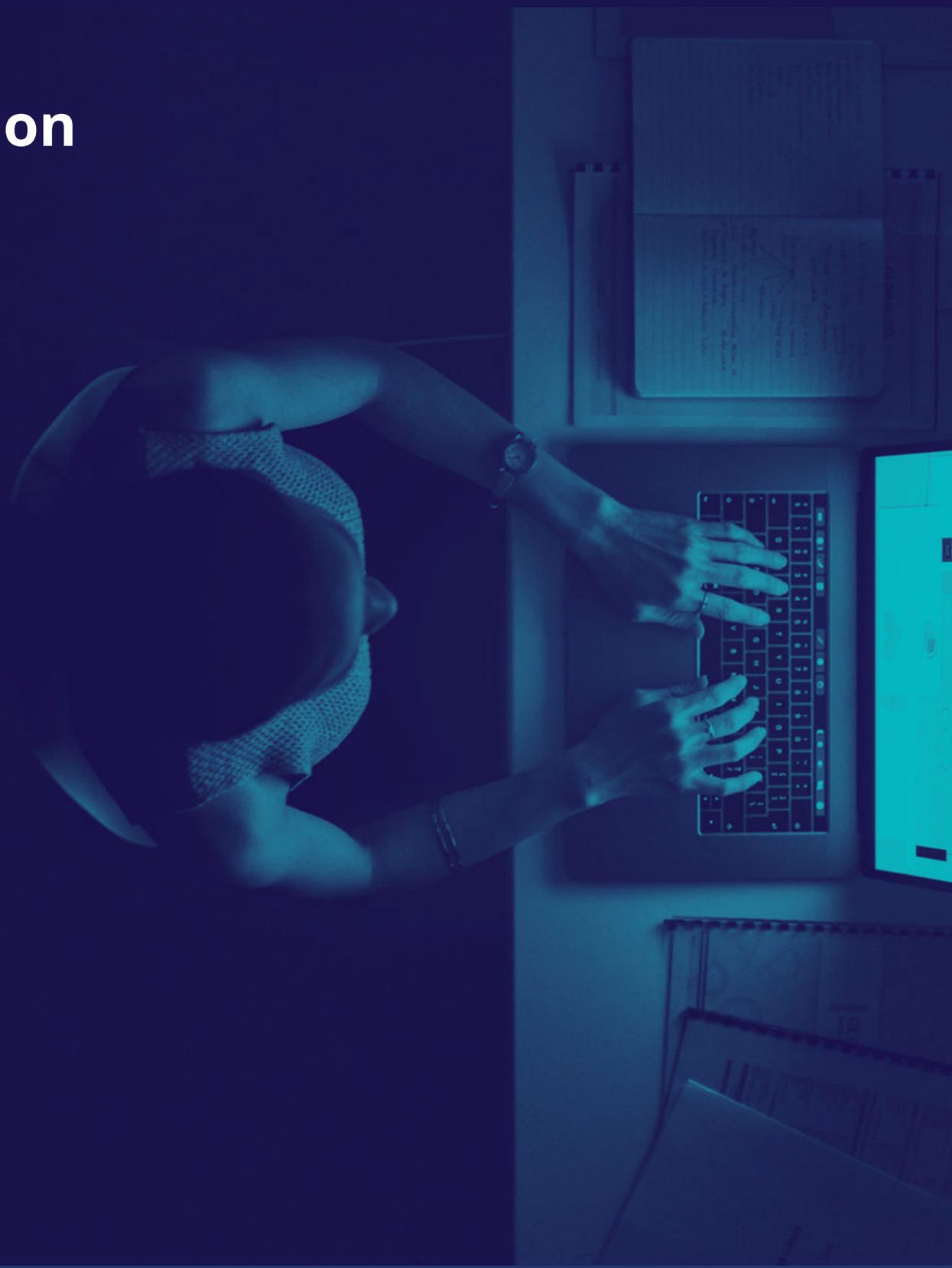
Just to add more context, if measured as a country, cybercrime's $6 trillion globally in 2021 would rank as the world's third-largest economy after the U.S. and China.

Cyber Attack Incidents with $1M+ in Reported Losses grew by over 500%

An Application Intelligent Solution

To fully protect your critical workloads, you need to be continuously detecting and monitoring for suspicious activities against established baselines between users and applications.

Too many organizations rely on solutions that notify them after an event has occurred, and many others are too siloed in their approach, making it difficult to alert and understand the severity of suspicious activities on specific applications. By creating trusted profiles, you can enable a proactive security model by alerting or blocking on activities outside the expected norm.



What does a flexible and proactive security solution deliver?

Imagine driving in your car in the middle of a rainstorm and suddenly your wipers only remove about half of the incoming water splashing against your windshield.

Does that make you feel vulnerable?

Cybersecurity works in the same manner.

Limited visibility is ineffective. How can you feel that your environment is adequately protected if you can't observe, behaviorally baseline and alert on deviations in real-time? Insulating your environment against compromise from lateral movement, dreaded supply chain attacks, compromised or rogue service accounts, file and configuration drift and insecure ephemeral containers enables you to insulate against compromise.

Areas of Focus

Step 1 – Reduce Risk

Limit the consequences security incidents can cause across critical environments. By taking action to baseline normal activity, you eliminate risks within your production environment and increase your overall resiliency while also avoiding costly downtime.

Step 2 – Limit Exposure

Shrink your organization's exploitable attack surface. This will enable you to greatly reduce the attack impact of incidents that reach your public-facing environments.

Step 3 – Empower your SOC

Allow your team to take immediate action to contain cloud attacks and expand their ability to isolate the extent of an attack before it can reach privileged information.

Create a Shield of Protection

Workloads must be protected across all environments. Consolidate or replace fragmented security tools across both the data center and cloud-native technologies:

1

Reduce the blast radius around legacy servers with Zero Trust segmentation

2

Protect database and workloads by enforcing good behavior

3

Secure your Kubernetes and service mesh environments without code change

While it's simply not realistic to completely secure every aspect of your business, you can protect critical workloads by combining environment-wide security observability with real-time detection and response, intelligent microsegmentation, service account behavioral analytics, file integrity monitoring, CIS-certified hardening, and container / Kubernetes behavioral security.

A solution that protects applications through an application-centric lens, enables you to clearly see applications, their components and dependencies, and continuously profile and detect to find anomalies while enforcing zero-trust segmentation and workload protection.

What can TrueFort offer?

Understanding the pressing need for a comprehensive solution is only the first step, ensuring you're working with a trusted provider who can deliver protection is just as important. TrueFort's platform combines behavioral analytics with real-time security telemetry to establish a full process, user, and network behavioral profile across data center and cloud environments.

By continually analyzing workload behavior as changes are happening and comparing each one against baseline expectations we're able to identify activities that are outside the norm. We provide runtime environment protection in 6 key ways:

Cloud Workload Protection

Dynamically adapting to unusual activities detected across on-premises and cloud workloads.

Microsegmenting Environments

Intelligently baselining normal, high-volume activity, limiting future behavior to what should be trusted.

File Integrity Monitoring

Validate unexpected changes to discover novel malicious activity.

Service Account Behavior Analytics

Identify, monitor, and learn trusted connection patterns.

Workload Hardening

Adaptive configuration policy monitoring, with immediate notification when gold image drift occurs.

Container and Kubernetes Security

Protect containers from compromise by baselining runtime behavior to find anomalies and respond in real-time.

Only TrueFort combines environment-wide security observability with real-time response, workload protection, Microsegmentation, service account behavior analytics, file integrity monitoring, and CIS-certified hardening and container and Kubernetes security in a single platform.

The two constants that comprise our modern business reality are the need for ever-expanding technology and the threat of those who will look to exploit it for their own gain. The more data and applications you rely on as your business grows, the more exposed you are to cyber threats.

It's estimated that the global cost of cybercrime will grow by 15% each year over the next five years, reaching an unimaginable $10.5 trillion in annual expense by 2025. This figure represents more than the costs associated with natural disasters around the world and the global trade of all major illegal drugs combined.

In order to preserve your business and its financial integrity, you must have a comprehensive enterprise protection solution across each of your production environments. A reliable platform that provides a shield of protection while minimizing risk, restricting exposure and empowering your team to take decisive action.

TrueFort's innovative platform offers an intelligent approach that continuously insulates your environment against suspicious activities, detects malicious behavior, and prevents lateral movement.

Gain comprehensive protection by securing your workloads at the application level with TrueFort.