TRUEFORT

SOLUTION BRIEF

TrueFort® Platform: Application Discovery and Mapping

The Need for Application Discovery

Organizations face the complex challenge of managing a diverse array of enterprise applications, including cloud-based, legacy, and a hybrid of the two. This diversity, coupled with the increasing sophistication of cyber threats, makes it difficult to maintain visibility and control over the application environment.

Application discovery is crucial, providing essential insights into all workloads in use, including those unknown or unauthorized. This comprehensive visibility is indispensable for identifying vulnerabilities, ensuring regulatory compliance, and implementing effective security measures.

Comprehensive Application Visibility

TrueFort's real-time application visibility capabilities enable organizations to achieve comprehensive oversight of their application landscape. TrueFort Platform identifies and catalogs all workloads and communications, both known and unknown, including legacy systems, ensuring no assets goes unnoticed.

By doing so, TrueFort provides critical insights into the interactions and dependencies between applications and their associated workloads. This level of detail enhances security measures and pinpoints crucial workloads, understanding their usage and identifying which applications are interacting with them, offering a clear framework for effective cybersecurity management.

"We need to get this installed everywhere - right away!"

Cybersecurity lead for a national energy co.

- **48%** of security breaches occurred at the application layer, making it the most commonly identified attack vector.
  (Forrester)
- In the past year, **76%** of organizations experienced a security incident due to a lack of clear application visibility.
  (Cisco)

Enhancing Security with Application Behavioral Mapping

TrueFort's application behavioral mapping significantly deepens the understanding of application activities within an IT environment. This advanced feature constructs detailed profiles of normal application behavior, enabling the detection of deviations or anomalies that might signal potential security risks. Utilizing machine learning, TrueFort continuously monitors and analyzes application operations at various levels—from network to the service accounts executing commands on each workload. This allows the TrueFort Platform to swiftly identify unusual activities, such as unexpected data access or anomalous network traffic patterns, which are often indicative of security incidents or malicious exploits. Such capabilities are instrumental in maintaining a secure and resilient IT infrastructure.

Dependency Mapping and Risk Identification

TrueFort's application dependency mapping enhances cybersecurity by charting the interconnections and dependencies among various applications within an IT ecosystem. This mapping is vital for pinpointing risky practices, revealing the complex web of interactions where a single compromised application can impact others. By understanding these dependencies, TrueFort enables organizations to identify and fortify potential weak points in their network. This comprehensive understanding of application relationships strengthens the overall security framework, allowing for more targeted and effective defense strategies against cyber threats and ensuring a more secure and resilient IT infrastructure.

"This does even more than we thought."

Security Architect and TrueFort customer

Application Optimization and Allowlisting

Application optimization through insights gained from TrueFort Platform deep visibility, can help to optimize system stability and enhance security in IT environments. By efficiently distributing workloads across available resources, this can prevent the overloading of any single application, reducing the risk of crashes and performance issues. This ensures smoother operations and contributes to a more secure environment by reducing the points of vulnerability that can be exploited during times of stress or high traffic.

Additionally, TrueFort Platform's application allowlisting solutions play a crucial role in security by allowing only authorized applications to execute. This prevents the running of potentially harmful or unauthorized software, thereby safeguarding the system against cyber threats.

The Application-Centric Lens of TrueFort

TrueFort adopts an application-centric approach to network security, focusing on the specific behaviors and requirements of each application within an IT ecosystem. This strategy offers significant advantages, such as tailored security policies, precise threat detection, and more effective risk management. By concentrating on applications as the primary security entities, TrueFort provides a nuanced understanding of how applications interact within the network, vital for identifying and mitigating potential security incidents.

Catering to both application developers and network security engineers, TrueFort Platform facilitates the development of secure applications while ensuring that network security measures are robust, responsive, and aligned with the unique dynamics of each application.

Leveraging Existing EDR Agents

Through our technical partnerships with existing endpoint detection and response (EDR) agents, such as SentinelOne and CrowdStrike Falcon, TrueFort significantly amplifies an organization's cybersecurity capabilities. EDR agents, adept at detecting and responding to threats at the endpoint level, when integrated with TrueFort, extend their protective scope across the entire network. Our relationship with Armis ensures insight into OT/IoT devices and their network relationships. This integration results in a much deeper visibility into network and enterprise application activities. Such expanded oversight is crucial for identifying and countering sophisticated cyber threats, including elusive zero-day attacks. This comprehensive approach ensures that potential threats are identified and mitigated quickly and effectively, thereby fortifying the organization's overall cybersecurity posture against advanced, continuous cyber threats.

Bridging the Cybersecurity Gap

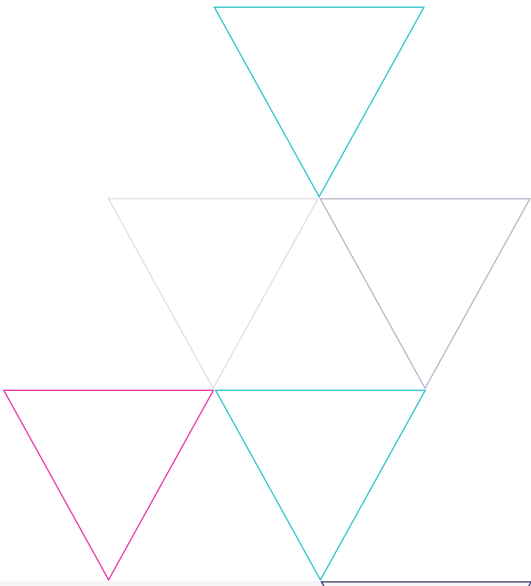
TrueFort plays a pivotal role in addressing the largest cybersecurity gap in application environments: the lack of comprehensive visibility and control within applications. By providing detailed insights into application behaviors, dependencies, and vulnerabilities, TrueFort closes the security gap that traditional, perimeter-focused solutions often overlook. Its application-centric approach ensures that each application's unique characteristics and interactions are accounted for, leading to more effective detection and mitigation of potential threats. This targeted strategy significantly enhances an organization's ability to safeguard against the evolving and sophisticated cyber threats targeting application infrastructures.

"This is a total eye-opener. Your product capabilities are massively understated."

CISO, Financial Services, TrueFort customer

"Nobody, and I mean NOBODY, else is doing this."

Director of Security Engineering for Forbes Top 5 Telecom provider, TrueFort customer



ABOUT TRUEFORT

TrueFort® Platform puts you in control of lateral movement across the data center and cloud, protecting service accounts and against zero-day threats. The TrueFort Cloud extends protection beyond network activity by shutting down the abuse of service accounts. Founded by former IT executives from Bank of America and Goldman Sachs, leading global enterprises trust TrueFort to deliver unmatched application environment discovery and microsegmentation for accounts and activity.

For more information on how TrueFort can enable enterprise-level application discovery, visibility, and relationship mapping, please contact us for a detailed demonstration.

TRUEFORT®

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM