KuppingerCole Report

EXECUTIVE VIEW

by Alexei Balaganski | November 2019

TrueFort Fortress XDR

TrueFort Fortress XDR is an application detection and response platform offering integrated application behavior analysis and security for real-time visibility into critical business applications, early detection of anomalous and malicious behaviors, and proactive tuning of security policies to prevent them from turning into data breaches.

by **Alexei Balaganski**
ab@kuppingercole.com
November 2019

Content

Related Research

Leadership Brief: Do I Need Endpoint Detection & Response (EDR)? – 80187

Leadership Brief: Do I need Network Threat Detection & Response (NDTR)? – 80296

Advisory Note: Integrating Security into an Agile DevOps Paradigm – 71125

Advisory Note: Connected Enterprise Step-by-step – 70999

Advisory Note: Real-Time Security Intelligence – 71033

1 Introduction

The proverbial “network deperimeterization” many security experts have been constantly talking about for years is no longer just an ongoing trend – it is the new reality modern businesses have to live and operate in. With a growing number of applications, data stores, and other workloads moving to the cloud as well as the increasing number of external partners, contractors or even customers accessing them, modern corporate networks no longer resemble traditional castles with walls and moats. Rather, they resemble sprawling urban areas, loosely connected and often governed by completely different IT teams or even 3rd party companies like cloud service providers.

The unfortunate downside of this digital transformation has been a sharp increase in the number and scale of data breaches. Whether focusing on targeted attacks for purposes of industrial espionage or sensitive data theft or drive-by attacks like ransomware, cybercriminals are constantly developing new methods of infiltrating corporate IT systems and traditional perimeter security tools like firewalls cannot stop them.

Unsurprisingly, in recent years, the focus of the information security market has gradually shifted from perimeter protection towards monitoring and detecting malicious activities within enterprise networks. However, neither manually operated security information and event management platforms (SIEM) that were once presented as the ultimate solution to all security problems nor the more modern AI-powered detection and response products that came to replace them later seem to fare substantially better.

Alert fatigue and the notorious skills gap, however, are only partially to blame here. Perhaps the most fundamental reason for the inability of even the most modern detection tools to keep up with the current risk landscape is that they are still implementing a siloed approach towards cybersecurity, leaving wide gaps in coverage between individual endpoint, network-level or cloud-focused products.

The latest trend that promises to overcome these limitations of isolated tools is XDR. “X” here represents a variable that can stand for anything but is generally understood as the evolution of EDR (Endpoint Detection and Response) to include more sources than just endpoints. In this sense, XDR tools can incorporate security data from network, cloud, threat intelligence and other sources, giving analysts full understanding of every stage of a cyberattack across multiple environments. Such tools are designed to assist analysts at mitigating attacks faster by automating the remediation activities. This approach can reorient security professionals more towards user- or business-focused protection.

However, as long as such solutions continue to focus on infrastructure alone, they are going to miss all the crucial business context information that is only available through higher-level analysis. For example, 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 of a vulnerability and to prioritize mitigation actions accordingly.

This seemingly obvious idea is the foundation of the TrueFort application analytics and protection platform. The company offers a comprehensive application-focused XDR solution to monitor modern cloud-native and hybrid workloads, detect and quickly remediate any cyber-threat and prevent data breaches, utilizing the telemetry from 3rd-party agents already deployed by most organizations.

2 Product Description

TrueFort is a privately held cybersecurity vendor headquartered in Weehawken, New Jersey, USA. The company was founded in 2015 by a group of veteran IT and security leaders that spent over 20 years protecting financial institutions from data breaches. The company's vision from the beginning was to develop an alternative approach towards protecting mission-critical business applications from external and internal threats.

TrueFort had the following design objectives for their product. First, it had to focus on the application and session layer, not on lower-level infrastructure to be able to understand and profile application logic in a business sense and thus better understand the risks and vulnerabilities that may lead to data breaches.

Second, it must be able to combine static security-related information collected from applications (such as source code analysis, vulnerability management, identity and access policies and even basic asset and configuration management) with dynamic real-time telemetry from multiple sources (endpoints, network, cloud APIs, application profilers, log files, etc.) to constantly adapt to new activity patterns in runtime environments.

Last but not least, the solution must not only provide intelligent automation capabilities but most importantly, help to fine-tune existing application security policies to prevent similar incidents from happening again.

Recently, after another successful investment round, the company has rebranded and restructured its portfolio to focus on a single integrated application behavior analytics and security platform named **TrueFort Fortress XDR**. As the new name indicates, the company is placing a strong emphasis on the broad scope of the collected security telemetry across on-premises and cloud environments, just like the other vendors in the emerging XDR-branded products market. However, we cannot but stress that the TrueFort primary competitive advantage over existing detection and response tools is the fundamental focus on high-level application behavior analysis and automatic remediation of IT problems regardless of underlying infrastructures: bare-metal systems, popular virtualization platforms, private and public clouds, and most recently containers.

Another notable distinction is the company's early realization that a substantial amount of the telemetry needed for such a platform to function is already being collected by existing security tools and integrating with them would result in a substantial reduction of wasted computing resources. In fact, the platform is designed to support open integrations with 3rd party EDR and other security solutions and, with certain limitations, is able to function completely without own agents.

The first such official partnership has been recently announced with CrowdStrike, which makes TrueFort available directly on the CrowdStrike Store for customers looking for full visibility into their application activities beyond just endpoints. Further integrations with security vendors like Tanium, InfoBlox, or F5 are supported as well, with more partnerships to be announced soon.

This agentless option makes TrueFort especially suitable for companies that wish to adopt modern application XDR technology without significant upfront investments and deployment efforts – existing

EDR users can start with a single management appliance tapping into existing endpoint telemetry and then gradually expand the coverage to cloud workloads, containers and so on by deploying the agents from TrueFort.

The platform is delivered as a pre-configured virtual appliance. Multiple appliances can be combined into a clustered setup for high-performance and high-availability deployments. From the very beginning, the platform was designed for cloud deployments and multitenancy, and some TrueFort customers already deploy it in public clouds like AWS and Azure.

Initial setup requires the definition of access roles and connection to external telemetry sources. Then customer admins can import an existing configuration management database (CMDB) and start the initial application discovery process. From that moment, the platform will work automatically to map your business applications, their components and data flows, producing a detailed visual map of application behaviors in real-time and for any historical moment.

The TrueFort platform utilizes machine learning (ML) algorithms to examine over a hundred raw data points and build application-specific behavior profiles, detect deviations from the norm and alert security analysts when malicious or suspicious activity is identified.

For forensic investigations, Fortress XDR provides all the required capabilities expected from a detection and response solution: the ability to drill into any detail of an incident, see all application and network events associated with it, pivot to related assets, and so on. However, it is also possible to go back in time and see the exact state of an application at any moment from the recorded past. From the same interface, an analyst can initiate a response workflow or push the event into an external incident response platform. Of course, all discovered events can be also automatically pushed into an existing SIEM solution like Spunk.

Examples of automated responses include terminating malicious processes and injecting firewall rules to block data exfiltration. In fact, one of the biggest TrueFort differentiators is that these activities can be policy-driven, effectively implementing dynamic application-centric network micro-segmentation. This means that, based on current and historical data analysis, the platform can update a security policy and enforce a mitigation control proactively, possibly even before a security incident can turn into a data breach. Again, it is the application-relevant context available to the analytical engine that enables this process to happen automatically, as opposed to more traditional micro-segmentation solutions that require manual configuration.

For its native agents, TrueFort provides support for a variety of platforms, including Windows, Linux, Solaris, VMware vSphere and all major cloud service providers. Network-level protection and micro-segmentation can be implemented on endpoints by directly manipulating existing Windows and Linux native firewalls, or via integrations with network security products like VMware NSX or Fortinet.

A major addition to the latest TrueFort release is support for dynamically monitoring and protecting Kubernetes container orchestration environments. A specialized TrueFort agent must be deployed to a Kubernetes cluster using the DaemonSet approach. This means that a single configuration file that's added to the cluster causes a copy of the agent to be automatically deployed on each cluster node, providing full coverage of all internal and external activities and communications.

With this approach, TrueFort is now able to not just efficiently collect infrastructure-level telemetry from Kubernetes clusters, but to analyze application-specific network and process data and isolate or terminate anomalous activities in real time. Currently in beta, this capability looks promising for customers that develop and operate modern containerized and microservice-based applications.

Among other notable new features of the latest version is support for additional “legacy” operating systems like HP-UX and AIX, as well as improved CrowdStrike integration to consume more telemetry and threat intelligence data. In addition, a new Reporter module is introduced, which implements advanced searching and filtering capabilities to let users configure precisely which telemetry they want to see in the management console.

Additional external telemetry source integrations and improvements in the Reporter module are expected to be delivered in the next version planned for early 2020.

3 Strengths and Challenges

The TrueFort Fortress XDR platform implements a really unorthodox combination of more traditional (if this term can be applied to a very recent technology trend) infrastructure-focused XDR platforms and of more application-focused monitoring and protection solutions, which are usually lacking intelligent automation capabilities. By combining the benefits of both approaches, TrueFort strives to deliver a full-featured application detection and response solution that not only provides full visibility into business-critical applications and quick threat detection but enables automated proactive tuning of existing security policies, blocking malicious activities before they even occur.

By integrating with existing EDR solutions and reusing their endpoint agents, the platform not just helps prevent "agent sprawl" but makes the deployment process much more cost- and time-efficient. It's a pity though that the company does not yet offer their technology as a SaaS-based solution, as this would make it much more accessible and frictionless to deploy. Hopefully, this will change in the near future.

Strengths	Challenges
• Unique focus on application-level security analytics provides business context for analysis and remediation • Open XDR platform to consume static and dynamic telemetry from multiple IT environments • Integrations with EDR vendors enable existing 3rd party agent reuse • Proactive tuning of security and micro-segmentation policies • Automated threat remediation with own or third-party enforcement	• Built-in incident workflow management capabilities are quite rudimentary, rely on 3rd-party integrations • Not available as a SaaS solution yet

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstraße 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com