Brought to you by Informa Tech
OMDIA

Publication date:
01 Jan 2023
Author:
Rik Turner, Principal Analyst, Emerging Technologies

On the Radar: TrueFort offers workload protection via microsegmentation

Summary

Catalyst

TrueFort delivers protection for workloads in customers' data centers and cloud environments, with its current focus being microsegmentation technology.

Omdia view

The steady advance of both the infrastructure- and platform-as-a-service (IaaS and PaaS) modes of delivering cloud computing means that ever more workloads need protection from cyberattacks. Microsegmentation is a prescriptive, zero-trust approach to the problem in that it curtails access rights to the bare minimum, then monitors continuously to see whether, even so, someone has managed to mount an attack.

The fact that TrueFort's platform can also be used for other security activities, such as file integrity monitoring and service account behavior analysis, all from the same underlying technology, further enhances its overall attraction. It also enables the vendor to target different use cases and, potentially, even different buyers within the enterprise.

The TrueFort Cloud offering should expand the vendor's market reach considerably, as its technology can now be delivered entirely in hosted mode, making it available to a broader swathe of potential customers.

Why put TrueFort on your radar?

Microsegmentation is a zero-trust approach to securing data center and cloud workloads. Organizations considering its adoption should get to know TrueFort's offering and test its claims of greater scalability vis-à-

vis the competition, thanks to its agentless approach and the fact that it does not rely on pre-defined rulesets.

Market context

Workload protection is mainly spoken of in the context of the cloud, which is logical given the speed with which application code is updated in that environment and, therefore, the need to protect it from attacks at runtime. In recent years, cloud workload protection platforms (CWPPs) have become an established part of the cloud security landscape. CWPPs are also a core component of the cloud-native application protection platforms (CNAPPs) emerging to address the broader security requirements of IaaS and PaaS environments.

That said, there are distinct advantages to deploying workload protection technology that can span both the cloud and on-premises worlds, particularly for the hybrid cloud environments that prevail in many organizations nowadays. After all, if a workload can be compromised while it resides in an organization's own data center, there is the potential for it to cause much wider damage as and when it is migrated to a cloud environment.

Microsegmentation can be thought of as one flavor of CWPP. It harnesses the principles of network segmentation from the on-premises world, which was typically delivered by a physical firewall, with rules to govern access rights to assets on different parts of a corporate network. Indeed, since most firewall vendors have developed and launched cloud-based versions of their products, they are now among the contenders for delivering segmentation capabilities in those environments too.

Microsegmentation does something similar to the network segmentation delivered by on-premises firewalls but instead uses the internal firewalls built into common operating systems. To do so, it leverages the user-space utility programs, that is, Windows Firewall in Microsoft environments and iptables in Linux, which enable it to configure the IP packet filter rules of the operating system's kernel firewall.

Product/service overview

TrueFort uses a combination of behavioral analysis (in this case of "entities," i.e., workloads rather than humans), microsegmentation to control access, and continuous monitoring to pick up anything unexpected in the way that a workload is operating or being accessed even after the microsegmentation has been established. As such, TrueFort is effectively competing in a range of discrete markets:

File integrity monitoring (FIM) – FIM is a process for validating the integrity, originally of operating systems and application software files, but now also of configurations, databases, cloud accounts, and other objects.

This is done using a verification method that compares the current object state and a known, good baseline, which entails calculating a known cryptographic checksum of the object's original baseline and comparing with the calculated checksum of the current state. This method was pioneered by Tripwire (now part of HelpSystems, which itself has just rebranded as Fortra) around the turn of the millennium for Unix files. TrueFort says it is often deployed as a replacement for Tripwire FIM because traditional FIM technology is not cloud-friendly and lacks contextual notification—that is, it can notify that something has changed within an object but doesn't necessarily pinpoint where or what.

Behavioral analysis – in this case, behavioral analysis is specifically for service accounts rather than regular end users. User and entity behavior analysis (UEBA) is a technology that gained considerable attention during the 2010s and, where it was once sold as a standalone product, has now largely been subsumed into

broader portfolios to assist with the detection of and response to threats. It works by modeling what constitutes normal behavior for a subject (whether human or non-human) and building a profile against which anomalous activity can be detected and an alert issued.

In TrueFort's case, the entities it analyzes are accounts that grant privileged access to systems within an infrastructure and that are used by system administrators. Hijacking such accounts is clearly an ideal way of gaining high-level access to an organization's infrastructure and is, therefore, a useful first step toward the theft of intellectual property or other types of sensitive data, or indeed, of doing damage to the infrastructure as part of an attack.

Microsegmentation, meanwhile, is a form of workload protection that enforces the principle of least privilege, thereby reducing the attack surface for that application. Continuous monitoring after the microsegmentation has been enacted enables ongoing protection by detecting threats and making it possible to respond to them in real time. The technology also enables workload hardening and, in TrueFort's case, can be used for virtual machines (VMs), containers, and Kubernetes, the orchestration platform for containers that is now all but universally adopted in this market.

In April 2022, the vendor sought to broaden its addressable market with the launch of TrueFort Cloud, an AWS-resident version of the platform, which enables it to meet the needs of a wider market and, as the company itself said at the time, make "application-intelligent workload protection, service account analytics, and microsegmentation accessible to customers in one day."

Company information

Background

TrueFort was founded in 2015 by CEO Sameer Malhotra and CTO Nazario Parsacala, the two men having met while working on Wall Street. Malhotra was previously a managing director at JP Morgan Chase and, before that, held executive roles at BofA Merrill Lynch, Goldman Sachs, Bear Sterns, and Salomon Bros. Similarly, Parsacala was most recently an executive director at JPMC and, before that, held leadership posts at BofA Merrill Lynch and Goldman.

The two cofounders' experience fending off high-stakes attacks as they led security and IT at these global banks, and in particular, a major breach suffered by JPMC, led them to create TrueFort.

The vendor has raised a total of $48m in funding, most recently announcing a $30m Series B round in September 2021, led by Shasta Ventures, with the participation of Canaan and Ericsson Ventures, as well as existing investors Evolution Equity Partners, Lytical Ventures, and Emerald Development Managers.

Current position

The company launched its first technology offering in December 2019, calling it TrueFort Fortress XDR and describing it as an "application detection and response platform to secure applications and cloud workloads." Since then, it has expanded into a fully-fledged technology platform and been rebranded as the TrueFort Platform, which can be acquired for a range of use cases, namely

- Workload protection across on-premises and cloud environments. Starting by building a profile of what constitutes normal behavior for a given workload, the platform proceeds to implement segmentation based on that understanding, imposing the principle of least privilege. It then continuously monitors to detect anomalous activity and take remedial action in real time.

- File integrity monitoring, which actually goes beyond traditional files into configurations and binaries, enabling an organization to identify configuration tampering and malicious replacement.
- Service account behavior analytics, which aim to detect insider threats and/or account takeover exploits when a service account used by a sysadmin is compromised, giving attackers unrestricted access to move laterally across environments and access critical data.
- Workload hardening, whereby the platform performs adaptive profiling such that security teams can continuously validate configurations against CIS benchmarks and avoid risks finding their way into an environment.
- Microsegmenting environments, using behavior-based profiling of workloads to model normal access patterns and activities, then block abnormal ones.
- Container and Kubernetes security, protecting containers from compromise by baselining their runtime behavior to find anomalies and enabling a real-time response.

Most recently, the vendor has added a hosted version called TrueFort Cloud to enable an expansion further downmarket than the high-end enterprise customers it addresses with the TrueFort Platform.

Future plans

TrueFort's technology roadmap encompasses continued expansion in the cloud-native application arena, with the addition of service mesh support. The vendor also plans to expand its integrations with endpoint detection and response (EDR) vendors. It currently supports CrowdStrike agents, with the next EDR agents on its agenda being those from SentinelOne.

Beyond that, TrueFort plans to advance its current asset discovery capability, providing automatic fingerprinting probability and suggested protections.

Key facts

Table 1: Data sheet: TrueFort

Product/service name	• TrueFort Platform • TrueFort Cloud	**Product classification**	Workload protection, Microsegmentation
Version number	3.4.1	**Release date**	• December 2019 • April 2022
Industries covered	Financial services, healthcare, high tech, and the US federal government (no industry-specific blockers)	**Geographies covered**	Primarily North America (multiple customers in EMEA and Asia & Oceania)
Relevant company sizes	Primarily Enterprise today, TrueFort Cloud launched for mid-size expansion	**Licensing options**	Per-workload basis
URL	https://truefort.com/	**Routes to market**	Direct sales force, Founding technology partner for CrowdStrike Store, MSSPs for mid-market
Company headquarters	Weehawken, NJ, USA	**Number of employees**	105

Source: Omdia

Analyst comment

The microsegmentation concept is most immediately associated with two vendors, both of them founded in 2013, namely Illumio and Guardicore, with the latter being acquired by CDN market leader Akamai in September 2021. TrueFort was founded in 2015, launching its first product offering in 2019; therefore, it clearly entered the fray later, which has pros and cons.

On the plus side, it enables TrueFort to learn by its predecessors' mistakes and avoid some of their pitfalls. Indeed, the vendor argues that its technology has the built-in operational scalability that those agent- and rules-based approaches lack, referring to both their products as "shrunken host-based firewalls with blocklists" of who and what can't access the protected workload.

Meanwhile, the downside for later market entrants is, of course, that they must strive to gain visibility compared to the established players, who already enjoy mindshare within the target audience. This is not an impossible task, of course: Palo Alto Networks pulled it off when it came into a firewall market hitherto dominated by Check Point. It did so not only by launching more performant technology (the "application-aware" firewalls that could inspect traffic all the way up to Layer 7 of the OSI network stack) but also by cannily attaching it to an attention-grabbing new category name, the so-called "next-generation" class of firewalls.

TrueFort needs to create something that similarly fires the imagination of prospective customers, not to mention the chattering classes of IT, namely technology analysts and journalists. Of course, this cannot be just some hollow marketing exercise: if the vendor can convincingly demonstrate the prowess of its

technology vis-à-vis the incumbent players, it is well-placed to make serious inroads into the cloud workload protection market. This is particularly the case for TrueFort Cloud, which seeks to address a broader market than it has done with its previous offering.

The vendor's first foray into the market was for high-end enterprise customers, and it enjoyed success with a number of Tier 1 banks, where clearly the founders' own pedigree will have influenced the buying decision. To go broader and further downmarket, however, it needs to highlight its technology's advantages over those better-known competitors. It should be helped in this endeavor by the fact that it has other uses beyond microsegmentation, including FIM and the monitoring of service accounts.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Cloud security – IaaS and PaaS (December 2019)

Omdia Market Radar: Security Operations Solutions for Industrial IoT and OT, 2022 (October 2022)

"Cloudflare's Area 1 buy highlights CDNs pushing deeper into cybersecurity," February 2022

"Fortinet fills its zero trust access gap with OPAQ acquisition," (July 2020)

"Zscaler acquires Edgewise Networks for hybrid cloud data center security," (June 2020)

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com