SOLUTION BRIEF

Protecting both IT and OT environments against lateral movement attacks

The IT and OT domains have historically operated independently, each with distinct objectives, data-sharing needs, resource management approaches, and security protocols. However, as smarter systems (such as industrial, medical, and building technologies) continue to advance and the Internet of Things (IoT) gains widespread adoption, the OT environments face escalating risks due to deficiencies in their real-time situational awareness, risk assessment capabilities, and security practices. Consequently, it has become imperative to establish alignment between IT/ OT and IoT teams to achieve operational excellence and enhance the overall cybersecurity posture.

Modern enterprises encounter a range of complex challenges, such as zero-day vulnerabilities, increasing weaknesses in production applications, staffing shortages, and expanding regulatory demands. Despite the availability of tools and network segmentation solutions, there are limitations in effectively understanding enterprise applications and their communications in a secure manner. The integration of OT and IT environments within a single, flat network architecture further complicates matters by compromising visibility and control over communication flows between these interconnected environments.

Besides, organizations prioritize uptime over security, which exacerbates the existing difficulties. Adversaries exploit this priority by specifically targeting both OT and IT environments, taking advantage of vulnerabilities and discreetly moving undetected between them. Consequently, enterprises struggle to attain sufficient visibility and control to protect their systems and infrastructure from evolving threats.

TrueFort and Armis collaborate to establish robust security alignment by offering real-time visibility and control across IT, IoT, and OT environments, thereby enabling authorized communications exclusively. By leveraging their combined expertise, TrueFort and Armis facilitate a comprehensive mapping of all activities occurring within the production environment, encompassing IT, IoT, OT/ICS/IIoT, building management systems, and medical devices. This shared understanding of normal behavior ensures a holistic approach to security, empowering organizations to effectively monitor and manage their interconnected systems.

TrueFort leverages its advanced capabilities to discover and map applications, servers, and their interconnections within IT environments.

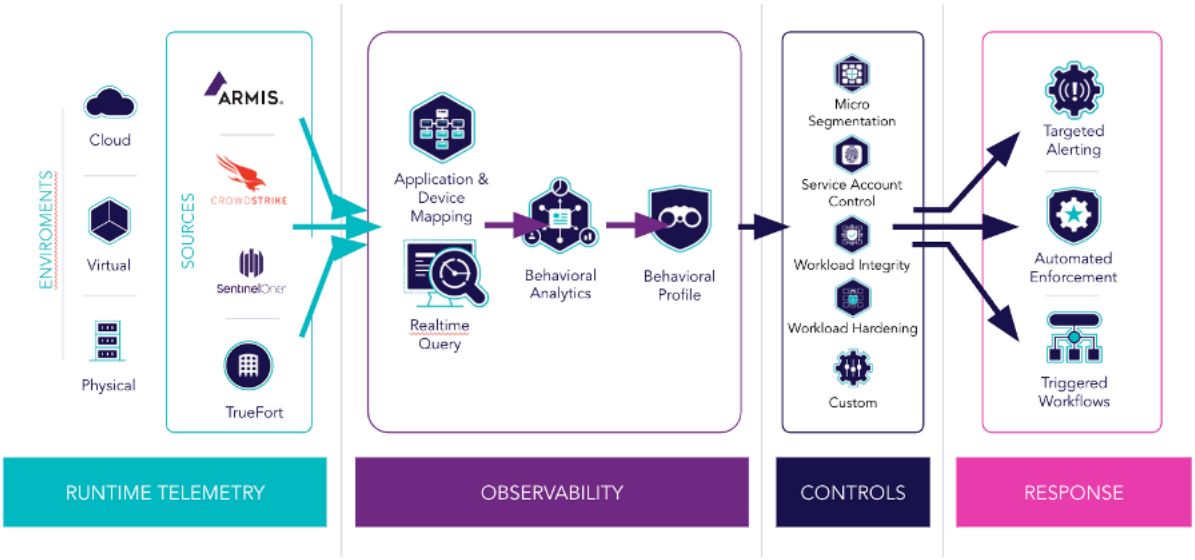
Challenges

- East/West traffic poses a risk as unmonitored communication occurs across different environments.
- Deployment of embedded systems with default or hardcoded credentials exposes vulnerabilities.
- Lack of monitoring for service account credentials increases the potential for unauthorized access.
- Applications communicating with unmanaged assets, servers, and external entities pose security risks.
- Unpatched, outdated, and misconfigured software/firmware create vulnerabilities within the network.
- Unauthorized insider access to systems and applications increases the risk of unauthorized actions and data breaches.

This is achieved by collecting telemetry data from the existing agents of leading cybersecurity solutions such as CrowdStrike, SentinelOne, and TrueFort itself.

Armis, on the other hand, employs agentless technology to perform network discovery, inventory management, and relationship mapping of devices across IT, IoT, and OT environments. This valuable information is then seamlessly integrated into the TrueFort Platform, enhancing the device information available for comprehensive analysis and protection.

How it works



Key Capabilities

- Implement microsegmentation within environments to enforce authorization for specific communication flows.
- Utilize application and network intelligence to effectively safeguard against lateral movement, reducing the reliance on costly legacy firewalls.
- Leverage the agentless solution provided by Armis, along with a combination of TrueFort, CrowdStrike, and SentinelOne agents, to comprehensively discover applications, workloads, devices, and their communications.
- Enhance the device information in TrueFort by integrating device intelligence obtained from Armis.
- Map the applications within IT environments, as well as track incoming and outgoing connections from IoT and OT sources.
- Gain a comprehensive understanding of communication flow behavior to establish baselines for acceptable interactions.
- Generate alerts for behavioral and configuration anomalies, preventing potential exploits and lateral movement.
- Discover both on-network and off-network devices to maintain an accurate inventory and monitor device status.
- Combine detailed device version and configuration information, network relationships, and application context for a holistic view of the environment.

TrueFort and Armis provide comprehensive protection for a wide range of assets by establishing intelligent baselines of normal, high-volume activities within and between applications. This approach ensures that future behavior is limited to trusted actions, effectively preventing compromise and reducing overall risk. By gaining valuable insights into the application environment, organizations can efficiently decrease the attack surface through the implementation of microsegmentation.

To address the dynamic landscape of IT, OT, and IoT devices, automatic identification and real-time profiling are crucial for detecting unusual behavior and promptly alerting on any anomalies. With the combined capabilities of TrueFort and Armis, organizations can effectively discover, comprehend, and enforce communication flows across these interconnected environments. This collaborative approach ensures definitive visibility and control, allowing only authorized communication while thwarting unauthorized access attempts by adversaries.

Furthermore, a deep understanding of the environment empowers organizations to implement robust mitigating controls, safeguard vulnerabilities, and enforce microsegmentation to effectively control lateral movement. Streamlining the microsegmentation journey becomes feasible through comprehensive inventorying of systems, software, and communications, enabling organizations to optimize their security measures.

Key Benefits

- Achieve comprehensive discovery of all assets, including applications, devices, service accounts, and infrastructure, within a single day using a combination of existing agents and agentless technology.
- Develop a deep understanding of workload behavior and establish mappings to specific applications, enabling the establishment of baselines for normal operations. This provides the necessary confidence to make informed decisions regarding blocking, disabling, and terminating certain actions.
- Implement granular enforcement measures by account and action, with the option to either push enforcement to host firewalls or utilize the TrueFort agent for blocking purposes. This approach ensures a robust and tailored enforcement strategy based on the specific needs of the organization.

About Armis

Armis, the leading asset visibility and security company, provides the industry's first unified asset intelligence platform designed to address the new extended attack surface that connected assets create. Fortune 100 companies trust our real-time and continuous protection to see with full context all managed, unmanaged assets across IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G. Armis provides passive cyber asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in California.

1.888.452.4011 | armis.com

About TrueFort

TrueFort Fortress is the real-time zero trust application protection platform that is purpose-built to secure dynamic and complex application environments cloud-to-ground, leveraging CrowdStrike telemetry, advanced behavioral analysis, machine intelligence and automation to reduce excessive trust and related risks.