IoT and Digitalization

SPARK Matrix™: Operational Technology (OT) Security, Q4 2023

Market Insights, Competitive Evaluation, and Vendor Rankings

December, 2023

TABLE OF CONTENTS

Executive Overview

This research service includes a detailed analysis of global Operational Technology (OT) security market dynamics, major trends, vendor landscape, and competitive positioning analysis. The study provides competition analysis and ranking of the leading Operational Technology (OT) vendors in the form of the SPARK Matrix. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors capabilities, competitive differentiation, and its market position.

Market Dynamics and Overview

Quadrant Knowledge Solutions defines OT security as "the holistic process of protecting assets, people, and information that governs any enterprise and uses operational technology (OT) & information technology (IT) through a suite of hardware and software that monitor, detects, respond and mitigate threats in the industrial environment. OT security encompasses a comprehensive set of practices and technologies that protect physical processes, devices, and industrial infrastructure to ensure total cyber resilience. It is designed to address the unique security needs of OT through the understanding of OT-specific protocols and the defense against cyberattacks targeting legacy & modern systems commonly employed in the OT ecosystem."

The terminology operational technology (OT) collectively represents all the hardware and associated instrumentation that helps monitor, regulate, and command a chain of industry-specific operations. The OT includes devices, systems, networks, and controls that automate industrial processes by governing its critical infrastructure. The common types of OT include Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, and Distributed Control Systems (DCS). The convergence of OT/IT in the industrial sector created a need for incorporating security in the industrial environment to mitigate and stop cyber-based attacks on OT assets. The vendors pertaining to the OT security market ensure that all the OT assets are continuously monitored for threats & anomalies. They provide visibility and defend & promote mitigation strategies to overcome cyber security challenges. Integrating IT with OT increased operational efficiency and paved the way for new capabilities, such as gaining visibility, connectivity, remote access, and new OT security protocols. The integration also created network protocols as the market demanded protection against vulnerabilities. These advancements propelled the demand for specialized OT security solutions that would protect against unauthorized access, data breaches, and disruptions to critical operations.

The Industrial Internet of Things (IIoT) technology within Industry 4.0 utilizes both OT & IT systems to operate in the industrial environment. The OT assets require a different approach to governance & security. It requires domain expertise and knowledge to fully comprehend the functionalities of OT assets. The OT security vendors in the market are continuously trying to bridge the gap for IT/OT convergence due to the interoperability and optimization of data transfer between its machines, infrastructure, assets, and applications.

The vendors in the OT security market provide overall security coverage to all OT assets connected to the industrial environment by continuously improving their current capabilities, such as gaining overall asset visibility, vulnerability management, use of artificial intelligence & machine learning for threat detection, and advanced threat mitigation strategies. The OT security landscape is being shaped by regulatory and protocol coverage. Governments and industry regulatory bodies are instituting stringent standards to improve the resilience and security of critical infrastructures and ensure total cyber resilience. Thereby, there is an increase in the adoption of OT security solutions that not only respond to immediate threats but also align with industry-specific regulatory frameworks. The end-user's requirements from the OT security vendors include ease of usage, overall security coverage, extended services, flexible deployment, and return on investments. As the threats rapidly progress in the OT market, vendors are utilizing resources and market research to constantly update emerging threats and vulnerabilities.

The future of OT security is promising as its technological advancements continue to address current challenges, vulnerabilities, and threats that emerge in the industrial environment. Anticipated developments in the OT security market include the increased use of artificial intelligence and machine learning for threat detection, further refinement of IoT device security, and the continued evolution of regulatory frameworks to keep pace with emerging cyber threats.

In conclusion, the OT security landscape is evolving in response to the intricate interplay between industrial processes and cybersecurity threats. As industries embrace digital transformation, the role of OT security becomes increasingly pivotal in safeguarding critical infrastructures. The trajectory of this market emphasizes the need for adaptive, integrated, and innovative solutions that can secure the complex and interconnected systems defining modern industrial operations.

Based on the analysis of the OT security market, a detailed description of the requisite key capabilities is listed below:

- **Asset Inventory:** Asset inventory is the accurate and timely accumulation of system data in OT environments. The asset inventory uses information pertaining to hardware data from both on and off the network, such as internet protocol (IP) address, serial number, and storage information, and software data, such as operating system (OS),

firmware, asset details, and location & vulnerability information, to provide greater insights in the OT environment.

Asset inventory utilizes improved 3D visibility, safe querying and parsing technology, endpoint management, and risk remediation & scoring to build a robust cybersecurity platform. Asset inventory enables the monitoring of active and/or passive assets. In passive monitoring, devices are classified based on their behavior, as either OT, ICS, IT, or IoT devices, and later monitored without interacting or intervening with their normal function. In active monitoring, device interaction takes place to receive in-depth information on the operating histories of the device. The asset inventory capability of the OT security platforms leverages asset discovery to have a common view of all assets in an organized way and provide complete visibility over assets. Asset inventory acts as a foundation for OT security by providing patch management, secure configurations, and robust recovery and building programs for OT/ICS environments.

Asset inventory enables the creation of a profile with a complete history of each device and provides a comprehensive visualization of the digital ecosystem. Asset inventory provides capabilities such as a threat visualizer for 3D representation of the digital workflows, network mapping to map all the internal and external endpoints, and creating facilities to watch drill-down OT device activities in real time. Asset inventory can also create alerts to eliminate the risk of potential cyber incidents when changes are made to hardware or software.

- **Asset Visibility:** Asset visibility provides the ability to visualize and track assets so that operators can make better-informed decisions on the operating device. Asset visibility facilitates protocol dissection, asset identification, zone mapping, historical timeline views, data synchronization, import/export capabilities, packet inspection, and device communications analysis. It provides a comprehensive asset inventory for effective industrial cybersecurity operations.

- **Vulnerability Management:** The vulnerability management capability in the OT/ ICS industrial environment assists business processes in identifying, prioritizing, and mitigating software vulnerabilities and threats in the OT endpoints. The capability facilitates end-to-end

vulnerability management using tools and strategies designed by vendors. A holistic vulnerability management capability identifies and assesses all the assets connected to the network, prioritizes the risks & impact, and offers remediation/mitigation strategies through configuration, firmware updating, and patch management. The vendors keep track of vulnerabilities through centralized repositories, such as common vulnerabilities & exposure (CVEs), National Vulnerability Database (NVD), and National Institute of Standards and Technology (NIST) Cyber security, along with its internal research database of all possible threats, and prioritize them based on the risk factors.

- **Threat Detection:** The threat detection capability detects and recognizes the frequency of threats along with their impact. It monitors a wide spectrum of assets in the industrial network and streamlines threats through monitoring device communication and data transfer. Using security information and event management (SIEM), it provides insights and analytics that mitigate cyberattacks in IT/OT environments.

  The capability helps detect threats, operational anomalies, and compliance gaps. It directs real-time endpoint data of all the assets in the network through its deep integration and advanced machine-learning solutions for unified alert systems, domain-specific threat intelligence, and industry-wide integrations. Threat detections in some OT/ICS security platforms are mapped as tactics and techniques in MITRE ATT&CK for OT to provide in-depth information and context about specific threats and help reduce threat discovery time, false positives, and alert fatigue.

- **Threat Hunting:** Threat hunting capability is a proactive countermeasure that is used during the early stages of the threat detection process to detect and mitigate the threat before the attack is compromised. Threat hunting assists end-users in discovering threats in the OT network using tools that analyze endpoints, data, assets, behavior, and applications in the industrial network. With human intervention, a dedicated team, and resources, it helps localize threats and deploy countermeasures effectively. The OT security solution detects both cyber and operational anomalies and provides contextual information, such as threat intel and playbooks, to improve incident response times.

- **Network Segmentation:** Network segmentation capability divides the network into different isolated segments by defining the perimeter. Each of the segments function independently with unique access and control for better performance, governance, and security. The segments are created physically using gateways or firewalls or virtually through software and micro-segmentation. The capability creates visibility of the assets by monitoring their behavioral patterns. It refines and enforces standards and policies into the infrastructure without hindering operations of assets. The capability is governed by its architecture and standards, such as Purdue Enterprise Reference Architecture (PERA),), and network access control (NAC).

  The vendors in the OT security market also adopt a zero-trust strategy based on user, device, and application identities, along with a next-generation firewall (NGFW). Zero-trust imposes and validates access control at the moment of access, in contrast to network access restrictions that are dependent on factors such as source and destination internet protocol (IP) addresses, protocols, and port numbers. The end users can profile assets based on attributes such as type, communication method, or current subnet and integrate assets into the network infrastructure using asset communications protocols, thereby creating easy governance of industrial assets.

- **Risk Assessment & Prioritization:** The risk assessment & prioritization capability assess all the industrial assets connected to the OT environment based on the priority or criticality of the asset and potential cybersecurity exposure of the asset. The risk in the network is predefined based on the prioritizing score allocated to it. These quantitative scores provide quantifiable and actionable recommendations to help users prioritize risk reduction efforts. The risk scores can also be weighted in terms of priority, depending on a user's unique needs and goals. OT/ICS security vendors use 360-degree risk assessment tools with a full software inventory that integrates all elements of endpoint security into a single database. They enable customers to identify and deploy compensating controls to achieve risk reduction and create overall OT asset visibility & communication.

- **Secure Remote Access (SRA):** The secure remote access capability enables configuration and control of OT assets within the industrial

network. The capability promotes secure access to industrial environments for both internal and third-party users and improves security with its architecture through role-based access control. The SRA enables remote maintenance and administration supported by firewalls, encryptions, access controls, and authentication. Vendors also offer SRA with zero-trust architecture to support role & policy-based access, secure authentication, and secure workflow processes.

- **OT Protocol Coverage:** The OT security solutions are governed by international security protocols that have a requisite prebuilt framework for compliance in the architecture. The vendors incorporate industry protocols and vendor-specific protocols specially designed for industrial applications into their OT security solutions. Some of the protocols in the OT/ICS security market include RS-232 and RS-485, Modbus, DNP3, highway addressable remote transducer (HART), TASE 2.0 and ICCP, common industry protocol (CIP), PROFIBUS and PROFINET, FOUNDATION Fieldbus, and building automation and control (BACnet). By providing in-depth coverage, OT security solutions can also detect anomalous activities, prevent unauthorized access, and mitigate potential threats within the communication frameworks of industrial networks.

  This capability is integral for enhancing the resilience of critical OT security infrastructure and incorporating the specific communication protocols that underpin operational processes in an industrial environment.

- **Response & Threat Mitigation:** The threat mitigation capability is deployed as the final process to fix or countermeasure against the identified threat. The mode of debugging or network protection is chosen by vendors or organizations based on research and historical analysis through basic functionalities, such as patch & configuration management. Based on the priority of risk, the OT security software suggests mitigation strategies that may or may not require human intervention.

- **Mode of Deployment:** The standard options for OT security deployment are cloud, on-premise, or hybrid software as a service (SaaS). Vendors deploy through the cloud by leveraging their dedicated partnership

with other leading cloud infrastructure providers to ease scalability and flexibility for their clients. Vendors also provide on-premise development options suitable for end-users lacking support for cloud infrastructure.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of the major OT Security vendors by evaluating their products, market presence, and value proposition. The evaluation was based on primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall OT security. This study mainly includes an analysis of various key vendors, which are as follows: Armis, BeyondTrust, Cisco, Claroty, Darktrace, DeNexus, Dragos, Forescout Technologies, Fortinet, Microsoft, Mission Secure, Nozomi Networks, OPSWAT, Ordr, Otorio, Palo Alto Networks, Phosphorus Cybersecurity, Radiflow, SCADAfence, Tenable, Verve Industrial (A Rockwell Automation Company), Waterfall Security Solutions, and Xage Security.

Armis, BeyondTrust, Claroty, Darktrace, Dragos, Forescout Technologies, Microsoft, Nozomi Networks, Tenable, and Verve Industrial are the top performers in the global OT security market. All the vendors mentioned above have been positioned as the SPARK Matrix™ leaders as per Quadrant's research on OT security.

Armis Centrix™, a cyber exposure management platform powered by Armis's AI-driven Asset Intelligence Engine, oversees, secures, protects, and manages a wide range of assets in real time. The cloud-based platform proactively mitigates all cyber asset risks, remediates vulnerabilities, blocks threats, and protects the entire attack surface. Armis Centrix™ offers solutions for asset management and security, OT/IoT security, medical device security, vulnerability prioritization & remediation, and managed threat services through its platform.

BeyondTrust's Privileged Access Management (PAM) solution empowers organizations to secure and manage their access to credentials and assets. Its integrated products and platform offer PAM solutions that enable organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments. BeyondTrust enables organizations to secure industrial networks without disrupting operations, compromising safety, or risking non-compliance. The BeyondTrust platform helps organizations gain complete visibility through remote operational technology (OT) access and secured vendor access. It also manages all privileged identities, accounts, and credentials and enables network segmentation and micro-segmentation, improving overall OT security.

Claroty's xDome is a modular SaaS-based cybersecurity platform that offers security to operational technology (OT) and industrial xIoT assets. It offers asset visibility, vulnerability management, and automated threat detection capabilities. Claroty provides customer-centric security solutions that offer comprehensive cybersecurity and operational resilience for vulnerability & risk management, network protection, threat detection, asset management, lifecycle management, operational intelligence, and remote access. The company's robust integration ecosystem and application programmable interface (API) provide use case-specific security solutions with dedicated frameworks for its end users.

Darktrace Cyber AI Loop is an adaptive feedback system that creates a virtuous cycle for each capability to interact, strengthen, and harden the security ecosystem. Darktrace PREVENT is a proactive AI engine that predicts and pre-empts the highest priority cyber-attacks, including both internal and external attacks. Darktrace DETECT+RESPOND is a self-learning AI that adapts to the unique footprints of an organization's operations to identify any unusual behavior that could indicate an attack. It responds instantly to any attacks detected and continuously feeds insights into Darktrace PREVENT to strengthen its AI Loop. Darktrace HEAL ensures that organizations can adapt when an incident occurs and recover by feeding back information to strengthen the overall ecosystem.

The Dragos Platform is an OT/ICS cybersecurity technology that provides comprehensive asset visibility into ICS/OT assets and communications. It detects threats using intelligence-driven analytics, assesses vulnerabilities, and offers playbooks for investigating and responding to threats. It equips security teams with technology and intelligence to counter industrial adversaries. Its core product offers asset & inventory visibility, vulnerability management, and threat detection. It offers on-premises deployment through hardware appliances, virtual setups, and cloud delivery managed by Dragos. Dragos's architecture consists of components such as the CentralStore, SiteStore, network sensors, and protocol & vendor support for flexible deployment options for both physical and virtual environments to bridge the gap between OT and IT environments.

Forescout Technologies's Continuum platform provides automated 360-degree asset visibility that helps organizations discover and continuously assess compliance & risk, govern the entire network for vulnerabilities, and offer proactive remediation. It also offers continuous asset governance and monitors OT network devices for threats and anomalies. Its wide product portfolio includes Forescout XDR, eyeSight, eyeInspect, eyeSegment, eyeControl, and eyeExtend. Forescout

Technologies enables ongoing discovery of cyber assets across networks, offering complete visibility into OT/ICS networks to preemptively identify cyber threats. Its asset management and monitoring capability leverages asset discovery techniques to identify assets, their locations, cyber postures, and anomalies.

Microsoft's cybersecurity and OT security solutions, part of its extensive portfolio, encompass various offerings. Microsoft 365 Defender is a unified security solution designed to identify IoT and OT devices, vulnerabilities, and threats. It provides enhanced visibility to complex, multistage attacks on industrial IoT, OT, and ICS. Microsoft 365 Defender prevents and detects attacks across identities, endpoints, applications, e-mails, data, and cloud applications, offering extended detection and response capabilities. Microsoft Sentinel serves as a cloud-native security information and event management (SIEM) solution, providing a comprehensive view across enterprises. Microsoft 365 Defender for IoT employs agentless network layer monitoring and seamlessly integrates with both industrial equipment and Security Operation Center (SOC) tools.

Nozomi Networks offers comprehensive OT security solutions, Vantage™ and Guardian™, managed by its Central Management Console™ (CMC). It offers asset intelligence and threat intelligence services. Its add-on functionalities, such as smart polling and remote collectors, augment its security solution. Guardian™ provides complete OT/ICS network visibility through visualizations of asset inventory and network. It also provides automated vulnerability assessment by continuously monitoring all vendor assets and network communications. Nozomi Networks provides comprehensive functional capabilities for complete network visibility and monitoring, advanced detection, automated vulnerability assessment, and incident response for the ICS, IoT, and OT environments.

Tenable OT Security safeguards industrial and critical infrastructure by disrupting attack paths. Its capabilities include inventory management, asset tracking, threat detection at both device and network levels, vulnerability management, and configuration control. Tenable's OT security capabilities enhance visibility, security, and control across entire asset operations. Tenable OT Security also provides extensive security tools and reports for IT and OT security personnel. It offers unparalleled visibility into converged IT/OT operations, delivering deep situational awareness across all sites and their respective OT assets, ranging from Windows servers to PLC backplanes through a unified interface.

Verve Industrial (A Rockwell Automation Company) is a specialized provider of OT security solutions. The Verve Security Center (VSC) platform offers

comprehensive capabilities for integrated endpoint management. It provides visibility, alert discovery, investigation, dynamic updating, and compliance capabilities for large enterprises. Verve offers Design 4 Defense services and managed protection services for an integrated OT security approach. Its Design 4 Defense services offer network design, segmentation, and monitoring capabilities and a roadmap for addressing security vulnerabilities. Its managed protection services offer routine maintenance, patch management, security and compliance monitoring, and expert on-call advice.

The strong contenders in the OT security SPARK Matrix include vendors, namely Cisco, Fortinet, Mission Secure, OPSWAT, Ordr, Otorio, Palo Alto Networks, Radilflow, SCADAfence, Waterfall Security Solutions, and Xage Security. The aspirants in the OT Security SPARK Matrix are DeNexus and Phosphorous Cybersecurity.

The above vendors in the strong contenders category offer industry-specific OT security solutions that address every client's specific requirements. These vendors offer extensive OT security capabilities backed up with extensive research and domain expertise in the security domain. The OT security solutions offered by these vendors are comprehensive and address new threats and vulnerabilities with assistance from emerging technology. The vendors also capture a large segment with a roadmap to be technology leaders in the OT security marketplace.

Key Competitive Factors and Technology Differentiators

The following are the key competitive factors and differentiators for the evaluation of OT security vendors. While most OT security vendors may provide all the core functionalities, the breadth and depth of functionalities may differ from vendor to vendor. Driven by increasing competition, vendors are increasingly looking at improving their OT security capabilities and overall value proposition to remain competitive. Some of the key differentiators include:

Threat Intelligence: The incorporation of threat intelligence capability is crucial for industrial organizations to safeguard the security and reliability of their OT infrastructure. Vendors must offer a holistic strategy for securing the OT environment by integrating security measures directly into the OT infrastructure. The OT security architecture should ensure secure communication, timely detection and response to security incidents, and the implementation of multiple layers of security controls. Vendor's offering must have the flexibility and scalability to adapt to future changes in the OT environment. The threat intelligence offered by vendors must also provide high-level information about threat mitigation strategies to its users. It must also enable them to detect all known and unknown threats using OT threat intelligence and behavior analytics. The organizations must look for vendors that offer Threat intelligence capability as part of their offering that has a significant impact on developing a holistic security approach

Integration and Interoperability: Integration and interoperability capability in OT security solutions serve as a unified defense against cyber threats in an industrial environment. Vendors must offer an integration and interoperability capability that not only optimizes the performance of individual security components but also ensures a collaborative and interoperable security landscape. It must help organizations adapt to the dynamic challenges posed by the modern industrial cybersecurity environment. It must offer seamless integration of diverse security solutions and interoperability between different components within an industrial network. This capability must also facilitate a smooth collaboration of security tools and enhance the overall efficacy of the cybersecurity infrastructure.

The vendor's interoperability capability must ensure that various security systems, such as firewalls, intrusion detection systems, and access control mechanisms, can communicate and share information effectively. Its interconnection capability must facilitate a synchronized response to potential threats, enabling a more

comprehensive and coordinated defense strategy. Organizations must opt for vendors whose integration and interoperability capability addresses the evolving landscape of industrial environments where disparate devices, protocols, and applications coexist.

IT/OT Unified Protection: The IT/OT unified protection capability for OT security provides a comprehensive solution for both IT and OT environments. The merging of IT and OT systems introduces challenges, as traditional IT security solutions may not effectively secure OT systems. A unified security platform offered by vendors must integrate IT and OT security measures to offer complete visibility across the entire infrastructure. It must enable organizations to detect and respond to security incidents in real time. Organizations must identify vendors that understand the entire IT/OT environment, can identify potential vulnerabilities, and offer structured change management processes for new threats to attain unified protection.

Real-Time Monitoring: Real-time monitoring capability in OT security solutions enables active observation of the OT environment to identify and address security incidents promptly. Vendors offering this capability must have the ability to utilize applications and tools to continuously capture snapshots of the network's performance. By tracking network activity, the vendor must be able to promptly identify potential issues and enhance network security. The vendor must also offer complete visibility into the infrastructure, enabling organizations to respond to security incidents in real time. Organizations must determine vendors whose real-time monitoring capability serves as a dynamic and responsive mechanism and enables them to effectively safeguard their critical infrastructure in the face of the ever-evolving cybersecurity landscape.

Artificial Intelligence & Machine Learning Inclusion: Vendors in the OT security market must be capable of using proprietary machine learning & artificial intelligence (AI) algorithms and self-learning AI tools to detect and autonomously respond to all forms of cyber threats. They must have the ability to determine subtle insider threats, zero-day attacks, hacked IoT devices, automated threats, and misconfigurations. Organizations should assess the OT security vendor's ability to incorporate new technologies in their software for detecting advanced threats in the market.

Managed & Professional services: Some vendors in the OT security market extend their product portfolio by offering customized services and consulting.

The service portfolio offered by vendors must be powered by internal research and a partnership ecosystem that supports services designed to meet customer requirements. The vendors must have the capability to support specialized industry verticals, such as power, energy, utility, and defense. They must cover a wide range of industry protocols, security controls, regular auditing, and consulting & managed support in functions such as patching, vulnerability assessment, and compliance reporting. Organizations should assess the additional services provided by the vendors to utilize the fullest potential of the security solution.

Partnership Ecosystem: OT security vendors must have significant partnerships with top technology vendors to cater to multiple industries along with IoT vendors. There is a mutual relationship between the partner ecosystem and the effectiveness of a vendor solution since many of the important requirements for a vendor solution may depend on partner integrations. To strengthen their regional or worldwide footprint, certain vendors are collaborating with technology providers, system integrators & value-added resellers (VAR), managed solutions security providers, and global networks for distribution partners. Organizations are recommended to evaluate vendors based on their partner ecosystem for having a flexible solution. In the OT security market, the partnership ecosystem depends on technology collaboration, integration providers, cloud platform providers, and service providers. Therefore, organizations must carefully assess each OT security vendor's partner ecosystem and prefer vendors who leverage their partnership to offer multiple capabilities.

Domain Knowledge and Industry Experience: Organizations should evaluate the expertise and domain knowledge of OT security vendors to understand their ability to address unique and complex business challenges, use cases, and industry-specific requirements. Organizations must consider vendors' in-depth knowledge of a specific industry, such as how it is evolving, emerging trends, and factors that could influence the overall industry. Organizations should evaluate the vendor's offering based on its ease of use, comprehensiveness, and flexibility to adapt to dynamic market changes and regulatory requirements to minimize the total cost of ownership and transparency.

Vendors should be able to understand and uncover unmet business requirements, as well as bridge the technology and service gaps. Due to IT/OT convergence, organizations must also evaluate the vendor's ability to tailor to the needs & preferences of their business. Organizations must opt for vendors that offer advanced threat detection, secure remote access, third-party vendor management, device lifecycle management, vulnerability & risk management,

network segmentation, compliance & audit support, incident response, asset & change management, and performance measurement & reporting. While assessing the best practices for OT security solution deployments, organizations should look for a solution with a history of successful large-scale deployments and carefully analyze the existing case studies of those deployments.

Ability to support use cases: Organizations should evaluate the ability of the vendor's OT/ICS security solution to support a wide range of industry-specific and organization-specific use cases. Vendors must offer modular and tailored specific solutions for industries such as manufacturing, healthcare, commercial, public sector, and defense. OT security vendors must offer a platform that supports a wide range of protocols along with industry-specific compliance and environmental requirements.

Vendor's Product Strategy and Roadmap: OT security vendors are constantly evolving to accommodate ongoing and emerging technology disruptions and market trends and identify new threats in the market. Vendors must have the ability to leverage their domain expertise and partnerships to formulate strategies and roadmaps that enhance the capabilities of OT security. In the long run, they must cater to a wider variety of industry verticals. Therefore, organizations should carefully evaluate the product strategy & roadmap of each vendor before finalizing on any OT security vendor.

Pricing Model: Organizations should carefully evaluate the competitive pricing model of potential OT security vendors. They should prefer OT security vendors who offer a flexible pricing structure and the highest value relative to the cost. Some vendors in the OT market offer pricing based on subscriptions and the number of devices or customized pricing based on customer use cases.

SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix™ provides a snapshot of the market positioning of the key market participants. SPARK Matrix™ provides a visual representation of market participants and provides strategic insights on how each supplier ranks related to their competitors concerning various performance parameters based on the category of technology excellence and customer impact. Quadrant's Competitive Landscape Analysis is a useful planning guide for strategic decision-making, such as finding M&A prospects, partnerships, geographical expansion, portfolio expansion, and similar others.

Each market participant is analyzed against several parameters of Technology Excellence and Customer Impact. In each of the parameters (see charts), an index is assigned to each supplier from 1 (lowest) to 10 (highest). These ratings are designated to each market participant based on the research findings. Based on the individual participant ratings, X and Y coordinate values are calculated. These coordinates are finally used to make the SPARK Matrix.

Technology Excellence	Weightage
Asset Visibility & Management	15%
Vulnerability & Risk Management	10%
Application Management	10%
Threat Detection & Mitigation	20%
Protocol Coverage	5%
Network Topology Mapping	10%
Analytics & Dashboard	5%
Application Diversity and Use Cases	5%
Competitive Differentiators	10%
Integration and Interoperability	5%
Vision & Roadmap	5%

Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Customer Service Excellence	15%
Unique Value Proposition	15%
Ease of deployment	15%

Evaluation Criteria: Technology Excellence

- **Asset Visibility & Management:** The ability to map & classify devices and identify real time location & accurate inventory of all devices present in the organization.

- **Vulnerability & Risk Management:** The ability to identify and rectify vulnerabilities associated with the industrial environment and offer assessments and prioritisation of risk.

- **Application Management:** The ability to perform specialized operations and industrial processes through data collection, device management, and command execution.

- **Threat Detection & Mitigation:** The ability to detect threats, operational anomalies, and compliance gaps and ensure identified threat mitigation through patch and configuration management

- **Protocol Coverage:** The ability to incorporate industry and vendor-specific protocols, such as RS-232, RS-485, Modbus, DNP3, and PROFIBUS.

- **Network Topology Mapping:** The ability to offer network segments for performance, governance, and security using gateways and firewalls; secure remote access to both internal and 3rd-party users; and network and endpoint security to protect devices from malicious threats and cyberattacks.

- **Analytics & Dashboard:** The ability to track the usage of devices to optimize performance and minimize risk. It also takes into account the ability to provide real-time reports on the dashboard regarding security threats and compliance with regulations.

- **Application Diversity and Use Cases:** The ability to demonstrate product deployment for a wide range of industry verticals with multiple use cases through integrated OT security solutions.

- **Competitive Differentiators:** The ability to differentiate from competitors through functional capabilities, innovations, GTM strategy, customer value proposition, and such others.

- **Integration & Interoperability:** The ability to offer a product and technology platform that supports integration with multiple best-of-breed technologies, provides prebuilt out-of-the-box integrations, and offers open API support and services.

- **Vision & Roadmap:** Evaluation of the vendor's product strategy and roadmap based on the analysis of key planned enhancements, products, and technology that improve the customer ownership experience.

Evaluation Criteria: Customer Impact

- **Product Strategy & Performance:** Evaluation of multiple aspects of product strategy and performance in terms of product availability, price to performance ratio, excellence in GTM strategy, and other product-specific parameters.

- **Market Presence:** The ability to demonstrate revenue, client base, and market growth along with a presence in various geographical regions and industry verticals.

- **Proven Record:** Evaluation of the existing client base from SMB, mid-market and large enterprise segment, growth rate, and analysis of the customer case studies.

- **Customer Service Excellence:** The ability to demonstrate vendors capability to provide a range of professional services from consulting, training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.

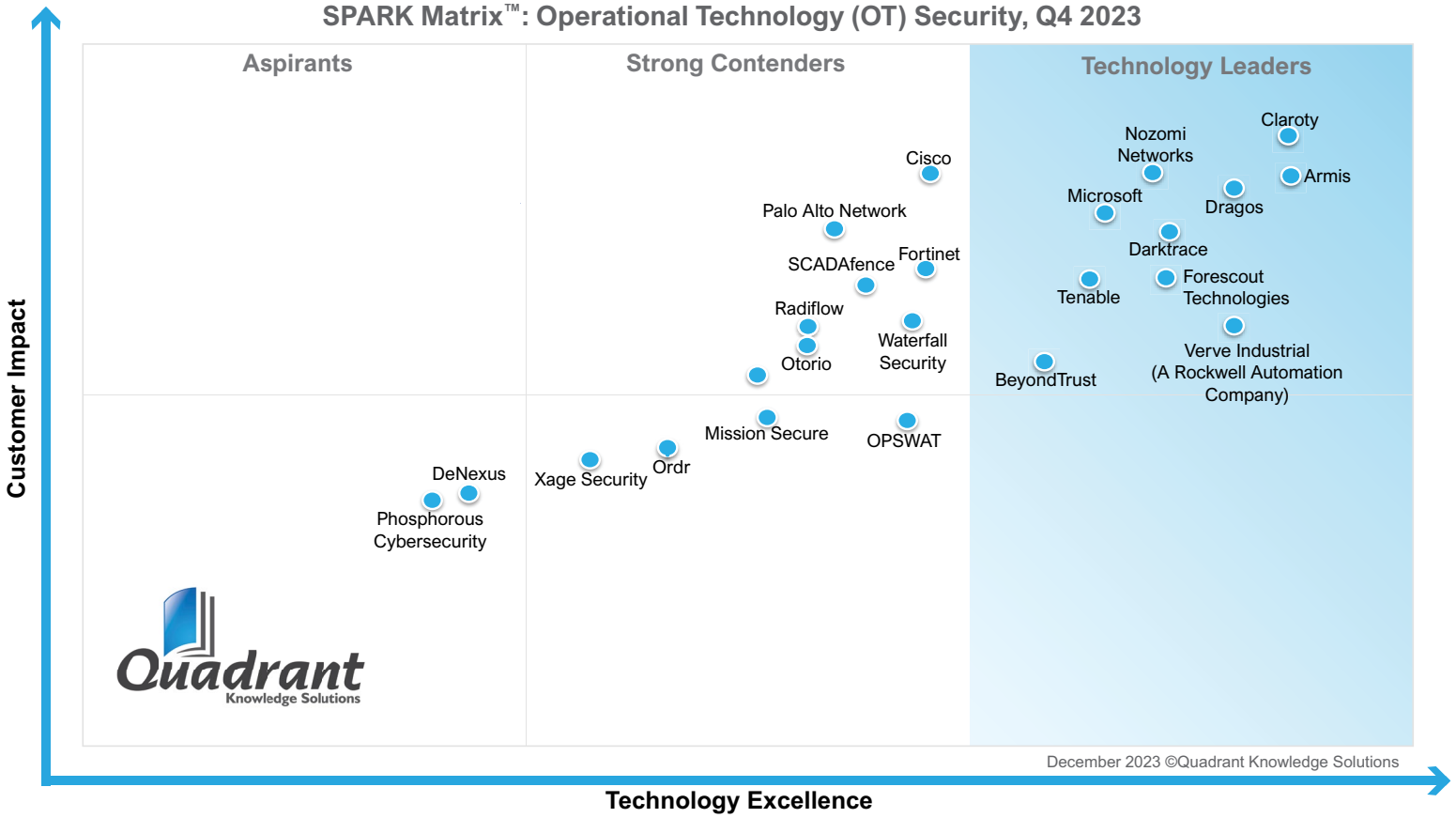
- **Unique Value Proposition:** The ability to demonstrate unique differentiators driven by ongoing industry trends, industry convergence, technology innovation, and such others.

- **Ease of Deployment & Use:** The ability to provide superior deployment experience to clients supporting flexible deployment or demonstrate superior purchase, implementation and usage experience. Additionally, vendors' products are analyzed to offer user-friendly UI and ownership experience.

SPARK Matrix™: Operational Technology (OT) Security, Q4 2023

Strategic Performance Assessment and Ranking

Figure: 2023 SPARK Matrix™
Strategic Performance Assessment and Ranking)
Operational Technology (OT) Security, Q4 2023



Vendor Profile

Following are the profiles of the leading OT security with a global impact. The following vendor profiles are written based on the information provided by the vendor's executives as part of the research process. Quadrant research team has also referred to the company's website, whitepapers, blogs, and other sources for writing the profile. A detailed vendor profile and analysis of all the vendors, along with various competitive scenarios, are available as a custom research deliverable to our clients. Users are advised to directly speak to respective vendors for a more comprehensive understanding of their technology capabilities. Users are advised to consult Quadrant Knowledge Solutions before making any purchase decisions, regarding OT security and vendor selection based on research findings included in this research service.

Armis

URL: http://armis.com

Company Introduction

Founded in 2015 and headquartered in San Francisco, CA, Armis offers a cyber exposure management platform powered by its AI-driven Asset Intelligence Engine. The platform, Armis Centrix™, sees, protects, and manages critical assets in real-time for IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G environments. For OT/IoT environments, Armis Centrix™ provides unparalleled visibility, continuous security, and deep insights across the converged IT/OT/IoT Attack Surface.

Product Introduction

Armis Centrix™ for OT/IoT security enables organizations to see and secure OT/IOT networks and physical assets, ensure uptime, and build an effective & comprehensive security strategy. It is powered by Armis's AI-driven Asset Intelligence Engine and oversees, secures, protects, and manages a wide range of assets in real time. The cloud-based platform proactively mitigates all cyber asset risks, remediates vulnerabilities, blocks threats, and protects the entire attack surface. Armis for OT/IoT security provides deep visibility to all OT assets as well as to the OT/ICS networks and environment. It allows companies to manage the OT/IT convergence, bridge the IT / OT gap and protect OT networks, monitor connectivity, and track behavior.

Technology Perspective

Following is the analysis of Armis's capabilities in the global OT security market:

- Armis Centrix™ for OT/IoT Security offers a cloud-native solution that has an extremely flexible deployment model with hardware or virtual collectors (appliances) and direct cloud-to-cloud integrations. Armis Centrix™ for OT/IoT Security first gathers a live inventory of all assets in the environment and provides a deep situational awareness, which includes the make and model of the asset as well as patch level and much more across IT, OT, IoT, and IoMT

devices. With this knowledge, Armis Centrix™ can identify vulnerabilities and, indicators of compromise (IOCs) through signature, anomaly-based detection, behavioral analysis, and abnormal asset activity. It helps organizations with the early detection of compromised devices and preventing the further spread of an attack. It also gathers and analyzes threat forensic data pre-, during, and post-incidents, enabling security teams to make informed, data-driven decisions and prioritize responses.

- Some of the key capabilities of Armis Centrix™ for OT/IoT Security include asset management, security access & control, vulnerability prioritization and remediation, domain expertise with extensive research, and the most coverage for managing, detecting, & responding to threats.

- Armis asset management capability leverages the existing security ecosystem through data aggregation from hundreds of sources through out-of-the-box pre-built integrations and agentless network traffic inspection. It performs full asset profiling, powered by its AI-driven Asset Intelligence Engine, offering robust protection of a wide variety of assets in real-time. Armis Centrix™, the cyber exposure management platform, uses its contextual knowledge to automatically generate network segmentation policies based on the needs of each device.

- Armis Centrix™ for OT/IoT Security employs a cloud-based threat detection engine that uses policies as well as behavioral analysis, machine learning, and AI to identify deviations. These deviations may result from misconfigurations, default settings, policy violations, and abnormal behaviors such as inappropriate connection requests, unusual software, or indications from threat intelligence to suggest device compromise. Armis Centrix™ Vulnerability Prioritization and Remediation enhances security by providing comprehensive vulnerability lifecycle management. It offers continuous monitoring, dashboards, and reports to detect, manage, track, and demonstrate improvements in the organization's security posture and ongoing vulnerability mitigation efforts.

- The key differentiators of Armis Centrix™ for OT/IoT Security include the AI-driven Armis Asset Intelligence Engine, its cloud-native architecture, partnership ecosystem, out-of-the-box-functionalities, threat detection engine, extensive integration library, and Armis Centrix™ Value Packs.

- Armis Centrix™ is an agentless SaaS platform authorized by FedRAMP and the US Department of Defense at Impact Level 4 (IL4). It has easy deployment and covers diverse assets, such as wired, wireless, managed, and unmanaged, spanning IT, IoT, IoMT, and OT. The platform's SaaS model ensures effortless management and continuous updation of the platform's enhancements and emerging threats based on the latest research data. Offering real-time threat detection and alerts, Armis Centrix™ enables swift responses to threats through automated security orchestration. The network monitoring technologies are safe for deployment in sensitive environments without causing network latency or stability issues.

- The top use cases of Armis Centrix™ for OT/IoT Security include unified visibility and security and control for OT environments. The platform identifies, monitors, optimizes, and secures all IT, OT, nested OT, IIoT, IOMT, SCADA, ICS, and BMS assets, systems, & processes in the industrial environment and ensures safe & reliable operation. In addition, it is used to protect OT networks, monitor connectivity, and track the behavior of all assets in the networks, which enables real-time threat detection, overall asset life cycle management, and risk assessments.

Market Perspective

Regarding geographical presence, Armis has a major presence in North America, Canada, UK/I, Germany, Italy, Spain, the Middle East, as well as a major presence in the public sector (SLED and FED), with its largest customer base in the USA and numerous international customers with global deployments. Regarding industry verticals, the company's primary verticals include energy & utilities, healthcare, manufacturing, retail, transportation, finance, education, and the public sector.

Challenges

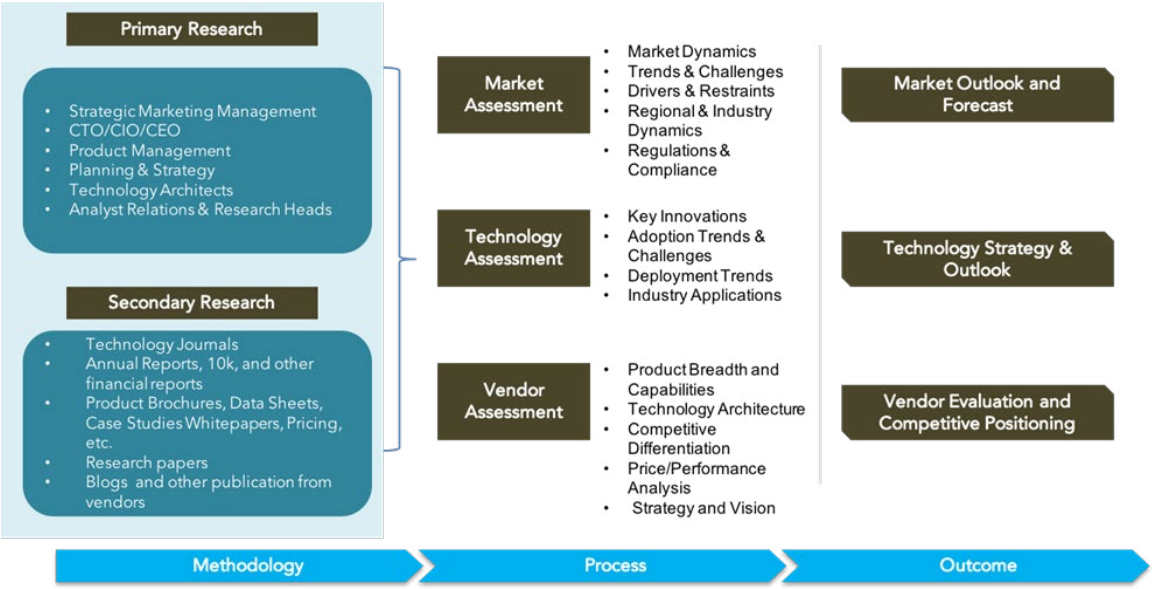
The key challenge Armis faces is the increasing competition from emerging and niche vendors in the OT market space with advanced capabilities to cater to a wide range of end users across the globe. However, Armis, with extensive capabilities in IT and OT security, powered by its AI engine & threat mitigation strategy, addresses a wider range of use cases

Roadmap

Armis roadmap focuses on the enhancement of capabilities for its current portfolio offerings. It also places a significant emphasis on expanding its verticals with geographic expansion strategies. Additionally, the organization is continuously expanding to cater to more use cases and industry-specific requirements in the OT market landscape.

Research Methodologies

Quadrant Knowledge Solutions uses a comprehensive approach to conduct global market outlook research for various technologies. Quadrant's research approach provides our analysts with the most effective framework to identify market and technology trends and helps in formulating meaningful growth strategies for our clients. All the sections of our research report are prepared with a considerable amount of time and thought process before moving on to the next step. Following is the brief description of the major sections of our research methodologies.



Secondary Research

Following are the major sources of information for conducting secondary research:

Quadrant's Internal Database

Quadrant Knowledge Solutions maintains a proprietary database in several technology marketplaces. This database provides our analyst with an adequate foundation to kick-start the research project. This database includes information from the following sources:

- Annual reports and other financial reports
- Industry participant lists
- Published secondary data on companies and their products

- Database of market sizes and forecast data for different market segments
- Major market and technology trends

Literature Research

Quadrant Knowledge Solutions leverages on several magazine subscriptions and other publications that cover a wide range of subjects related to technology research. We also use the extensive library of directories and Journals on various technology domains. Our analysts use blog posts, whitepapers, case studies, and other literature published by major technology vendors, online experts, and industry news publications.

Inputs from Industry Participants

Quadrant analysts collect relevant documents such as whitepaper, brochures, case studies, price lists, datasheet, and other reports from all major industry participants.

Primary Research

Quadrant analysts use a two-step process for conducting primary research that helps us in capturing meaningful and most accurate market information. Below is the two-step process of our primary research:

Market Estimation: Based on the top-down and bottom-up approach, our analyst analyses all industry participants to estimate their business in the technology market for various market segments. We also seek information and verification of client business performance as part of our primary research interviews or through a detailed market questionnaire. The Quadrant research team conducts a detailed analysis of the comments and inputs provided by the industry participants.

Client Interview: Quadrant analyst team conducts a detailed telephonic interview of all major industry participants to get their perspectives of the current and future market dynamics. Our analyst also gets their first-hand experience with the vendor's product demo to understand their technology capabilities, user experience, product features, and other aspects. Based on the requirements, Quadrant analysts interview with more than one person from each of the market participants to verify the accuracy of the information provided. We typically engage

with client personnel in one of the following functions:

- Strategic Marketing Management
- Product Management
- Product Planning
- Planning & Strategy

Feedback from Channel Partners and End Users

Quadrant research team researches with various sales channel partners, including distributors, system integrators, and consultants to understand the detailed perspective of the market. Our analysts also get feedback from end-users from multiple industries and geographical regions to understand key issues, technology trends, and supplier capabilities in the technology market.

Data Analysis: Market Forecast & Competition Analysis

Quadrant's analysts' team gathers all the necessary information from secondary research and primary research to a computer database. These databases are then analyzed, verified, and cross-tabulated in numerous ways to get the right picture of the overall market and its segments. After analyzing all the market data, industry trends, market trends, technology trends, and key issues, we prepare preliminary market forecasts. This preliminary market forecast is tested against several market scenarios and the most economical and accurate forecast scenario for the overall market and its segments.

In addition to market forecasts, our team conducts a detailed review of industry participants to prepare a competitive landscape and market positioning analysis for the overall market as well as for various market segments.

SPARK Matrix: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix representation provides a visual representation of market participants and provides strategic insights on how each supplier ranks in comparison to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact.

Final Report Preparation

After finalization of market analysis and forecasts, our analyst prepares necessary graphs, charts, and table to get further insights and preparation of the final research report. Our final research report includes information including market forecast; competitive analysis; major market & technology trends; market drivers; vendor profiles, and such others.

Client Support

For information on hard-copy or electronic reprints, please contact Client Support at

ajinkya@quadrant-solutions.com | www.quadrant-solutions.com