Knowledge Brief

Quadrant Knowledge Solutions

Safe-T is Emerging Leader in SPARK Matrix: Zero Trust Network Security (ZTNS), 2021

An Excerpt from Quadrant Knowledge Solutions
"SPARK Matrix: Zero Trust Network Security (ZTNS), 2021"

Safe-T is Emerging Leader in SPARK Matrix: Zero Trust Network Security (ZTNS), 2021

The Zero Trust framework became popular in the wake of data breaches and modern cyber-attacks. It contends that no entity, whether inside or outside a network perimeter should be trusted without verification. The conventional security practice focused on creating a network perimeter to defend resources and trust entities on the inside, where everything outside the perimeter was untrusted. This model assumed that those inside the perimeter are inherently trusted and gave them more unfettered access to internal resources. This model could not adapt to the dynamics of virtual and cloud computing, as well as the changing threat landscape with more advanced, coordinated outside attackers and malicious insiders trying to move laterally within the network perimeter to exploit important resources.

To address these challenges, the Zero Trust model treats all access requests without inherent trust and gives access permission on a strict need-to-know, least privilege basis. Traditional perimeter-based security models employ tools such as firewalls, that focus their defensive measures on checking entities originating outside the perimeter. This could give greater latitude to the users and devices within the networks, subnets, and virtual zones. Even if used for further network segmentation, employing multiple firewalls for internal segmentation can be cumbersome and challenging to scale.

Zero Trust Network Security is an approach in network security that safeguards user access to applications and information irrespective of the location, time, and nature of the device used. Zero Trust Network Security follows the Zero Trust approach, wherein the default network security posture is that of deny. Access is granted upon authenticating and authorizing both user and device. By pre-authorizing users and devices prior to making the application layer access (applications and resources), Zero Trust Network Security protects enterprises from a range of attacks, such as denial-of-service, credential theft, server exploitation, connection hijacking, and APT/Lateral movement. Unlike security models that work at the network layer, Zero Trust Network Security works to the application layer. It provides granular control for secure communications directly from the user and device to the application. Users are only allowed to see and access resources that they are authorized to access.

Quadrant Knowledge Solutions' Zero Trust Network Security (ZTNS) market research includes a detailed analysis of the global market regarding short-term and long-term growth opportunities, emerging technology trends, market trends, and future market outlook. The study provides a comprehensive market forecast analysis of the global market in various geographical regions and the overall market adoption rate as well. This research provides strategic information - for technology vendors to better understand the existing market, supporting their growth strategies; and for users to evaluate different vendors' capabilities, competitive differentiation, and market position.

The research includes a detailed competition analysis and vendor evaluation with the proprietary SPARK Matrix analysis. SPARK Matrix includes ranking and positioning of leading Zero Trust Network Security (ZTNS) vendors, with a global impact. The SPARK Matrix includes analysis of vendors, including Cisco, Okta, Akamai Technologies, Zscaler, Appgate, Ivanti, Perimeter 81, Zentera Systems, Safe-T, Broadcom, Palo Alto Networks, Check Point, Proofpoint, Forcepoint, Netskope, Unisys, InstaSafe, BlackRidge, NeuVector, and Waverley Labs.

Market Dynamics and Trends

The following are the key research findings of Quadrant's Zero Trust Network Security (ZTNS) research:

- Organizations are offering a higher level of mobility and flexibility to increase their employees' efficiency and productivity. This has resulted in the increasing popularity of IoT devices, and the BYOD and WYOD phenomenon in the enterprise network. Owing to the BYOD and WYOD phenomenon, more and more people are connecting their mobile devices like smartwatches, tablets, smartphones, and others to the enterprise network. This has increased the number of unsecured endpoints and expanded the attack surface. Organization needs an advanced security solution to protect IoT devices and devices utilizing BYOD and WYOD policies without hindering user experience. A Zero Trust solution solves this problem by following the principle of 'trust nothing, verify everything.' By ensuring that all users and devices are authenticated and authorized before permitting access, Zero Trust Solution secures the vast array of IoT & BYOD devices like never before.

- Data breaches, DDoS and ransomware attacks are not only increasing in frequency but also becoming more sophisticated and complex. The advancements in IT and security technologies are enabling cybercriminals to increasingly utilize advanced techniques to launch sophisticated, complex, and targeted attacks. For cybercriminals, the integrated power of IoT botnets, automation, AI and machine learning tools will enable them to cause the next wave of prominent attacks including DDoS attacks, unauthorized access to enterprise network and resources, and information theft. A Zero Trust Network Security solution addresses this problem by providing granular and contextual access control and performing continuous adaptive authentication. By making applications and resources invisible to unauthorized users and granting access post-authentication, ZTNS solutions drastically reduce network-based attacks.

- With the growing adoption of multi-cloud and hybrid IT environments organizations are looking at enhancing their threat defense measures to address ever-growing security risks, internal threats, external malware, and compliance requirements associated with hybrid IT infrastructure. A Zero Trust Network Security solution provides direct and secure access to public cloud applications & resources and hence is becoming the popular security measure for a hybrid IT environment.

- Numerous compliance frameworks, such as NIST, FISMA, HIPAA, PCI-DSS, and others, are significantly impacting the overall enterprise security strategies across industry verticals and geographical regions. While compliance with global, country, and industry regulations can help improve an organization's security posture, non-compliance can result in a higher risk of information theft, fines, liabilities, negative publicity, and more. A Zero Trust Solution can significantly help organizations ensure adherence to the ever-changing industry and regulatory compliance specifications. It improves compliance data collection, reporting, and auditing by centrally controlling secure connections between users and resources.

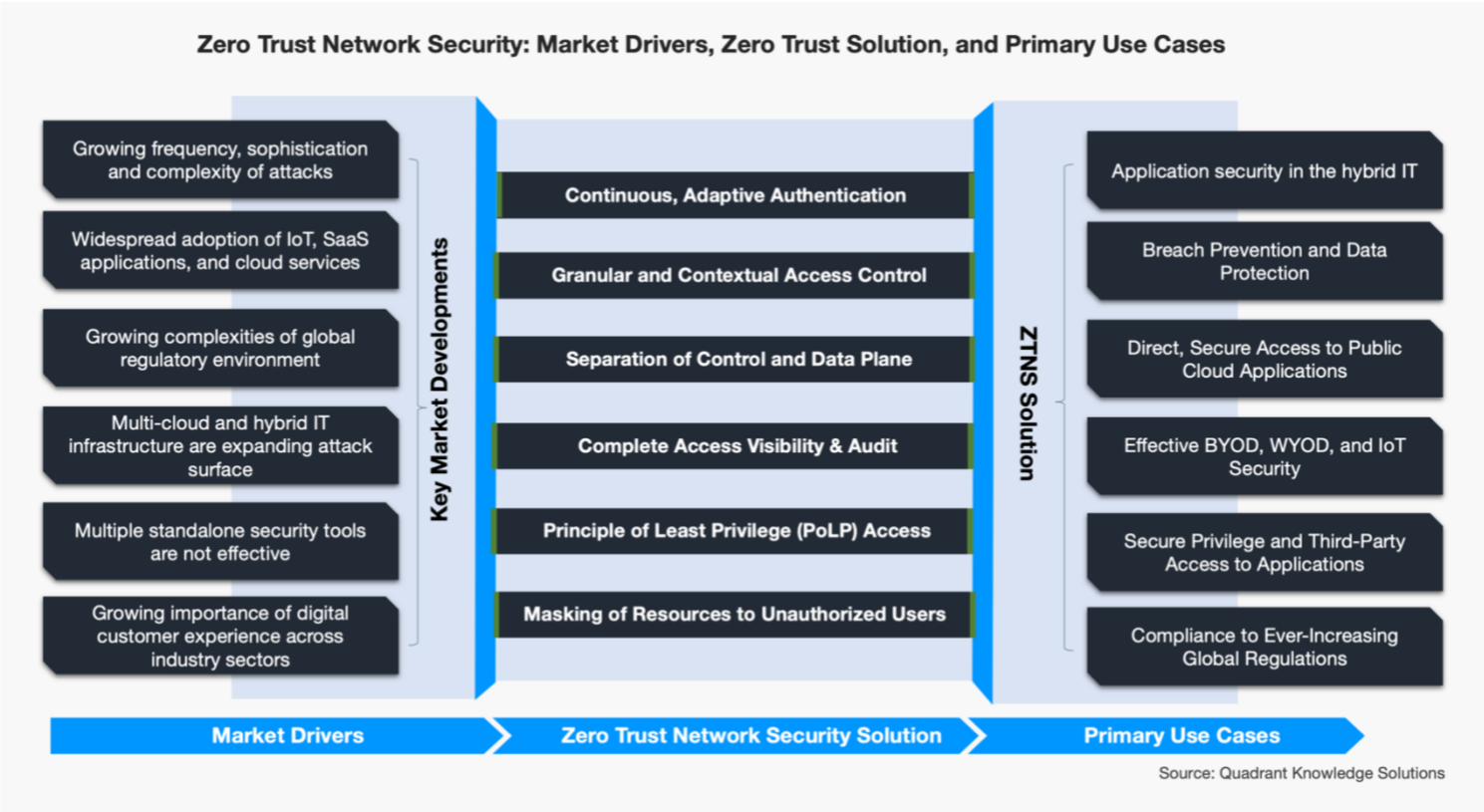
- The coronavirus outbreak has impacted the world's economy and driven the global workforce indoors. This increased remote working is creating its fair share of problems, with the biggest one being security. With the global organizations allowing work from home, employees/ vendors/ contractors are using their own devices and personal networks, which are not as secure as compared to corporate systems

and connections. Because of this, hackers are having a greater chance to gain access to sensitive organizational data. Driven by these challenges, Zero Trust Network Security solution is getting a lot of traction from organizations as it can provide secure access to applications and data in the cloud and on-premises. ZTNS provides flexible and modern cloud-based security to respond to the risks of remote users.

- With the rise in the remote workforce around the world and increasing attacks on VPNs, organizations are considering either augmenting their traditional VPNs or replacing them with zero trust solutions. Although VPN has been the preferred choice by organizations to provide secured remote access, its inherent perimeter methodology makes it particularly vulnerable to attackers. Not only traditional VPNs are falling short to protect today's complex networks with a huge mobile workforce, but they also offer low visibility for hybrid IT and multi-cloud environments. Organizations are either complementing or replacing their traditional VPNs with a more agile and granular security framework called zero trust.

- Driven by growing market opportunity, Zero Trust Network Security vendors are augmenting their zero-trust offering with enhanced security features and extending support for IoT and OT. Vendors are also ensuring that their solution is minimally disruptive to the existing infrastructure and operation and can seamlessly integrate and co-exist with other security solutions, and therefore does not need a rip-and-replace strategy.

Figure: A Framework for Holistic Zero Trust Network Security



SPARK Matrix Analysis of the Zero Trust Network Security (ZTNS) Market

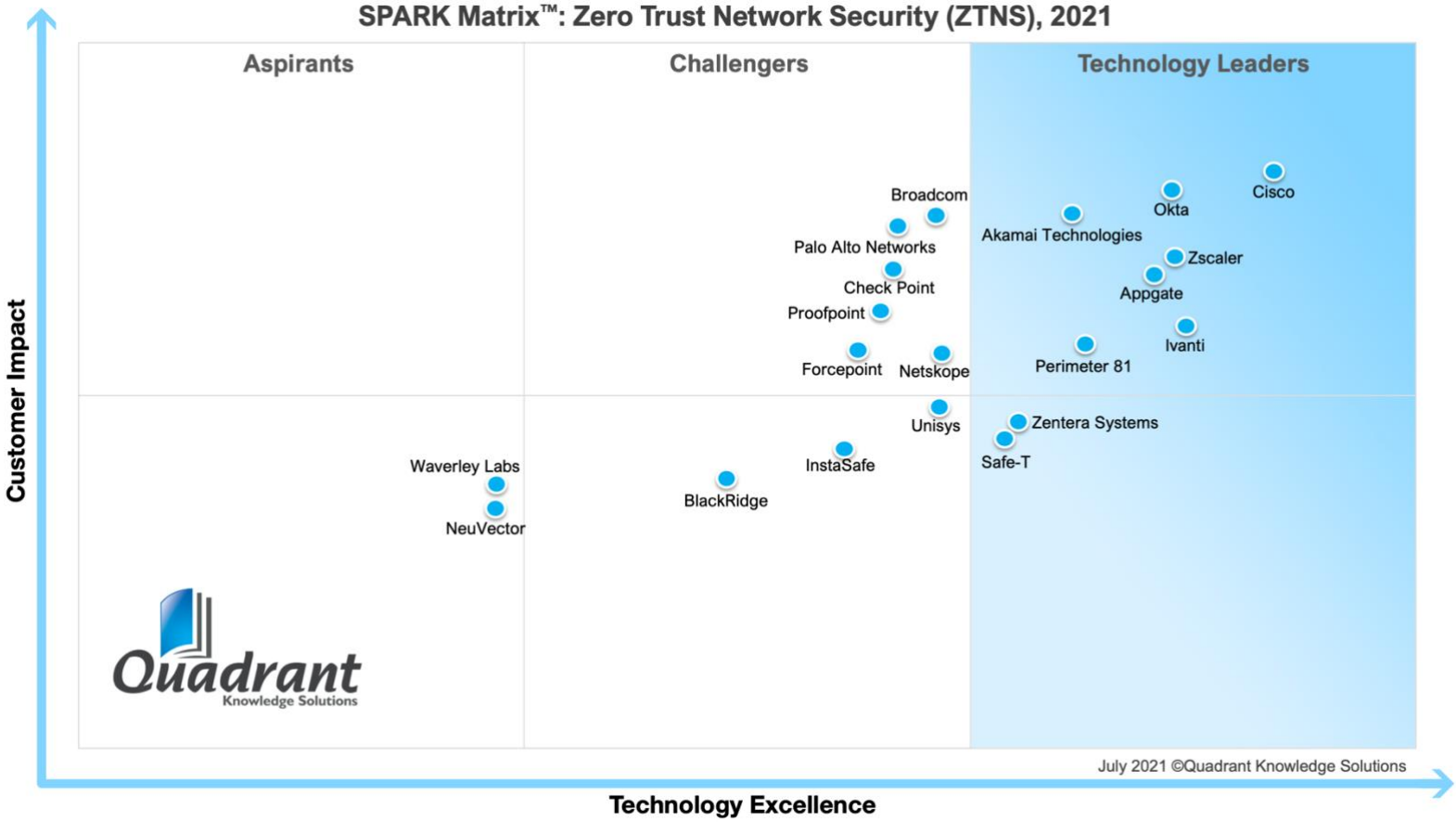
Quadrant Knowledge Solutions conducted an in-depth analysis of the major Zero Trust Network Security (ZTNS) vendors by evaluating their product portfolio, market presence, and customer value proposition. The Zero Trust Network Security (ZTNS) market outlook provides competitive analysis and a ranking of the leading vendors in the form of a proprietary SPARK Matrix™. SPARK Matrix analysis provides a snapshot of key market participants and a visual representation of market participants. It provides strategic insights on how each vendor ranks related to their competitors based on their respective technology excellence and customer impact parameters. The evaluation is based on the primary research including expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall Zero Trust Network Security (ZTNS) market.

Technology Excellence	Weightage
Sophistication of Technology	20%
Competitive Differentiation Strategy	20%
Application Diversity	15%
Scalability	15%
Integration & Interoperability	15%
Vision & Roadmap	15%

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

According to the SPARK Matrix analysis of the global Zero Trust Network Security (ZTNS) market, “Safe-T, with a robust functional capability of its products- ‘ZoneZero SDP’, has secured strong ratings across the performance parameters of technology excellence and customer impact, and has been positioned amongst the technology leaders in the 2021 SPARK Matrix of the Zero Trust Network Security (ZTNS) market.”

Figure: 2021 SPARK Matrix
(Strategic Performance Assessment and Ranking)
Zero Trust Network Security (ZTNS) Market



Safe-T Capabilities in the Global Zero Trust Network Security (ZTNS) Market

Headquartered in Herzliya, Israel, Safe-T Data, a subsidiary of Safe-T Group Ltd. (NASDAQ, TASE: SFET), is a well-known provider of Zero Trust Access solutions. Safe-T offers ZoneZero™, a perimeter access orchestration platform. The platform enables administrators to manage all remote and internal applications access requirements via one holistic platform. The ZoneZero™ platform also allows administrators to deploy new Software-Defined Perimeter (SDP) solutions, upgrade existing Virtual private network (VPN) infrastructure to Zero Trust Networks Access (ZTNA), and add MFA to any VPN, service, and application. The platform encompasses SDP, Multi-factor authentication (MFA) (built-in or via integration), and integration to commercial VPNs to provide centralized management of all secure-access technologies and enables support to all access situation for all user types, locations, and applications.

Safe-T utilizes patented reverse access technology which eliminates the need of opening LAN-DMZ firewall and provides smooth, efficient, and secured operations. ZoneZero SDP enables organizations to reduce the attack surfaces and protect sensitive data, resources, and networks from internal and external threats. The platform offers secured and transparent access to any internal applications, services, and data like HTTP/S, SMTP, SFTP, SSH, APIs, RDP, thick-client applications, and file shares for all types of entities including people, applications, and connected devices. ZoneZero SDP offers organizations a clientless, centrally managed secured access technologies to achieve Zero Trust Networks Access (ZTNA).

The ZoneZero™ VPN is designed to add ZTNA capabilities to existing VPN solutions. It seamlessly integrates with commercials VPNs and allows separating the authentication flow from the access flow when connecting via a VPN. Additionally, it allows adding MFA as a second layer of defense after the VPN, invoking MFA at the beginning of the session and during the session. allowing users to enhance their VPN infrastructure by utilizing ZTNA features.

The ZoneZero™ MFA enables organizations to quickly integrate multi-factor authentication (MFA) and identity awareness into any service or application for remote and internal users, VPNs, web applications, and non-web applications. It also provides application access control policies for internal users. It also offers seamless integration and rapid deployment to optimize cost, a unified approach without client-side integration, and supports continuous authentication.

Safe-T allows users to implement solutions without changing the endpoints. The platform supports all corporate services. It allows the users to add SDP and ZTNA for any services. In addition, it supports all the access use cases for internal and VPN users and allows integration with corporate IAM/MFA, IIoT environment deployment. It also provides a patented outbound based solution that eliminates the need of opening the LAN-DMZ firewall and provides advanced authentication workflows.

Analyst Perspective

Followings is the analysis of Safe-T's capabilities in the global Zero Trust Network Security market:

- Safe-T offers ZoneZero™ SDP, a part of Safe-T's ZoneZero Perimeter Access Orchestration suite, which provides central management of all secure-access technologies and allows organizations to achieve Zero Trust Network Access (ZTNA). Safe-T supports existing VPN solutions and eliminates the need for network and access flow re-design. It also supports all types of users and applications. It is also able to integrate with the latest access technologies and is thus suitable for both current and future access needs.

- Some of the key differentiating features for Safe-T are patented reverse-access technology, clientless support for TCP applications, ability to unify all the access use cases including internal and VPN users, and multiple deployment options such as on-premises, IaaS, MSSP, or as a cloud service.

- From a geographical perspective, Safe-T has a strong presence in the US, APAC, and EMEA. From the industry vertical perspective, while the company has a presence across a wide variety of industries, its primary verticals include banking & financial services, govt & public sectors, manufacturing, IT & telecom, education, healthcare & life sciences, and energy & utilities. Safe-T supports various use cases including WFH secure remote access, contractor and third-party secure remote access, VPN replacement, zero trust access for VPN users, and zero trust access for internal users.

- The primary challenges for Safe-T include the competition from well-established vendors with innovative technology offerings. Safe-T might also face a challenge in expanding its presence in Canada, Asia Pacific,

and Latin America. However, Safe-T, with its comprehensive functional capabilities, and robust customer value proposition, is well-positioned to maintain and grow its market share with continued success amongst small to large enterprise segments.

- Concerning future roadmap, Safe-T is focusing on developing strong UBA capabilities and specialized ZTNA container-based client applications.