QSIGHTS

QSights, published by Q Advisors, provides thought-leadership, independent opinions and data on topics of interest to the telecom, media and technology sectors.

Cybersecurity a Top Priority for Work-From-Anywhere Services and Cloud Native Explosion – Part II: Emerging Solution Trends in 2021

By Dmitry Netis & Jordan Rupar / 3.23.21

As part of Q Advisors' two-part industry leadership series on cybersecurity software and services [**download Part I**], this QSights explores the key technology trends underpinning cybersecurity growth and M&A in 2021 and beyond following a year of monumental change.

A Disruptive Year's Impact on Cybersecurity

The global pandemic accelerated digital transformation, fundamentally changing how people live and work. Enterprises made an overnight shift to work-from-anywhere ("WFX") environment, supported by a massive migration to cloud-based applications requiring robust security frameworks. Cyber threats accelerated to an unprecedented level, with over 90% of enterprises reporting an increase in cyber- attacks during the pandemic[1]. As a result, cybersecurity companies did relatively well during the pandemic, as enterprises scrambled to implement security frameworks to adequately support remote work.

Cybersecurity Public Trading Index
Relative Performance vs. S&P 500

Source: S&P CapitalIQ

The cybersecurity public index is up 60% over the last 12 months as compared to the S&P 500 at 21%[2]. Similarly, M&A activity remained strong in deal volume and size, with several major platform acquisitions exceeding $1 billion in enterprise value, including Forcepoint (Francisco Partners), Armis (Insight Partners), and RSA Security (STG).

As if the global pandemic did not wreak enough havoc in 2020, the year concluded with the SolarWinds breach, one of the most complex and potentially far-reaching cyber-attacks in history. SolarWinds is a cybersecurity software company serving global enterprises and governments. The software updates that SolarWinds released to its clients to protect their data were compromised at the code level. Preliminary estimates indicate at least 18,000 organizations could be affected, with the origin of the breach potentially dating back several years. The fallout from the breach will continue for years to come and have significant implications for how enterprises address security in the software supply chain and development process.

Q Advisors expects the global pandemic and SolarWinds breach to have lasting implications on how organizations approach enterprise security. The distributed nature of work, cloud native workflows and potential vulnerabilities down to the code level point toward a new security paradigm shift where the enterprise network perimeter no longer exists and where security responsibilities have now shifted from CIOs/CISOs down to application developer and network operations level ("DevSecOps"). Organizations must secure and protect all software, regardless of where it is found—in the public cloud, private cloud, on-premise, or on a user's mobile device. Several strategies such as ***zero trust networks access ("ZTNA")*** and ***secure access service edge ("SASE")*** will accelerate in 2021 to embrace this reality. ***Q Advisors believes*** these strategies and their underlying technologies will have a profound impact on the managed cloud services landscape and will ultimately drive much of the M&A consolidation activity and valuations over the next several years.

Sources: (1) Tanium (2) S&PCapitalIQ

QSIGHTS

Top Cybersecurity Technology Themes for 2021 and Beyond. Below are Q Advisors' top cybersecurity solution and technology themes for 2021. Many of these technologies are also featured in the **Q Advisors' sector** matrix [**download vendor matrix**] of up-and coming security vendors in the cybersecurity market.

Trend 1: Cloud and Hybrid Security are Table Stakes

Digital transformation and the work-from-anywhere paradigm shift is increasing demand for flexible security frameworks that can serve the massive shift to cloud applications. Cloud security solutions offered in a multi-cloud fashion across AWS, Azure, Google Cloud, and Kubernetes will be crucial in the new normal. Additionally, hybrid capabilities that bridge the gap to on-premise or dedicated server environments are particularly critical as a significant portion of workloads reside on premise. ***Q Advisors believes*** both hybrid and cloud security platforms will be a key technology focus in 2021 and expect to see acquirers from the traditional security realm (e.g., Rapid7, Palo Alto Networks) as well as the cloud infrastructure realm (e.g., IBM, VMware).

Select Recent M&A

vmware → octarine

Q2 2020: Cloud provider VMware purchased Octarine, a cloud-native security platform for applications running on Kubernetes.

RAPID7 → DivvyCloud

Q2 2020: Rapid7 acquired DivvyCloud for its multi-cloud security platform, running on AWS, Azure, and Google Cloud, among others.

FireEye → CLOUDVISORY

Q1 2020: FireEye acquired Cloudvisory ($13.5M) for its security workload platform, running on AWS, Azure, Kubernetes, as well as on-premise.

Trend 2. Emergence of Zero Trust Network Security Architectures

CISOs are increasingly implementing zero trust network access ("ZTNA") architectures across enterprise networks. "Zero trust" is a security concept centered on the belief that organizations should not automatically trust anything *inside* or *outside* its perimeters and instead must verify anything and everything trying to connect to its systems before granting access. Entry points at the network perimeter, once thought to be vulnerable, are gradually dissolving with zero-trust architecture. This change makes traditional network firewalls and intrusion detection appliances less useful and elevates identity and access management solutions to the pole position. In Gartner's words, "Identity is the new perimeter" and the castle and moat cybersecurity strategies of the once defined enterprise perimeter are now a thing of the past.

Select Recent M&A

Barracuda → Fyde

Q4 2020: Security provider Barracuda acquired Fyde, a ZTNA provider, expanding its solution capabilities optimized for WFX environments.

FORTINET → OPAQ

Q3 2020: Security provider Fortinet acquired OPAQ ($13.3M), a ZTNA and SASE provider, enhancing its network security solutions offering.

CROWDSTRIKE → preempt

Q3 2020: CrowdStrike acquired Preempt Security ($96M), a ZTNA provider, to help the company grow its portfolio of next generation network security solutions and proprietary platform.

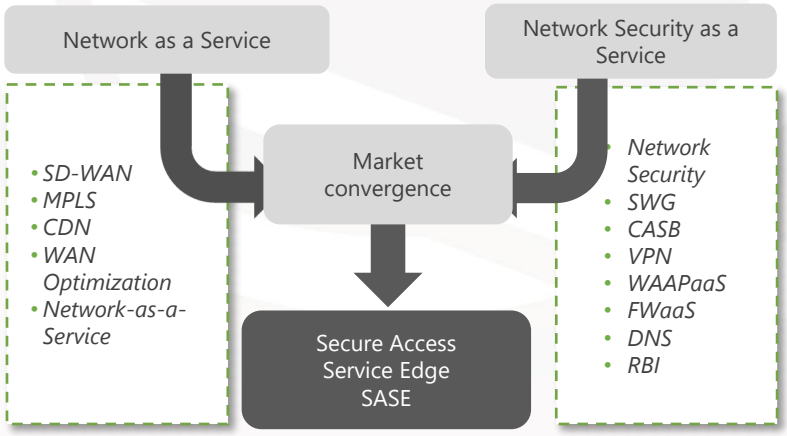
Trend 3: Emergence of Network Security 2.0 with SASE

As part of a zero-trust network strategy, secure access service edge ("SASE") – the convergence of SD-WAN and security offerings delivered to the edge – has emerged as a fast-growing solution driven by the need for branch offices and remote workers to access networks in a secure, cost-effective manner, while not degrading application performance.

SASE reflects the marriage of enterprise networks and cloud security. The solution combines WAN, MPLS, SD-WAN and similar network capabilities with comprehensive security functions to support the dynamic secure access needs of digital enterprises. SASE capabilities are delivered as a service based upon the *identity of the entity*, which can be associated with people, groups of people (branch offices), devices, applications, IoT systems, etc. It replaces the enterprise perimeter as the secure point of access, and defaults to the identity of the worker accessing the network from any device or location.

Secure Access Service Edge (SASE) Overview

Convergence of Network as a Service with Security



Source: Gartner

SASE is in its early days but has had a profound impact on the implementation of effective security policies in the new remote work and cloud landscape. According to Gartner, by 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018. ***Q Advisors believes*** SASE will cause traditional managed network providers to embrace advanced security capabilities at a rapid pace. Much of this adoption will be through M&A, such as Expereo's recent acquisition of Videns IT Services, an SD-WAN and SASE provider. The continued maturity of vendor offerings in this market, coupled with heightened M&A, will ultimately redefine the enterprise network and cybersecurity landscape in 2021.

Select Recent M&A

Akamai → Inverse

Q1 2021: CDN provider Akamai, acquired Inverse, a provider of zero trust and SASE solutions for Internet of Things applications.

expereo → videns

Q1 2021: Expereo, a managed network provider, acquired Videns IT Services, an SD-WAN and SASE provider.

paloalto NETWORKS → CLOUDGENIX

Q4 2020: Palo Alto acquired CloudGenix ($420M) to incorporate its best-in-class SASE platform.

Trend 4: Acceleration of DevSecOps and Developer-First Security

The SolarWinds breach exposed the long overdue need to prioritize security in the software development process. Implementing security procedures early in the development lifecycle has historically slowed development timelines. According to a recent study, 79% of organizations are under greater pressure to accelerate their development cycles and 55% of developers admit to skipping security processes when releasing code[1]. In the wake of the SolarWinds breach, ***Q Advisors believes*** more enterprises will adopt secure DevOps ("DevSecOps") processes. DevSecOps assumes organizations will shift responsibility for application security to developers earlier in the software development process. Security M&A activity is also expected to coalesce around developer-first security platforms, such as Palo Alto's acquisition of Bridgecrew earlier this year.

Select Recent M&A

paloalto NETWORKS → bridgecrew

Q1 2021: Palo Alto announced its acquisition of Bridgeview ($156M), a cloud and developer-first security platform to streamline DevOps.

Progress → CHEF

Q4 2020: Progress Software, an application development provider, acquired Chef ($220M), a provider of DevOps and DevSecOps.

snyk → DEEPCODE

Q4 2020: Synk, a developer-first cloud security provider, acquired DeepCode, a real-time semantic code analysis platform to deepen its DevSecOps capabilities.

Trend 5. Evolution to Active Endpoint Management with AI/Machine Learning

Endpoint security is focused on locking down endpoints—individual computers, phones and other network-enabled devices—in order to keep networks safe. While endpoint security has traditionally taken a reactionary approach to threats across devices, a more "active" and preventative approach is needed to properly address cyber threats. As a result, endpoint detection and response ("EDR") has emerged —a subset of endpoint security technology that addresses the need for continuous monitoring and response to advanced threats. Several vendors and service providers are taking the next step with EDR technologies to include artificial intelligence ("AI") and machine learning ("ML") to identify threats in real time with only the most pressing needs escalated to human attention. ***Q Advisors believes*** the complexities around management of the EDR environment will cause increasing adoption of AI/ML tools as well as accelerate M&A consolidation in the space.

Select Recent M&A

HUNTRESS → LEVEL EFFECT

Q1 2021 : Huntress, a ThreatOps provider, acquired EDR technology from Level Effect. Huntress' acquisition resulted in a combined EDR/MDR solution for its channel partners.

vmware → Carbon Black.

Q1 2020: VMWare, a provider of cloud and virtualization services, acquired Carbon Black ($2.1B), a cloud-native end point protection platform.

elastic → ENDGAME.

Q4 2019: Elastic, a security SIEM and threat hunting platform, purchased Endgame ($227M), a managed endpoint protection and response platform.

Sources (1) Contrast Security

Trend 6: Dire Need for Security Operations Center ("SOC") Automation

Enterprise security operations centers ("SOCs") can encounter tens of thousands to a million alerts per day. The primary barrier to success of a security operations team is lack of cyber resources to scale with the sheer number of threat incidents and alerts. By combining security information and event management ('SIEM") capabilities to ingest large amounts of data and generate alerts with SOC automation tools such as security operation automation and response ("SOAR") solutions, organizations can manage the incident response process to each alert, to automate the response, and do more with software versus humans. ***Q Advisors believes*** advanced technology in SOCs, such as SOAR, will continue to improve response times and drive M&A, as acquirers across the MSP and MSSP landscape seek out these capabilities.

Select Recent M&A

ConnectWise → STRATOZEN / PERCH

Q4 2020: Connectwise, a software provider for MSPs, purchase two SIEM and SOAR platforms to automate SOC solutions for channel customers.

MICRO FOCUS → atarlabs

Q3 2020: Micro Focus, an IT software and services provider acquired Atar Labs, a SOAR technology software provider to integrate the offering into its SIEM solution.

SWIMLANE → SYNCURITY

Q2 2020: Swimlane, a SOAR provider acquired Syncurity for their automated SOAR and analytics capabilities.

Trend 7: Identity as the New Enterprise Network Perimeter

Identity and access management ("IAM") is about managing the roles and access privileges of individual network users and the circumstances in which users are granted those privileges. These capabilities were vital during the shift to remote work during the pandemic and will remain crucial in a post-pandemic world.

The objective of IAM systems is one digital identity per individual. Once that digital identity has been established, it must be maintained, modified, and monitored throughout each user's access lifecycle. IAM business value spans several categories: 1) customer/employee IAM, 2) identity analytics, 3) identity-as-a-service (IDaaS), 4) identity management and governance (IMG), and 5) risk-based authentication (RBA). Strong authentication capabilities married to an IDaaS make up key attributes for data loss prevention, managing of digital risk, and standing up zero-trust network environments—key areas of current investment for CISOs. ***Q Advisors believes*** identity will continue to serve as the enterprise network perimeter in a post-pandemic world, accelerating enterprise adoption and M&A activity across IAM, IDaaS, IMG, RBA, and other advanced identity platforms.

Select Recent M&A

protiviti → identropy

Q4 2020: Proviti, a global consulting firm, acquired Identrophy, an advanced IAM provider to incorporate the solution into its digital identity as a service offering.

HERJAVEC GROUP → securience

Q3 2020: Herjavec, a global MSSP, acquired IAM provider Securience to expand and enhance its identity services globally.

Atos → IN|FIDEM

Q1 2021: Atos, a security services provider, acquired In Fidem, a cybersecurity provider focused on identity solutions in order to enhance Atos's IDaaS solution.

okta → Auth0

Q1 2020: Okta, the leading independent identity provider, acquired Auth0, an identity platform for application teams to build an internet service that establishes identity as the primary cloud.

PingIdentity → SYMPHONIC

Q4 2020: Ping Identity, an enterprise identity solution, acquired Symphonic, a leader in dynamic authorization to address the scalability and performance requirements needed to secure access to critical data.

CYBERARK → idaptive

Q2 2020: CyberArk, the global leader in IAM, acquired IDaptive, leader in both Privileged IM and IaaS to deliver the industry's only modern identity platform with a security-first approach.

Conclusions

1	**Heightened M&A Activity Across Hybrid and Cloud Security**	The enterprise network perimeter is obsolete. Organizations must secure and protect all software, regardless of where it is found—in the public cloud, private cloud, on-premise, and endpoint devices. Because of this, hybrid and cloud security platforms will be a key technology focus in 2021 and we expect to see an increase in acquisitions in both the traditional *and* cloud native realms.
2	**Emergence of ZTNA and SASE to Address Paradigm Shift to WFX Models**	Digital transformation resulting from more geographically-dispersed workforce will require traditional managed network providers to rapidly adopt advanced security capabilities such as SASE. Increased vulnerabilities associated with WFX will force more enterprises to adopt emerging security technologies such as zero trust network access.
3	**Adoption of Developer-First Security Models**	Given recent attacks on the software supply chain coupled with the rise in DevOps, agile software development, and open-source architectures, we expect security M&A activity to ultimately consolidate down to the code level, around developer-first security platforms.
4	**Evolution of EDR to Preventative, AI / ML Driven Frameworks**	The complexities around managing EDR environments will cause increasing adoption of AI tools while accelerating consolidation in the space. With the lack of cyber resources presenting a primary challenge to organizations, AI/ML technology will be crucial to automate security procedures as companies face an increasing number of complex cyber threats.
5	**Network Identity as the New Security Standard**	The concept of unique digital identity will continue to serve as the enterprise network perimeter in a post pandemic world, accelerating enterprise adoption and M&A activity across IAM, IDaaS, IMG, RBA, and other identity platforms. The continued maturity of vendor offerings in this market, coupled with heightened M&A, will ultimately redefine the enterprise network and network security landscape in 2021.

About Q Advisors

Q Advisors LLC (www.qllc.com) is a world-class global boutique investment bank formed in 2001 serving public and private companies, PE firms, entrepreneurs and large multi-nationals in the telecom, media, and technology (TMT) sectors. The firm has extensive, global reach, while also providing the personalized service of a boutique advisory firm. Thanks to our partners and senior staff, who come from leading investment banks and operating companies, we leverage extensive industry knowledge and analytical insights to help our clients achieve successful M&A and capital markets transactions.

Dmitry Netis / Managing Director, Head of Business Development / *netis@qllc.com*

Dmitry brings 25 years of unique background that combines finance, venture investing, sell-side equity research, and operational industry experience across the TMT sector. Before joining M&A advisory, Dmitry was an equity research analyst on Wall Street, first at William Blair & Company for over 10 years as a founding member of the TMT team, where he established cloud communications, data networking and storage, and infrastructure software practices and later at Stephens, Inc., as a Managing Director and head of TMT sector research. Prior to that, Mr. Netis worked for more than a decade in the high-tech industry, holding engineering and management roles at Conexant Systems and IBM Corporation. Mr. Netis holds a B.S.E.E. from the University of Rochester, a M.E. from Cornell University, and an M.B.A. from Rensselaer Polytechnic Institute.

Jordan Rupar / Vice President / *rupar@qllc.com*

Jordan Rupar joined Q Advisors in 2012. During this time, she has executed numerous mergers and acquisitions, equity financings and strategic advisory assignments for clients across the TMT industries with a deep focus on cloud communications, software and technology, communications infrastructure, and other emerging growth sectors. Jordan received her B.S.B.A. in Finance with Distinction, as well as minors in both Mathematics and Economics from the University of Denver.