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-Home Services and Cloud Native Explosion

By Dmitry Netis & Jordan Rupar / 7.30.2020

Q Advisors is broadening its focus on Cybersecurity software in 2020 and beyond. Commensurate with our recent publications on Cloud Native and DevOps, ***Q Advisors believes*** cloud-native security will remain a key investment area and an integral part of the cloud native infrastructure given the implications of the velocity and volume of distributed, ephemeral, and remote access services that the move to the cloud brings. Moreover, our attendance at RSA tradeshow in March—amid the developing coronavirus outbreak—underscored the growing importance and mission-critical nature of security in virtually every area of IT. Far outstripping any other enterprise IT budget item, spending on cybersecurity continues to ratchet up each year—eclipsing $130 billion in 2020—with long-lasting implications driven by COVID-19 and the surge in demand for Work-From-Home (WFH) access services.

In the post-COVID-19 world, ***Q Advisors believes*** that corporate networks are likely to see an accelerated shift towards mobility-enabling services, which in turn provide a strong secular tailwind to cloud-based security, identity access and management (IAM), next-gen endpoint detection and response (EDR) tools, and AI-based analytics and automation. We expect this to result in a heightened response toward consolidation by legacy security and IT vendors.

Beyond the emergence of new tools, enterprise security mindset and practices will equally need to change. Cybersecurity has historically been viewed as a necessity, but also as an impediment to time to market, scale and innovation within an enterprise. We are now seeing a seismic shift in the market's perception of security as an enabler of product differentiation and customer confidence. Whether the organization views security as a cost center or an enabler is a strong indicator of the success of a security strategy. Chief Information Security Officers (CISOs) and outsourced managed security service providers (MSSPs), which often replace or supplement an in-house security team, are becoming commonplace, playing a key role in shaping the future of business practices across enterprises of all sizes.

Security Mindset: Four Tribes of Organizations

The CISO's mindset is a strong indicator of the success of a security strategy and overall business

Source: CISO Report (Synopsis)

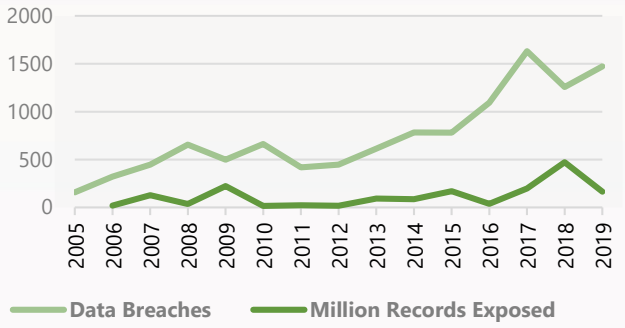
Four mindsets exist in today's security organizations. These mindsets range from viewing security as an enabler (Tribe 1) to viewing it merely as a cost center (Tribe 4). The group that views security as an enabler (Tribe 1) is seeing the most success in both risk mitigation and business processes.

QSIGHTS

Cybercriminal Activity Spiking More Than Ever

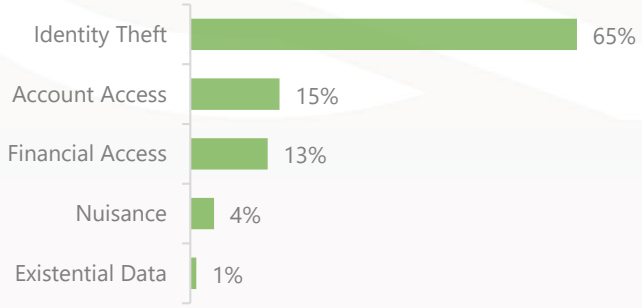
Cybercrime has become nearly impossible to track given the growing level of cybercriminal activity in the form of hacking, malware, phishing, and ransomware, among several other tactics. Damage related to cybercrime is projected to hit $6 trillion annually by 2021[1]. Additionally, COVID-19 has ushered in a wave of cybercriminal activity. Since mid-February, cybercrime incidents per day have increased dramatically from a few hundred thousand to as high as over a million incidents per day in early March 2020[2]. Most attacks are targeting identity and credentials, keeping emerging "zero trust" networks and related defense mechanisms top of mind for enterprises. The largest data breach to date was uncovered at Yahoo! in 2016, as hackers stole user information associated with three billion user accounts.

Annual Number of Data Breaches and Records Exposed



Source: Identify Theft Resource Center

Percent of U.S. Data Breach Incidents by Type (2018)

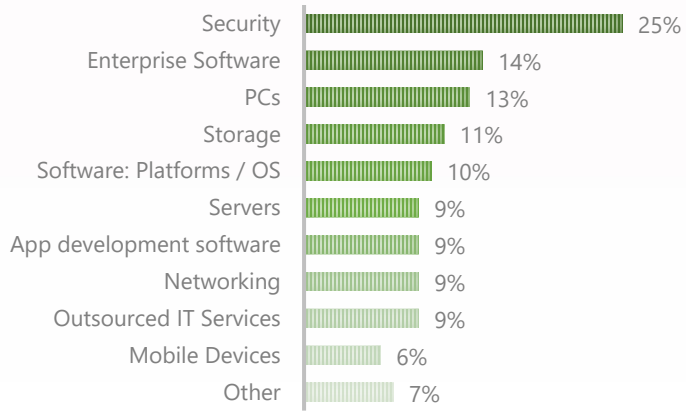


Source: Statista

Cybersecurity Gains the Biggest Share of Enterprise IT Wallet

As enterprise priorities are constantly changing to combat emerging threat vectors, which are stretching beyond immediately recognizable ones such as viruses, malware, phishing attacks and data breaches, cybersecurity budgets continue to rise each year. Cybersecurity is seeing stratospheric growth, ballooning to over 25% of the overall enterprise IT budget. Even before the COVID-19 crisis, 87% of enterprise buyers reported increases in their security budget during 2019, which rose by an average of 22%. The WFH shift is bound to accelerate this trend.

IT Budgets: Where will your Company Spend the Most in 2020?



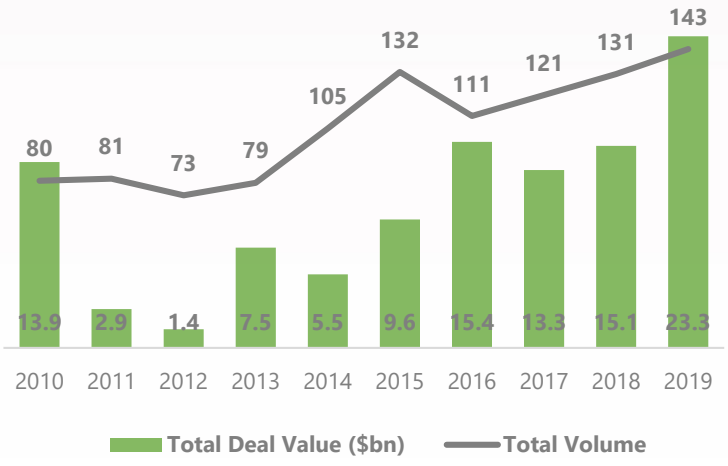
Source: 451 Research

(1) Cybersecurity Ventures (2) Microsoft

M&A Implications and Vendors to Watch

The threat landscape remains highly fluid with new cyber crime vectors introduced to enterprises almost daily. Funding keeps coming in with more unicorns being born every month and more M&A occurring despite the rising macroeconomic concerns. ***Q Advisors assembled*** a matrix of up-and-coming security vendors across nine subsegments of the cybersecurity market. On the deal front, M&A in the space saw a 50% increase in the number of transactions in the second half of the last decade (2015-2019) over the first half (2010-2014). M&A activity in 2019 culminated with major platform acquisitions of Sophos (Thoma Bravo), Symantec (Broadcom) and Imperva (Thoma Bravo), and Forescout (Advent International) which found amicable grounds to closure after discussions failed to advance initially in the midst of pandemic. Private equity buyers represented about 30% of deals historically with 70% going to strategics. While rising concern for available credit and higher premiums on risk likely will curtail some private equity activity, smaller bolt-on acquisitions for portfolio companies will likely continue. A new class of strategic buyers has emerged with Palo Alto Networks and Proofpoint versus historical acquirers—Symantec, Sophos, and McAfee. Palo Alto Networks paid 25x median EV/trailing sales on average for nine transactions in the last two years, staying at or below the $100 million to $500 million deal category. The M&A market is likely to witness accelerated demand as the number of remote and smart devices accessing enterprise networks and hosted services has grown exponentially because of the COVID-19 crisis. Lastly, as security infrastructure, along with related services, plays right into managed service providers strength, MSSPs are in position to capitalize on pent-up demand from secure connectivity services—endpoint protection, access control, analytics, and security monitoring—within distributed network environments, and will be active as both buyers and sellers on the M&A front.

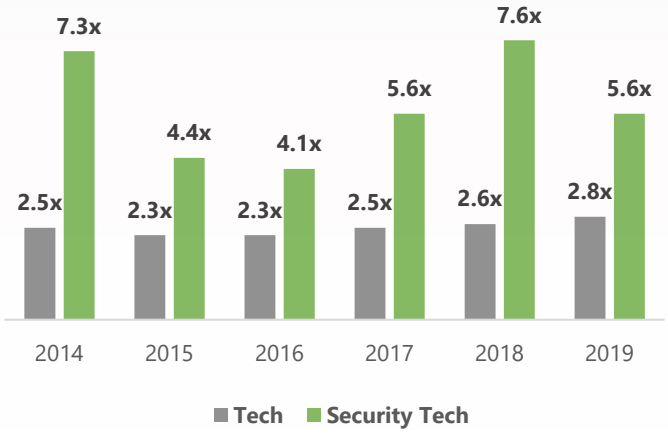
M&A Volume: Cybersecurity Acquisition Volume and Spending, 2010-2019



Source: 451 Research

M&A Valuations: Cybersecurity Transactions vs. Broad-market Transactions

Price / Sales Ratios



Source: 451 Research

QSIGHTS

Cybersecurity and Risk Management Market is Large and Broad

Cybersecurity market is estimated to absorb over $130 billion in enterprise spending in 2020, according to Gartner, growing in aggregate at a five-year CAGR of 8%. The fastest growing segment is cloud security (23% CAGR), which is table stakes as digital transformation and WFH initiatives force enterprises to shift more workloads from on-premise to the cloud. Other double-digit growing segments include data governance (15%), endpoint detection & response (10%), security analytics and automation (20%), identity and management (13%), and DevSecOps (20%). With the shift to the cloud, more security solutions are being offered as-a-service, creating growing secular opportunities for MSSPs. In fact, spending on security services is well-outpacing spending on security software, with over half of overall information security spending (53%) directed toward it.

Total Information Security and Risk Management End User Spending by Subsegment in 2019

Network Security (NS)

$13.2B [1]
5-year CAGR: 14.4%

Application/Email Security (AS)

$3.0B [1]
5-year CAGR: 10.0%

Identity & Access Management (IAM)

$9.7B [1,2]
5-year CAGR: 13.0%

Endpoint Protection (EPP), Endpoint Detection & Response (EDR)

$12.8B [2]
5-year CAGR: 7.6% & 10%

Cloud & Web Security (CS)

$5.1B [2]
5-year CAGR: 23.0%

Security Info & Event Management (SIEM), Analytics & Automation

$2.9B [1,3]
5-year CAGR: 9.9% & 20%

Infrastructure Protection & DevSecOps (DSO)

$14.9B [1,4]
5-year CAGR: 8.7% & 20%

Security Services

$64.5B [1]
5-year CAGR: 8.8%

(1) Gartner, (2) Markets and Markets, (3) Global Market Insights (4) Research and Markets

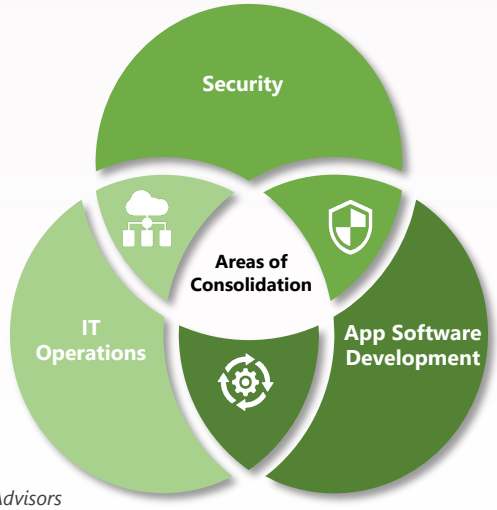
Five Macro Security Trends Driving Investment

1. Long-lasting Impact from Shift to Work-From-Home (WFH): The WFH shift created by the COVID-19 pandemic is causing an additional level of complexity to protect the enterprise perimeter. ***Q Advisors expects*** that the WFH explosion will spark initiatives to modernize enterprise security, catalyzing long-term investment and M&A activity. In a world where cloud concepts increasingly dominate, many existing approaches to securing hosted services predicated on deployment within a traditional enterprise network are showing their age. Newly emerged vectors such as phishing attacks targeting employees scrambling to access enterprise resources or high-jacking of virtual collaboration platforms must be dealt with via new security frameworks. Challenges with WFH environments include remote user-owned endpoints, local networks (home WiFi/private LTE), VPNs (where variety of consumer devices may connect with endpoints used in the enterprise), unforeseen bandwidth requirements (for virtual desktop infrastructure, or VDI), and visibility to identify anomalies and impose control to limit malicious behavior when discovered. In addition, increased reliance on third-party cloud services means that enterprise users can access these resources from anywhere and perform far better when connected directly to these third-party resources than when funneled back to the enterprise network. This is part and parcel of the move toward "zero trust" network access and secure access service edge (SASE) that combines software-defined network with network security functions like secure web gateway, and firewalls.

2. Convergence of IT Operations, Apps Development and Security in Race for Digital Transformation: Security frameworks are a big part of enterprises' push for digital transformation (DX). Enterprise C-suite is concerned about time efficiency, business friction, and wasted time and resources as DX initiatives are put in place. Having a rigorous security framework is key to successful DX initiatives. ***Q Advisors expects*** digital transformation initiatives to drive a further blurring of the lines between security, software development (DevOps), and IT infrastructure. Secure DevOps (DevSecOps) will ultimately yield better customer experiences and richer services. ***Q Advisors further believes*** this trend will drive continued consolidation across these three markets. As an example, NTT's acquisition of WhiteHat last year, a pioneer in application security and the DevSecOps, reflects the Company's emphasis on adding secure DevOps capabilities to its managed and consulting security service portfolio.

Convergence of Three Distinct Functions within an Enterprise

Digital transformation is blurring the lines between security, software development and IT infrastructure



Source: Q Advisors

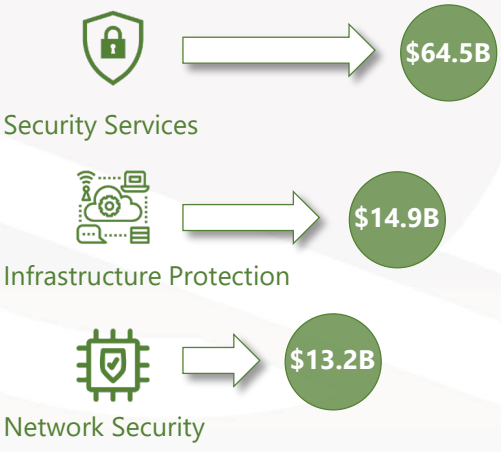
Convergence of three key functions within an enterprise will result in new practices, ultimately ushering in an era of efficiency and growth. Secure DevOps (DevSecOps) is an example of an emerging business model and practice that combines these three elements.

Five Macro Security Trends Driving Investment *(cont'd)*

3. Security Services Outpacing Point Products: Enterprise adoption of security services is accelerating due to the growing complexity of security threats. Four-times the spending is being directed to cybersecurity services than any other area of IT, a relatively recent trend, with spending on security services outpacing other IT investments for the first time in 2018[3]. MSSPs are also advancing their offerings to address the full security lifecycle, from alerts, triage, and remediation, in order to increase relevancy in the enterprise. As a result, several managed security specialists have emerged to embrace the latest technologies and tactics including Managed SIEM Providers and Managed Detection and Response (MDR / SOAR) Providers. Traditional managed cloud service providers will also emerge as security specialists by adding security, through acquisitions or partnership, to their core cloud and IT infrastructure solutions.

Top 3 Categories of Investment

Security services outpacing other areas of enterprise security investment



Source: Gartner (2019A)

Security is highly complementary to other cloud managed services such as cloud voice, networking, and cloud computing / IaaS and often results in a "stickier" end-user bundle of cloud solutions. ***Q Advisors believes*** that the ability to acquire, integrate and scale security solutions as part of an overall managed services suite will result in long-term valuation premiums for the combined entity. As an example, Dyonyx, a virtual cloud services provider, and Single Path, a cybersecurity-solutions consulting provider, merged their MSP and MSSP businesses to form a new company called Dyopath earlier this year. Orange, France's incumbent telecom provider, recently purchased SecureLink to roll out cybersecurity to its enterprise base as part of its cloud and collaboration offering. ***Q Advisors expects*** to see more transactions of this nature as MSSPs and MSPs continue to converge.

4. Emergence of Data Protection, Privacy, and Compliance Services: Enterprises are increasingly subject to regulatory compliance requirements such as PCI, GDPR, and HIPAA, among several other recently enacted consumer privacy regulations. Penalties for not adhering to these regulations are costly and can significantly impact the financial and reputational health of a business. As a result, IT budget investments into areas such as compliance, identity and access management, identity governance, and data loss prevention (DLP) are outpacing others by roughly 10%[2]. These investments are intricately linked with security budgets, as a consumer data exposure is often caused by a network security breach.

(1) Gartner, (2) Cybersecurity Ventures, (3) Forrester

Five Macro Security Trends Driving Investment *(cont'd)*

Q Advisors believes having a robust compliance and data privacy solution is paramount to any security and cloud solution provider. Microsoft's acquisition of BlueTalon (data control and security) and Navex's acquisition of LockPath (compliance and data protection) are just two examples of the growing M&A in this space. Pure play cloud providers, like Calligo, are tackling this market and offering a full suite of outsourced data privacy and compliance services (e.g., outsourced Data Privacy Officer, GDPR and CCPA Privacy) in conjunction with their core cloud solutions.

5. Demand for Integrated Security Platforms vs. Point Products: The debate continues as to the benefits of an integrated solution over a best-in-breed point product. ***Q Advisors believes*** enterprises are in the throes of extreme vendor fatigue, where they are often forced to chain together dozens of cybersecurity vendors in deploying specific products. The scale is beginning to tip toward integrated security vendors capable of identifying threats in real time, combating insider risk, and delivering a cost-effective one-stop-shop solution. While best-in-breed point solutions may still win the hearts of customers due to unwillingness to sacrifice efficacy for vendor reduction, C-level execs aren't looking for the flashiest new point products.

Faced with a severe shortage of talent and up against rapidly evolving threats, CISOs are looking for strategic partners, advisory services, and vendors that offer broad platforms. Capabilities such as artificial intelligence (AI), alignment of security operations via automation and orchestration (SOAR), and user behavioral and event analytics (UEBA), are emerging as key add-ons of an integrated security ecosystem. ***Q Advisors believes*** M&A trends toward aforementioned areas as part of an integrated security platform will accelerate. Strategic buyers addressing these needs are: Akamai, Check Point, Cisco, Fortinet, Google, IBM, Microsoft, McAfee, Palo Alto Networks, Proofpoint, Sophos, and VMware.

> *"Cyberdefense is about having an integrated set of tools that work together to prevent attacks. But the industry now has a thousand points of light and no illumination. It's as if in the automotive industry, a spark plug company advertised itself as making the best transportation service in the world."*

Bill Crowell
Former Deputy Director
U.S. National Security Agency

> *"Individual entities will eventually be subsumed into a larger company that bottles 10 or 15 solutions into a suite. There are a lot of companies out there [now] that might just offer a feature when they think they have a whole product."*

Jeff Pollard
Analyst
Forrester

Conclusions

Heightened M&A and Investment Activity	The cyber security problem is far from being solved with new threat vectors emerging every day. Heightened demand for solutions will continue to drive investment and M&A activity by cloud providers and legacy security and IT vendors as buyers.
Shift to Integrated Security Platforms, Cloud Native and DevSecOps	Enterprises are in the throes of vendor fatigue, seeking simplified security products. A trend toward integrated security platforms versus best-in-breed solutions is picking up, leading to heightened consolidation of point solutions in the market. We also expect to see more implementations of Secure DevOps (DevSecOps), a practice that aims to embed security into the development process and in IT infrastructure, ultimately yielding better customer experiences for the enterprise.
WFH Explosion to Drive Surge in Secure Remote Access Services	The WFH explosion, largely from the recent coronavirus pandemic, will spark initiatives to modernize enterprise security, catalyzing long-term investment and M&A activity. The move toward "zero trust" and secure access service edge (SASE) could facilitate this sea change in distributed enterprise security.
Growing Opportunities for MSSPs	With the shift to the cloud, many security solutions are being offered as-a-service, creating growing secular opportunities for MSPs and MSSPs. In fact, spending on security services is well-outpacing spending on security software, with four times more dollars being directed to cybersecurity services than any other area of IT.

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 over 24 years of combined financial and operating industry experience in the telecom, media, and technology sector (TMT). Most recently, he consulted for several public and private companies under the practice he founded and was CFO/COO of CafeX Communications. Prior to this, he spent 12 years as an equity research analyst, 10 of those with William Blair & Company, where he was a founding member of the TMT team, where he established cloud communications and infrastructure software practices. 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 (cloud infrastructure, fiber, towers, etc.) 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.