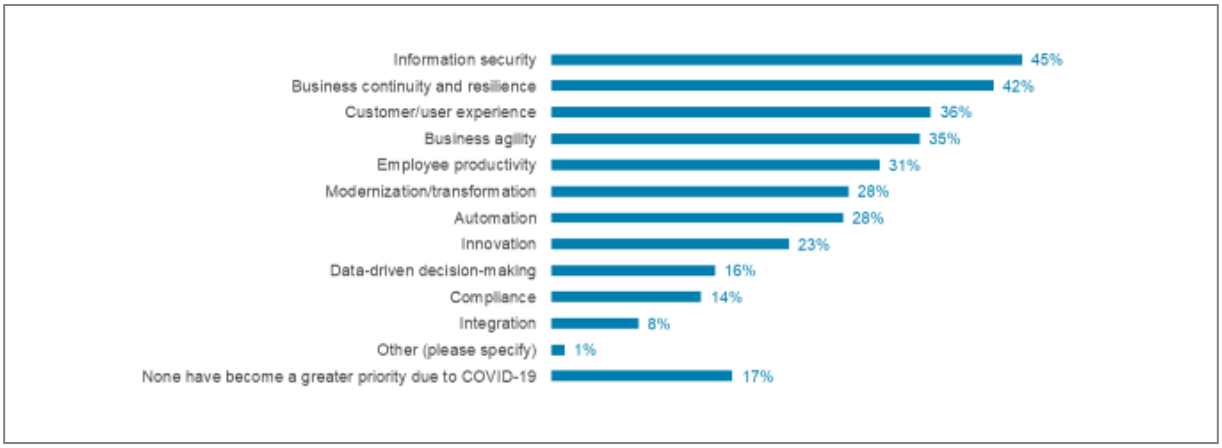
2021 Tech M&A Outlook: Information security

Analysts - Garrett Bekker, Scott Crawford, Daniel Kennedy, Fernando Montenegro, Aaron Sherrill, Eric Hanselman

Publication date: Wednesday, February 17 2021

In 2020, the pandemic turned much attention toward technology as a key enabler for sustaining businesses across the globe. But with substantial investment in enablers such as digital workspaces, virtual conferencing and collaboration, and customer experience for booming online retail, security inevitably rises to the fore as a concern. In fact, information security was the priority most often cited by respondents as having become greater due to the outbreak, according to 451 Research's Voice of the Enterprise (VotE): Digital Pulse, Coronavirus Flash Survey October 2020.

Security Is a Top Priority for COVID-19



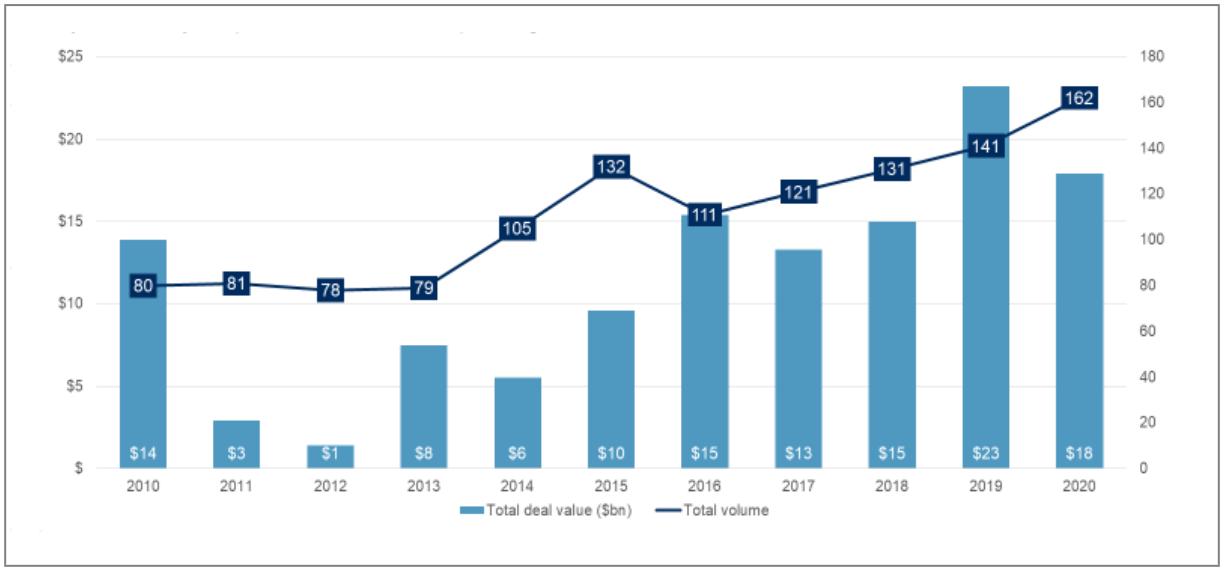
Source: 451 Research's Voice of the Enterprise: Digital Pulse, Coronavirus Flash Survey October 2020
Q. Which of the following technology objectives, if any, have become a greater priority for your organization due to the influence of the outbreak? Please select all that apply
Base: All respondents (n=371)

This means more, however, than just a greater emphasis on securing work from anywhere. It comes alongside a substantial expansion in multiple aspects of IT: A variety of deployment models for cloud

and datacenter computing, and dramatic growth in OT and IoT rising alongside millions of new remote user endpoints, aided by developments such as 5G that have led to an explosion of the attack surface.

Thus, it should come as no surprise that despite the lockdown and a predictably slow start to the year, overall infosec M&A – as measured by deal volume – was up for the fifth straight year, to a total of 162 transactions, handily surpassing the record total of 141 prints in 2019. In terms of deal value, however, the $17.9bn total fell short of the previous year's high-water mark of $23.2bn (which was inflated by Broadcom's $10.7bn purchase of Symantec's enterprise security business and Thoma Bravo's $3.8bn buyout of Sophos), although there were more billion-dollar-plus cybersecurity deals in 2020 (six) compared with 2019 (four).

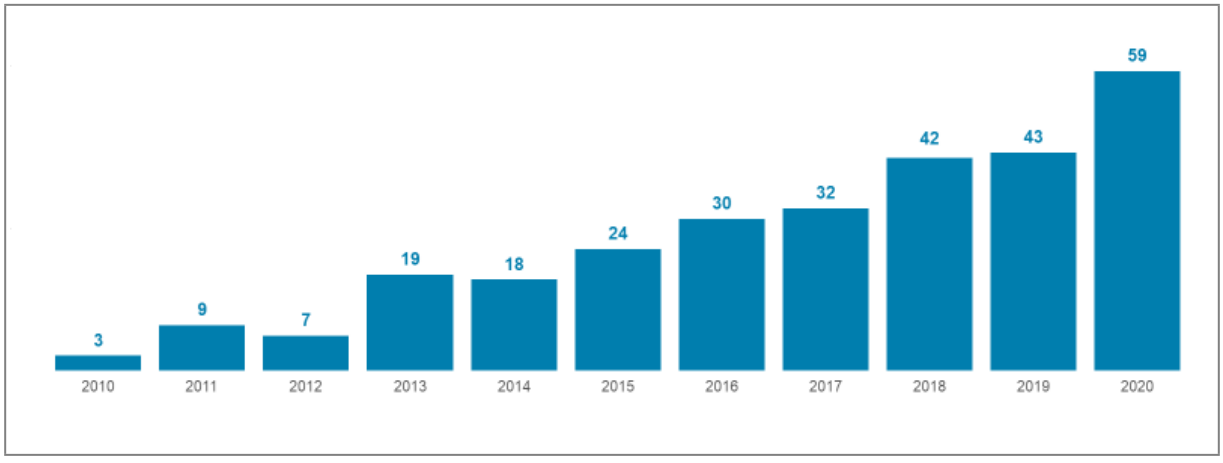
Infosec M&A: Cybersecurity Acquisition Volume and Spending, 2010-20



Source: 451 Research's M&A KnowledgeBase, January 2021; includes disclosed and estimated values

Private equity (PE) continues to expand its influence on cybersecurity M&A, with 59 PE-led deals in 2020, up from 43 in 2019 and accounting for just over one-third (36%) of all cybersecurity transactions. Five of the six billion-dollar acquisitions and seven of the top 10 were PE-led.

PE M&A: Number of Sponsor-Backed Infosec Purchases, 2010-20



Source: 451 Research's M&A KnowledgeBase, January 2021

As we have noted previously, with the ascendance of PE as the primary driver of cybersecurity M&A has come a matching decline in the volume of deals from 'traditional' security vendors. Just 41 transactions (25%) came from traditional security firms in 2020, down sharply from 53 deals (38%) in 2019. To some extent, this is due to the 'thriftiness' of once-profligate spenders like McAfee and Symantec, which had inked 55 and 29 prints, respectively, dating back to the formation of 451 Research's M&A Knowledgebase in 2002, but printed just one acquisition between them last year while on strict M&A 'diets' prescribed by their PE overlords.

In recent years, some of the slack has been taken up by Palo Alto Networks, which dropped a total of nearly $1.5bn last year on Expanse ($800m), CloudGenix ($420m) and Crypsis ($265m), and spent north of $3bn in aggregate over the past three years across 11 deals, at an average of $265m per print. The leading candidates for 'most valuable acquirer' last year include HelpSystems, continuing a recent data security rollup strategy that brought four new targets to the table, and Atos, with three service-based tuck-ins. FireEye, GitLab, J2 Global, Mimecast, Ping Identity and VMware all did two transactions apiece in 2020.

However, as we've noted in past reports, much of the strength in infosec M&A in recent years has been driven by non-security strategic vendors – i.e., buyers whose main revenue sources come from businesses outside of infosec, including players in adjacent segments like cable MSOs and telcos, financial services, networking, storage, and SIs. By our count, roughly 63 of the 162 deals (39%) were from non-security strategic acquirers, a massive 43 purchases (30%) last year. Notable examples include Accenture (managed security services), LexisNexis (antifraud and identity theft), MasterCard (cyber-risk management), Moody's (GRC and compliance), Nasdaq (antifraud) and Thomson Reuters (antifraud).

Signature Deals From 2020

Acquirer	Target	Deal Value	Comments
Nasdaq	Verafin	$2.8bn	Continuing its evolution from stock exchange to fintech, Nasdaq adds anti-money-laundering chops to bolster its financial crime portfolio.
Symphony Technology Group/Ontario Teachers/AlpInvest Partners	RSA Security (Dell Technologies)	$2.1bn	Dell-EMC's 14-year embrace of one of cybersecurity's pioneer vendors finally comes to a long-expected end. The acquirer's security products bet now rides primarily on VMware.
Advent International/Crosspoint Capital Partners	ForeScout Technologies	$1.7bn	After a slump that attracted activist investors, the network access control veteran fell into the arms of a buyout group led by ex-McAfee chairman Bryan Taylor and ex-Symantec CEO Greg Clark.
Hellman & Friedman	Checkmarx	$1.2bn	Insight Partners' flip of Checkmarx produces the first unicorn exit for the fast-growing application security market.
Ivanti [Clearlake Capital]	MobileIron	$930m	Ivanti's reach for MobileIron during the pandemic highlights the importance of unified endpoint management.
GI Partners	Sectigo (fka Comodo)	$900m*	Following its carve-out from Comodo in 2017, Sectigo is the latest PKI specialist to find a PE exit.
Insight Partners	Armis	$1.1bn	Following Palo Alto Networks' pickup of ZingBox and Tenable's purchase of Indegy, Armis' unicorn valuation may represent a turning point in the relatively tepid history of IoT exits.

Francisco Partners	Forcepoint (fka Websense)	$1bn*	Forcepoint's long-anticipated sale brings to a fitting end another unfruitful foray into the cyber realm by a defense contractor (Raytheon).
Palo Alto Networks	Expanse	$800m	Expanse shows that Palo Alto aims to address the challenges customers face managing their ever-growing IT estates.
Fastly	Signal Sciences	$775m	Fastly adds a web application firewall (WAF) platform with API security and bot detection and mitigation capabilities with a reputation for overcoming a key limitation of legacy WAFs: running effectively in blocking mode.

*Source: 451 Research's M&A KnowledgeBase. *451 estimate*

Identity and access management (IAM) and managed security services remain the two most active sectors for M&A, although the two switched places last year: Managed security service provider (MSSP) deals increased from 28 to 32, while IAM transactions fell by nearly the same amount, from 32 to 27. We expect the two sectors to remain highly active, for several reasons. First, the IAM segment consists of at least five subcategories and several hundred vendors covering a breadth of use cases spanning authentication ('who are you?') to access controls ('what are you allowed to access?') and access governance ('who should have access, and why?').

Additionally, the decline of the traditional network perimeter is making identity a central control point for new, alternative frameworks such as zero trust networking that reject the notion of 'trusted' and 'untrusted' networks. The MSSP market, on the other hand, is highly fragmented, and thus consolidation of small, regional players is common. Further, as firms are stretched for resources and searching to replace manual processes, security services are in increasing demand.

Data security rounded out the top three, with 21 transactions, adding six deals for the largest year-over-year increase of any category. On the negative side, threat protection showed the biggest decline, with 18 transactions vs. 26 in 2019, although still good enough for fourth place overall. Sector preference among buyout shops mirrored overall consolidation activity, with IAM, data security and MSSPs leading the way in terms of PE investments as well as strategic tie-ups.

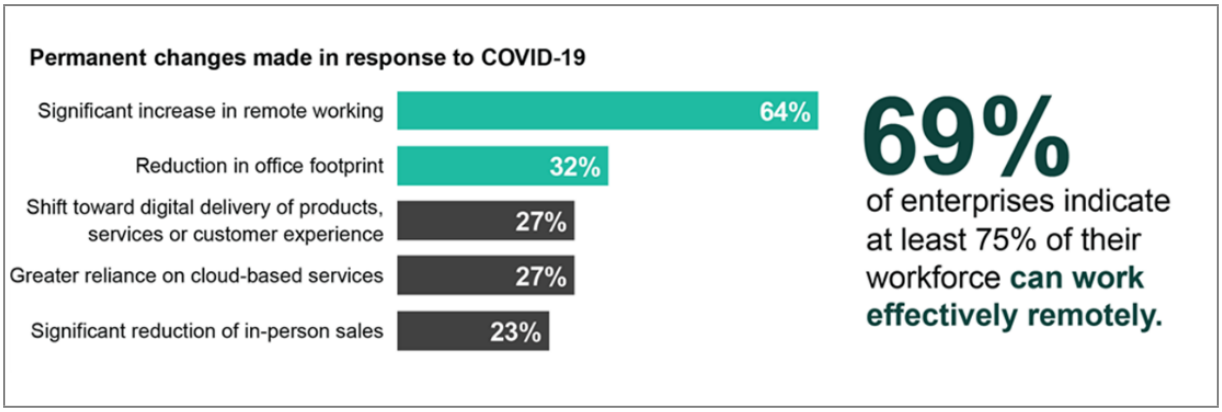
Macro-level drivers

Securing remote work

While 2020 did many things in technology, one of the most visible impacts was the shift to remote work. As 451 Research's VotE survey data indicates, 69% of enterprises claim to have three-fourths of their employees working effectively remotely. Said otherwise, what had been an exception became the rule and security teams scrambled to adapt. Securing remote work and doing it at enterprise scale became one of the year's more urgent projects, which increased focus on the providers and technologies that could get it done, spurring a substantial number of acquisitions.

The emergence of the secure access service edge (SASE) concept was an embodiment of the desires of many for scalable and secure access infrastructure, but a growing amount of hype around the idea has clouded market realities. Enterprise shifts to new access models are inevitable, but will take time for the broad market. This has driven several deals that are looking to lash together SD-WAN, zero trust, identity, and other poorly defined technologies into a larger, security-centric whole, which will likely play out in dealmaking over the next few years.

COVID-19-Inspired Practices Become Permanent Policy



Source: 451 Research's Voice of the Enterprise: Digital Pulse, Coronavirus Flash Survey October 2020
Q. Which, if any, of the following permanent changes has your organization made due to the influence of the pandemic? Please select all that apply. (n=378)
Q. Approximately what portion of your organization's workforce is unable to work effectively remotely? (n=345)
Base: All respondents

Evolution of cloud usage means newer challenges

Even amid the disruption caused by the lockdown, organizations have continued their long-term journey of increasing cloud adoption. For many, this means adopting SaaS-delivered functionality covering a multitude of use cases. For many others, it's deploying infrastructure in IaaS or PaaS with compute taking place in hosted cloud environments, on-premises, or on edge locations. Indeed, having a multitude of technology options, each increasingly tailored to specific nuances, gives organizations tremendous resources to achieve their objectives.

This reality presents a host of challenges for security teams seeking to support these efforts. Whether ensuring that the growing number of niche SaaS vendors are following proper security practices or supporting multiple cloud teams, security personnel are scrambling to update their skillsets, processes and tooling to support both the distributed nature of cloud as well as the consistency needed to maintain the organization's overall security posture.

Vendors have approached this from different perspectives. Cloud service providers have poured significant resources into offering security functionality on their clouds, often with strong support for automation and APIs. There's also an increasing number of third-party suppliers, large and small, that have latched on to these APIs both to deploy cloud services themselves as well as offer a layer of security functionality across multiple cloud providers.

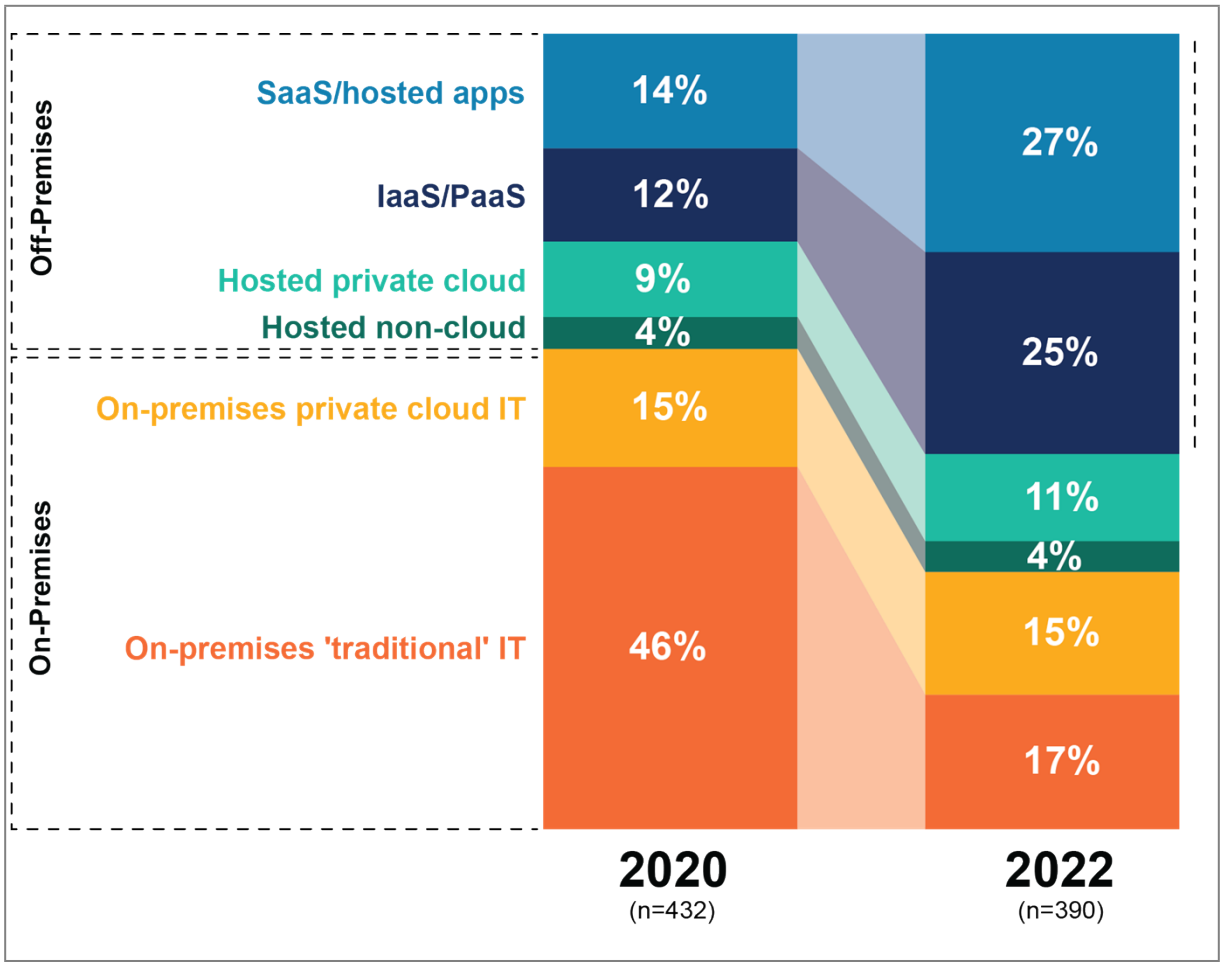
As they consider how to tackle cloud security governance, customers have demonstrated an increasing interest in attaching themselves to more familiar governance patterns and processes rather than create entirely new approaches. From a technical perspective, there is growing interest in framing cloud security policies around topics such as data handling, audit and compliance, and identity management, which will likely drive the latest activity in cloud security M&A.

The challenge of covering an expanding attack surface

In part because of the pandemic, the attack surface has been stretched in many ways, not least being the extension of the enterprise network into home and remote environments, where the consistency and reliability of security controls may be less than certain. At the endpoint, the move toward personal and mobile devices has been going on for years. Now, with the proliferation of operational technologies and IoT, the number of connected devices in the enterprise (not including

consumer devices) is expected to grow by 2024 to roughly 75%, more than the nearly eight billion total of a year ago, according to 451 Research's IoT Market Monitor. The rise of 5G is projected to stretch the enterprise edge even further. At the other end of the spectrum, enterprises expect the sheer variety of deployment models at the center of IT to run the gamut.

Increased Complexity: IT Workloads Will be Deployed Across a Variety of Models



Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Workloads & Key Projects 2020

Q. Which of the following best describes the primary environment used to operate your organization's workload today?

Q. Which of the following best describes the primary environment in which your organization's workload will be operated two years from now?

Base: Respondents with workloads/applications

The integration of applications with each other via APIs is a further example of how exposures and dependencies can grow, while incidents from the exploit of vulnerabilities embedded in open source software to the recent SolarWinds breach exemplify how dependencies on the IT supply chain can have a cascading effect from one supplier to the next, and ultimately to the end user.

For years, IT security has focused on 'going deep' to better understand the details of adversaries and their tactics, and how best to disrupt the sequence of an attack. However, the joint influences of cloud, mobility, edge – and now, the work-from-home (WFH) phenomenon – mean that applications, workloads, infrastructure and users are highly distributed.

While these trends have certainly provided benefits – in elasticity, scale and performance at IT's center, plus a stunning range of adaptability at the edge – they have also driven complexity. It follows that infosec now must 'go wide' as well to help enterprises cope with the growing scope of their exposures, which may go some way toward explaining the increased frequency of 'platform' strategies that attempt to bridge multiple risk domains and security product categories via go-to-market partnerships, technical integrations and M&A.

VC funding as a macro-level driver

In addition to products and M&A, investment in cybersecurity is also at or near record levels in venture capital. Pre-exit funding rounds are now reaching levels previously anticipated only upon IPO or acquisition. Just in the past 12 months, cybersecurity companies have scored at least 14 rounds at or above $100m, according to S&P Global Market Intelligence data, with perhaps no better illustration than Lacework's notably massive recent $525m series D round.

Not all of these nine-figure VC rounds are late-stage. OneTrust and KnowBe4 each raised $300m C rounds, while Wiz brought A rounds to nine figures with a $100m December 2020 raise, succeeding the likes of QOMPLX (fka Fractal Industries) and its $76m A round in 2019. The security unicorn crowd has grown accordingly, and now includes – but is not limited to – Armis, Auth0, Netskope, Snyk and SentinelOne.

How does this impact consolidation? For starters, by fueling the continued growth of the security market with new vendors, which are now approaching a total of 4,000, compared with less than 1,000 barely a decade ago – in other words, by increasing the supply of potential targets. On the demand side, ample capital gives firms an alternative to the public markets as an avenue for liquidity events, which frequently culminate in a sale to a strategic or financial acquirer.

Micro-level drivers

SASE and ZTNA

As noted, WFH has almost become a standard expectation and long-term strategy for an increasing number of firms. While the nascent zero trust phenomenon had catalyzed several acquisitions of vendors providing what is called variously software-defined perimeter (SDP) or, increasingly, zero trust network access (ZTNA), both are essentially new names for remote access technologies. While we have already seen several SDP/ZTNA specialists scooped up (e.g., Luminate, Meta Networks, Odo Security, Pulse Secure, Vidder) by a varied range of potential suitors, the space remains one of the more crowded in security and thus should provide a buyer's market for interested parties.

Remaining names include AmZetta, AppGate, Axis Security, Banyan, Ericom, NetMotion, Safe-T and Wandera, while potential acquirers will likely continue to span multiple categories, such as network security (Fortinet, Palo Alto, SonicWALL, WatchGuard), privileged access management (PAM; BeyondTrust, One Identity, Thycotic), or IAM (OneLogin, Ping Identity). Broader IT suppliers could also have a stake in the race, including IBM, Oracle and VMware.

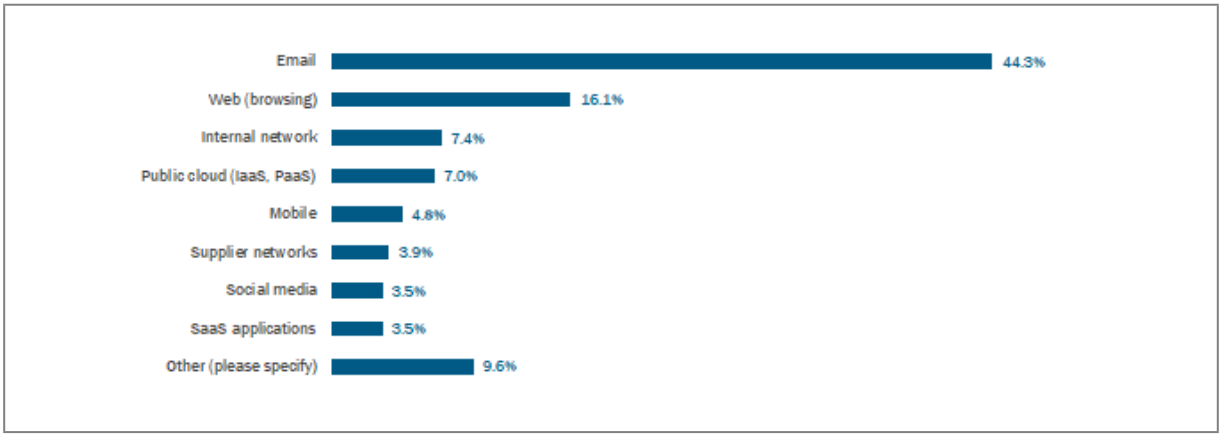
Security operations and the impact of XDR

Even before the pandemic, security teams were under the strain of inefficient security operations workflows – too many alerts, many of them false positives, too much effort to correlate information across sources, and so on. Fixing these underlying technical issues will likely have a positive effect on bigger topics, from improving resilience against increasingly capable attackers to addressing some of the ongoing concerns about staffing and skillsets.

Extended detection and response (XDR) has emerged as a possible approach to address these issues. While they have different flavors, XDR offerings basically come with prepackaged integrations of different sources of telemetry, fused with domain knowledge aimed at addressing common security operations use cases. The space has seen many releases, with products from Palo Alto, Trend Micro, Microsoft, FireEye, and many others. Still, there is plenty of possible activity left. Strategic vendors such as Check Point, Fortinet and VMware are ramping up their offerings and messaging and may be interested in accelerating via acquisitions, be it newer telemetry sources or analytic engines.

Buying brand-new telemetry sources may be trickier to ingest, although we can envision email security vendors making an increased contribution to threat detection and providing this insight to security operations, given how email is regarded as a key vector for attacks (see figure below). Email security specialists now in this market such as Inky, GreatHorn, Abnormal Security, and others may be of potential interest.

Greatest Security Threats for Organizations and Their Data



Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2020
Q. When it comes to data security, which one of the following do you think poses the greatest security threat to your organization?
Base: All respondents (n=230)

Alternatively, XDR firms may want to ingest new telemetry data via API integration. If thinking about acquiring analytic engines, though, specialists such as Hunters.ai, Confluera, Stellar Cyber and Kognos, among others, may attract attention.

Cloud identity and entitlements management

When thinking about an organization's efforts at governance over their cloud activities, the challenge of an expanding number of projects distributed across a multitude of increasingly heterogeneous technology choices makes it virtually impossible to keep up using a traditional security approach – too many details, moving too quickly, interacting in increasingly complex ways.

A relatively recent trend is the rise of the cloud identity and entitlement management (CIEM) niche, which is aimed at giving security teams a deeper look into how those interactions are expressed in permissions to access data or resources and controlling runaway 'permission sprawl.' The idea is to ensure that there are fewer opportunities for unintended overprovisioned access that could result in catastrophic breaches or security incidents.

Many security vendors – Palo Alto, DivvyCloud, CyberArk, Turbot, and others – have been building these capabilities organically, leveraging the open nature of cloud APIs. Still, specialists such as

Adaptive Shield, AppOmni, Authomize Britive, CloudKnox, Ermetic, Obsidian, Sonrai, and others may be of interest to shoppers looking to dive deeper into cloud permissions. We have seen some dealmaking – e.g., Varonis' pickup of Polyrize – and we could see other data governance and identity governance providers get in on the fun. PAM suppliers such as Thycotic, OneIdentity, BeyondTrust and IBM may also be interested, as may other cloud security vendors such as Trend Micro, Lacework, Check Point, VMware, and others.

Application security: Don't let bots spoil another holiday season

Anyone who shopped over the holidays looking for a popular game console like the PlayStation 5 is now intimately familiar with the problem of bots, automated programs that interact with websites. Malicious bots concerned with account takeover (ATO) in particular have seen advances in tooling, services to spread out an attack, and credentials harvested from a handful of large-scale data breaches.

There have been several relevant acquisitions in the bot detection and mitigation space, led by F5's pickup of Shape Security and including Radware's reach for ShieldSquare, Imperva's Distil Networks buy, and Equifax's recent purchase of Kount. This largely reflects the idea of putting bot detection alongside web application firewall offerings. The WAF space itself saw significant deals this year when Fastly nabbed Signal Sciences, while Thoma Bravo took Imperva private in 2019. Imperva had long been a recognized name in the WAF category with bot detection capabilities of its own, and was one of the last WAF-centric providers showing a wide install base in our VotE: Information Security studies.

There are also several largely pure plays in the bot detection arena. The Goldman Sachs Merchant Banking Division along with two partners purchased White Ops in December. PerimeterX, DataDome, Reblaze and Cequence have all received funding in the category. While Fastly CDN competitor Cloudflare is more known for acquiring smaller startups, Akamai, which has a foothold in this sector, has not shied away from larger acquisitions. A major network security provider with a WAF (Fortinet, Citrix?) may also determine that the nuances of bot mitigation fit well with existing web application security offerings and decide to upgrade via M&A, as F5 did. AWS and Azure, more known for building capabilities themselves, both have increasingly employed WAF offerings and have nonetheless printed purchases driven by security expertise as well.

Security validation and attack surface management

Most security teams find it difficult to confidently answer key questions about their organization's security posture. Is the security infrastructure keeping pace with adversarial tactics? What threats or attacks would have the greatest impact on the business if they were to occur? Is the organization prepared to detect and respond to the latest attacks? Is the stack of security tools and controls that have been invested in working effectively and as expected? Are we aware of the organization's entire digital footprint?

The inability to answer these and similar questions is fueling increased spending on security tools that can help organizations gain insights into their security posture to better understand how they can construct a more resilient cybersecurity program. Continuous and automated testing and validation platforms and services, including automated penetration testing, breach and attack simulation, automated red teaming, and attack surface discovery, can simplify resource-intensive tasks, enabling security teams with limited or overburdened expertise to continuously test, measure and assess the effectiveness of their organization's security posture.

Security validation and attack surface management platforms are becoming increasingly attractive to MSPs and MSSPs, as well as MDR and XDR providers. We have already seen movement in this area with Palo Alto acquiring attack surface management vendor Expanse and ReliaQuest buying breach

and attack simulation provider Threatcare. SafeBreach, Picus Security, Cymulate, AttackIQ, Randori, Pcysys and XM Cyber have all received funding over the past couple of years.

Traditional security assessment firms and cyber-insurance providers are also likely to make moves in this space. For traditional security assessment specialists, security validation and attack surface management technologies offer an opportunity to offload repetitive and mundane processes and scale their operations, but more significantly, they provide a path to offering managed services that incorporate the advantages of continuous automated testing with the benefits of traditional, manual testing. For cybersecurity insurance suppliers, automated testing and validation could provide insurers with a standardized risk score, enabling more accurate premium and risk calculations as well as greater transparency with customers.

The security services opportunity among smaller regional players

Many factors are driving consolidation in the regional security service-provider space as both MSSPs and MSPs seek to expand capabilities, gain a larger market share, and boost their valuation. The lack of available and affordable cybersecurity talent may be one of the most prevalent factors impacting security service providers, driving many to turn to M&A to find additional talent. However, when it comes to talent, dealmaking is not always just about gaining more people (as with so-called 'acq-hires'). Often, it is about obtaining new technologies and capabilities that can offset a lack of talent and expertise with greater levels of efficiency and scalability.

Regional security service providers continue to be attractive targets for buyers and investors due to their recurring revenue streams, strong growth trends fueled by the ever-increasing threat posed by cyber-criminals and the shortage of cybersecurity expertise, and the ability to scale operations. Many MSPs, SIs, MSSPs and consultancy firms are aiming to ink acquisitions in this space as they seek to expand their portfolios and provide one-stop shopping for their customers. Others are pursuing M&A to expand into new geographic regions, enter new verticals, or reach critical mass and scale to counter larger rivals.

Reaching critical mass and generating rapid growth has fueled several purchases in the regional security service-provider segment over the past couple of years, a trend that should continue in 2021. Among the numerous acquisitions in this category, we saw Terra Verde, TruShield Security Solutions, and Sword & Shield Enterprise Security come together in 2019 to form Avertium; and in March of last year, Dyonyx and Single Path merged to form Dyopath to offer managed IT and cybersecurity services nationwide.

Where else might security go wide?

In preceding descriptions of micro-level drivers, we talked about the many opportunities acquirers have to fill gaps in the need to go wide, with better visibility across a growing and dynamic attack surface. Buyers have already recognized the value of areas such as the continuous automated validation of security controls through deals such as FireEye's pickup in 2019 of Verodin, while XDR expands the context necessary to threat detection and response. Services help close the gaps of expertise required to make the most of these opportunities. What other moves might potential buyers explore in 2021?

Just getting a handle on the extent of exposure was reason enough for Palo Alto to reach for Expanse, which indicates that acquirer interest in this broad concern remains active. Other markets, however, may not be giving such strong signals. In domains such as managing vulnerabilities in open source, for example, software composition analysis vendors have been in the market for a few years already, while GitHub had offered a software dependency graph since before its sale to Microsoft.

Meanwhile, players like Axonius and Panaseer have taken a more modern approach to asset inventory, with the former winning the Innovation Sandbox competition at the 2019 RSA Conference US. Since then, however, vulnerability management incumbents such as Qualys, Rapid7 and Tenable have added asset inventory approaches to their portfolios, as well as varying degrees of vulnerability prioritization offered by startups like Kenna.

In other markets, third-party cyber-risk management has been a topic of interest for some time, but with limited scope and little M&A momentum to date. The impact of incidents such as the SolarWinds breach and the extent of exposure it reveals could enliven interest in many of these fields, perhaps raising the bar on the level of innovation needed to motivate buyers. Certainly, just going by network scans and questionnaires alone won't be enough to deliver the kind of visibility needed to defend against such threats to the IT supply chain.

Rise of the SPAC?

A special-purpose acquisition company, or SPAC, is an investment vehicle that allows a vendor to form without commercial operations and raise capital through an IPO for the purpose of acquiring a company later on. The concept has been around for some time, but the capital amounts flowing into this type of instrument have been increasing steadily, from $1.8bn in 2014 to $13.6bn in 2020. Last year was notable in particular for the number of suppliers to the autonomous and electric vehicle space that chose this route to additional capital rather than a traditional IPO, including Velodyne, QuantumScape, Fisker and Lordstown Motors.

This begs the question of whether infosec, a segment where many startups seem to develop features that appear to be intended for eventual integration into larger platforms, could see greater future usage of SPACs. In January, SCVX went public with just that purpose to acquire a 'cornerstone' security firm capable of consolidating other security technologies into an overall platform.

IPO candidates

Last year was a bit of a letdown for infosec IPOs, with just two vendors crossing the public threshold (McAfee and Sumo Logic) compared with four each in 2019 (Tufin, Ping Identity, Crowdstrike and Cloudflare) and 2018 (Avast, Carbon Black, Tenable and Zscaler). In addition to McAfee and Sumo Logic's IPOs, we removed Checkmarx from the list following its sale to Hellman & Friedman for $1.2bn, and also nixed digital certificate and key management specialist Venafi following a recent majority investment from Thoma Bravo.

This year's list adds two new names: Auth0 and Darktrace, while ForgeRock returns to the roster following a CEO change and refocus. Other vendors that could be IPO candidates in the near future but are not on our top 10 list include BlueVoyant, Centrify, ExtraHop, GitLab, Lookout, Malwarebytes, Pindrop, Sysdig and Tanium.

Security IPOs Since 2017

Year	Company	Amount raised
2020	McAfee	$740m
2020	Sumo Logic	$326m
2019	Cloudflare	$550m
2019	Crowdstrike	$612m
2019	Ping Identity	$188m

2019	Tufin	$108m
2018	Avast	$200m
2018	Carbon Black	$152m
2018	Tenable	$251m
2018	Zscaler	$192m
2017	Okta	$187m
2017	ForeScout	$116m
2017	SailPoint	$240m

Source: 451 Research's M&A KnowledgeBase, January 2021

Auth0: The customer- and developer-focused IAM high-flyer crossed into unicorn status after raising a $120m series F round that brought its total funding to over $330m. Auth0 is now the eighth cybersecurity provider to have raised north of $300m, according to the M&A KnowledgeBase (along with Netskope, Cybereason, Illumio, KnowBe4, SentinelOne, Sumo Logic, Tanium and Tenable).

Exabeam: The vendor has challenged the SIEM market with user and entity behavior analytics that help reduce false positives for enhanced security operations. The addition of security orchestration, automation and response capabilities has further bolstered its position as a security operations contender. Its total funding of $193m was last augmented by a $75m round in May 2019.

Cybereason: The firm's last raise was a $200m round in the summer of 2019, bringing its total haul to $390m. Its next move might very well be a dip in the public markets. If it did so, Cybereason would be putting forward a message built around how its endpoint-centric platform also supports use cases such as cloud workload protection and extended detection and response.

Darktrace: The network threat detection and response player has made much of its AI investments and now includes email as well as operational technology and industrial IoT security in its portfolio. Darktrace has not raised capital since a 2018 round brought its total financing to $230m, but once again appears to be bound for an exit. Existing penetration gives it a base from which to target continued growth as networks expand beyond the traditional enterprise.

ForgeRock: The open source IAM supplier with a strong focus on customer IAM raised a $94m series E round early in 2020 that brought its total funding to over $230m, which the company said would be its final raise before going public. ForgeRock was a perennial IPO contender until a CEO change several years ago, and 2021 could finally be its year.

Illumio: The company's latest raise is a $65m series E back in February 2019, leaving it with $333m in total, so the timing might favor another transaction, perhaps even a public one. Illumio also just added a board director with prior IPO experience, and has focused its messaging around the popular theme of zero trust. It also recently expanded its portfolio to better cover endpoints and cloud security use cases.

KnowBe4: The vendor has built an impressive library of anti-phishing content and security awareness training, augmented by acquisitions ranging from content producers to providers of security culture measurement. KnowBe4's total funding of $393m includes a $300m round fielded at a unicorn valuation in 2019.

Netskope: The CASB pioneer has raised $400m and recent moves into web security and zero trust network access could help Netskope tap into enthusiasm for the new secure access service edge paradigm.

SentinelOne: The firm has been on possible IPO lists before and instead of going public in 2020, it landed not one but two large funding rounds, bringing its total to just shy of $700m. SentinelOne has worked hard at growing beyond its endpoint roots and its platform now supports environments such as cloud and IoT, as well as several use cases spanning security and operations. It is also pursuing the XDR theme.