Imagine 2025

Faster to the Future; Thinking through the evolving Security Software landscape

EQUITY RESEARCH | JULY 6, 2020

For required conflicts disclosures, please see page 36.

Disseminated: Jul 6, 2020 00:43ET; Produced: Jul 6, 2020 00:24ET

RBC Capital Markets, LLC
Matthew Hedberg (Analyst)
(612) 313-1293
matthew.hedberg@rbccm.com
Dan Bergstrom (Analyst)
(612) 313-1254
dan.bergstrom@rbccm.com
Alex Zukin (Analyst)
(415) 633-8659
alex.zukin@rbccm.com
Matthew Swanson (AVP)
(612) 313-1237
matthew.swanson@rbccm.com

July 6, 2020

Faster to the Future; Thinking through the evolving Security Software landscape

Imagine 2025...and beyond

COVID changes everything and moves security Faster to the Future: While mega-trends such as cloud adoption and digital transformations seem well-established, we believe COVID could accelerate changes in the security fabric by up to five years which could dramatically change the security landscape. Key trends worth watching include the Secure Access Service Edge framework (SASE) and Zero-Trust Network Access (ZTNA).

Key components of the 2025 and beyond Security stack:

- **Cloud Security/Application Access and Security:** As we look beyond 2025 and in the context of SASE and ZTNA, we believe cloud security including application access & security takes on a new level of importance and expands sub-categories of spending such as application and data security while potentially cannibalizing or superseding existing infrastructure and network security. We believe this is being driven by the "perimeter" moving further out to the "edge" and closer to the user that could accelerate in a post COVID world with more distributed workforces.
- **Identity:** Over the next five plus years as cloud security/SASE takes hold, adoption of Identity solutions is likely to increase as well as the potential to expand the TAM. As such, we believe protecting identities of workers, customers, and increasingly APIs/bots will likely increase in importance.
- **Protecting Workloads:** Historically, we would have referred to this category as Endpoint Security or Anti-Virus but as we think in a post COVID world, the idea of endpoint security is limiting. As such, we believe the more important category will be protecting workloads. These workloads could certainly exist on traditional endpoint devices (laptop, etc.), but also and increasingly exist in the public cloud as ephemeral workloads. As a result, we think with higher levels of WFH and a faster migration to public and hybrid compute, the broad category of workload security increases.
- **Security Monitoring/Visibility:** We are bullish on monitoring/observability beyond 2025 and believe the sub-category of security monitoring (generally SIEM and SOAR) could be increasingly important given an evolving network/security landscape.

Vendors to watch post COVID:

- **CRWD:** Should benefit from the need to protect devices and workload wherever they reside; more than just AV & desktops/laptop protection legacy AV vendors addressed.
- **NET:** Cloud-based platform should benefit from greater use of internet due to global PoP network, higher levels of remote workers and zero-trust application access.
- **OKTA:** Security around point of access, which requires identity to provide context around user and device; could consolidate Identity spending beyond SSO/MFA.
- **PANW:** Of the firewall vendors, we believe PANW could be best positioned to leverage cloud-security trends (Prima Access), but need to offset a reduction in on-premise firewalls.
- **SPLK:** We think a focus on SIEM and SOAR as an aggregator puts SPLK in an interesting position to help consolidate security spend.
- **VMW:** Could be in a unique position to consolidate spend (endpoint, SD-WAN, etc) and also move deeper into adjacent categories such as ZTNA.
- **ZS:** Control plane, or digital/intelligent switchboard, enables secure connection to any application from any device/location; benefits from ZTNA.
- **Overall category of Identity**: In addition to **OKTA**, we also think **PING** and **SAIL** can benefit from an increasing TAM.
- **Others**: **AKAM** (global PoP network), **CSCO** (global network footprint), **Azure/AWS/GCP** (global Internet traffic/bandwidth).

Priced as of prior trading day's market close, EST (unless otherwise noted).
All values in USD unless otherwise noted.
For Required Conflicts Disclosures, see Page 36.

Faster to the Future – Thinking through the Security landscape longer-term

RBC Capital Markets

Matt Hedberg (Analyst) (612) 313-1293 matthew.hedberg@rbccm.com

All values in US dollars unless otherwise noted.

Table of contents

All statements in this report attributable to Gartner represent RBC Capital Markets' interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this report). The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.

If you read only one slide

Everything changes post COVID, as we believe many enterprises will move faster to the security future

- **COVID changes everything and moves security Faster to the Future:** While mega-trends such as cloud adoption and digital transformations seem well-established, we believe COVID could accelerate changes in the security fabric by up to five years which could dramatically change the security landscape. Key trends worth watching include the Secure Access Service Edge framework or "SASE" as well as a variety of sub-categories such as Zero-Trust Network Access or "ZTNA".
- **Key components of the 2025 and beyond Security stack:**
  - **Cloud security/application access and security:** As we look beyond 2025 and in the context of SASE and ZTNA, we believe the broad category of cloud security including application access & security takes on a new level of importance and expands sub-categories of spending such as application and data security while potentially cannibalizing or superseding existing categories such as infrastructure and network security. We believe this is being driven by the "perimeter" moving further out to the "edge" and closer to the user that could accelerate in a post COVID world with more distributed workforces.
  - **Identity:** Within the broad category of Identity, we think of three main sub-categories: 1) SSO/MFA, 2) Governance, and 3) PAM. Over the next five years as cloud security/SASE takes hold, adoption of Identity solutions is likely to increase as well as the potential to expand the overall Identity TAM. As such, we believe protecting identities of workers, customers, and increasingly APIs/bots will likely increase in importance.
  - **Protecting Workloads:** Historically we would have referred to this category as Endpoint Security or simply Anti-Virus but as we think in a post COVID world and as we look beyond 2025, the idea of endpoint security is limiting. As such, we believe the more important category will be protecting workloads. These workloads could certainly exist on traditional endpoint devices (laptop, etc.), but also and increasingly exist in the public cloud as ephemeral workloads. As a result, we think with higher levels of WFH and a faster migration to public and hybrid compute, the broad category of workload security increases.
  - **Security Monitoring/Visibility:** We are bullish on monitoring/observability beyond 2025 and believe the sub-category of security monitoring (generally SIEM and SOAR) could be increasingly important given an evolving network/security landscape.
- **Vendors to watch post COVID:**
  - **CRWD:** Should benefit from the need to protect devices and workload wherever they reside; more than just AV & desktops
  - **MSFT:** Should benefit from increased levels of O365 and add-on security services; more focused on security than ever
  - **NET**: Cloud-based platform should benefit from greater use of internet/remote workers and application access
  - **OKTA:** Security around point of access, which requires identity to provide context around user and device
  - **PANW:** Of the firewall vendors, we believe PANW could be best positioned to leverage cloud-security trends (Prima Access)
  - **SPLK:** We think a focus on SIEM as an aggregator puts SPLK in an interesting position to help consolidate security spend
  - **VMW:** Could be in a unique position to consolidate spend (endpoint, SD-WAN, etc) and also move into adjacent categories
  - **ZS:** Control plane, or digital/intelligent switchboard, enables secure connection to any application from any device/location
  - **Overall category of Identity:** In addition to **OKTA**, we think **PING** and **SAIL** can benefit from Identity TAM increases
  - **Others: AKAM** (global PoP network), **CSCO** (global network footprint), **Azure/AWS/GCP** (global Internet traffic/bandwidth)

Source: RBC Capital Markets, company reports

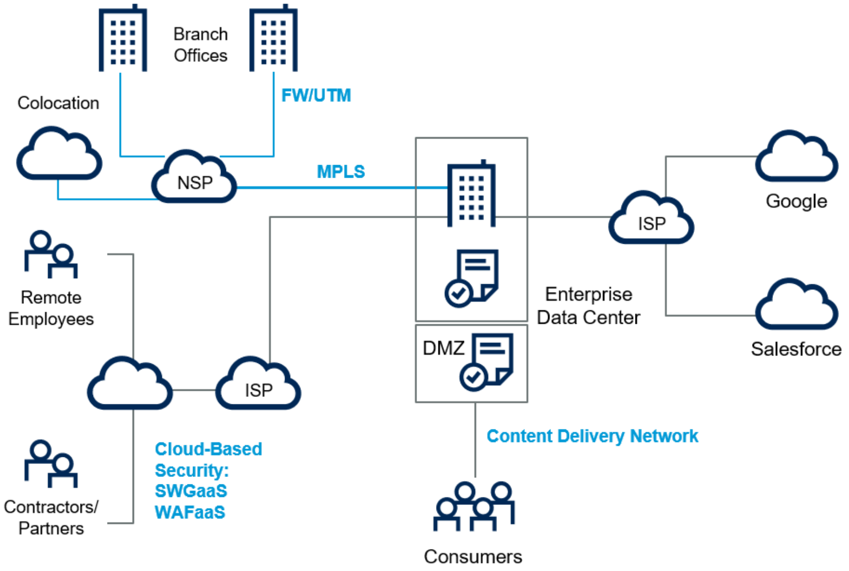
Important building blocks of Security through 2025 and beyond

Part 1

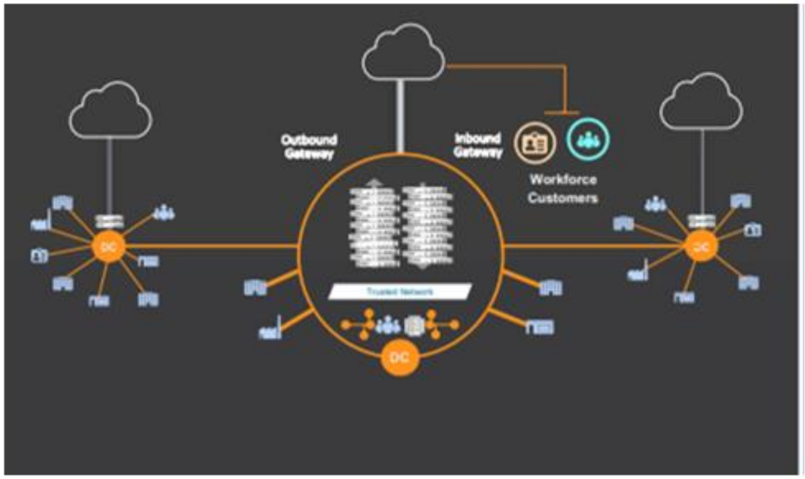
COVID changes everything and moves Security "Faster to the Future"

- Traditional networks were built around on-premise data centers, which made sense in a pre-cloud world.
- When desktops, data, software, applications and users all resided within the traditional network perimeter, this strategy was effective, but as endpoints and workers became distributed and the rise of the cloud sent software and applications off-premise, enterprises needed to increasingly modify the network perimeter to accommodate the "new normal" of work.
- As enterprises found out recently with COVID, this traditional infrastructure was never designed to scale out when companies tried to adapt continuity plans which were typically for 15-20% remote workers that went to 100%.
- While workers and devices being remote may be new, the software, applications, services and data have become increasingly remote over the past several years.
- As seen in the image to the upper right, branch offices, remote employees and cloud-based applications all have had their own software and services developed to work back into this datacenter-centric security design.
- With the rapid push toward distributed workforces due to COVID, employees and their devices have now joined applications and data in residing off-premise, changing the paradigm for the center of network security, which is now the individual user and the cloud vs a hub and spoke design around the datacenter.
- As we look to the future and to enable this new normal, we believe several new aspects of security will come into focus; most notably SASE (Secure Access Service Edge) and ZTNA (Zero-Trust Network Access).

Traditional Data Center-Centric, Hub and Spoke Network and Network Security Architecture
Data-Center-Centric Networking and Security Model



Legacy IT world



.

Source: RBC Capital Markets, Gartner, "The Future of Network Security Is in the Cloud" by Neil MacDonald, Lawrence Orans and Joe Skorupa on August 30, 2019

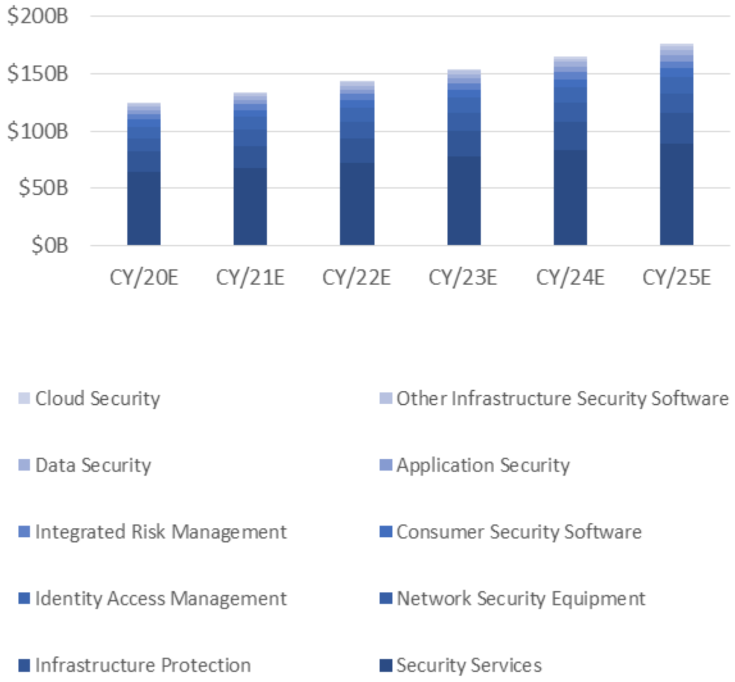
What legacy market share could be up for grabs though 2025?

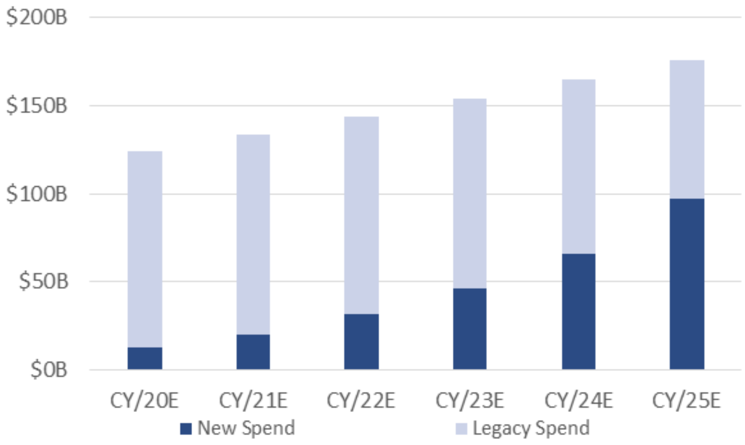
- **We believe there is a significant amount of legacy market share that could be available through 2025**

  - Gartner currently sizes the Information Security and Risk Management market at $124 billion in 2020, which we believe could reach $176 billion in 2025, representing a CAGR of 7.3%.

  - Of this amount, we believe approximately 90% could be considered legacy spend and could be ripe for disruption. We expect a rapid shift to new spend driven by digital transformation which we believe could be accelerated by five years due to COVID.

  - **By our estimate, just over 50% of legacy spend, or $97 billion could be available for displacement through 2025, which would represent a CAGR of 51%.**

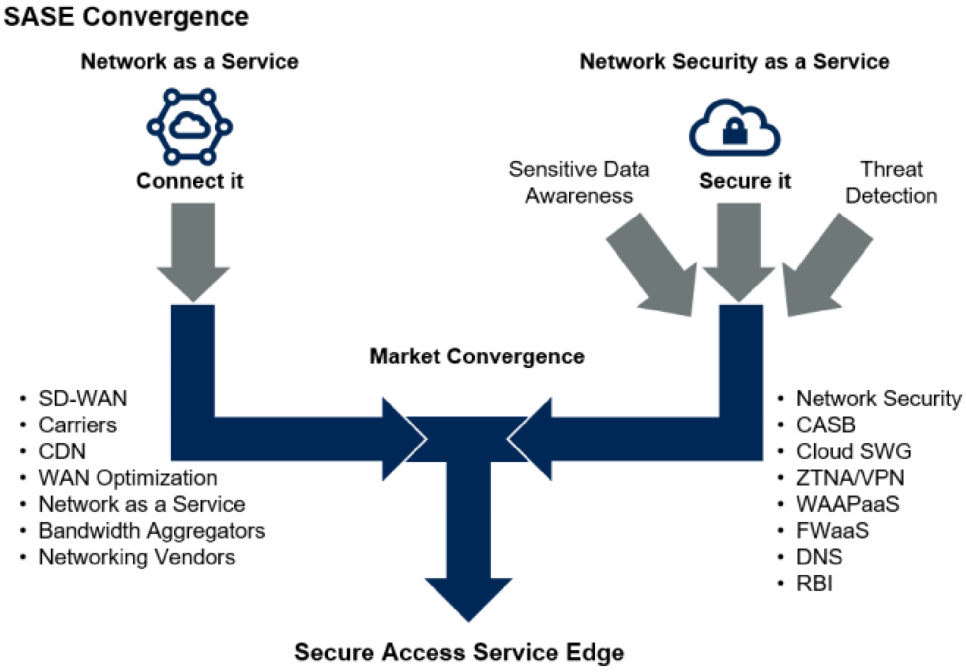




Source: RBC Capital Markets, Gartner “Forecast: Information Security and Risk Management, Worldwide, 2018-2024, 1Q20 Update” by Rustam Malik, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John Wheeler, Mark Driver, Nat Smith on June 17, 2020, RBC Capital Markets

Where we are headed: A SASE future

- We view the future as enterprises moving from surviving to thriving in a distributed work environment.
- The Secure Access Service Edge or "SASE" is a security strategy to support the digitization of the enterprise and the dissolution of the traditional network perimeter allowing for security at the point of access.
- SASE converges network (SD-WAN) and network security services (such as SWG, CASB, FWaaS and ZTNA) and is primarily delivered as a cloud-based service.
- Gartner predicts that by 2024 at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018.
- Security needs to follow users to remote endpoints and allow access to data, applications and services which are increasingly also outside the data center.
- SASE is enabled by policy based security that can be applied at the point of access revolving around the ability to properly identify endpoints and users and understand access requirements.
- This type of dynamic policy-based security requires a next-gen solution that can combine the speed and scale of the cloud-based environments they are securing.
- One of the key tenets of SASE is zero trust security, an area we will go deeper into. This builds on the idea that access needs to focus on people, not IP addresses. The assumption that all networks are hostile leads to secure policy-based controls.

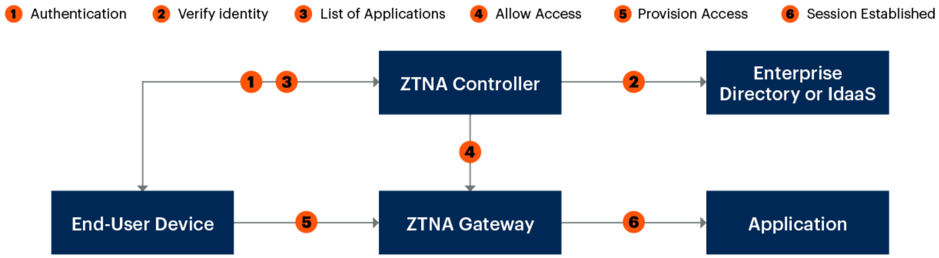


Source: RBC Capital Markets, Gartner, "The Future of Network Security Is in the Cloud" by Neil MacDonald, Lawrence Orans and Joe Skorupa on August 30, 2019

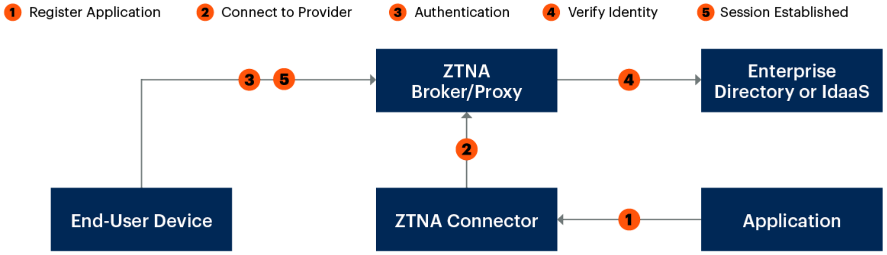
Where we are headed: Zero-Trust Network Access (ZTNA)

- Traditional networks and VPNs establish access that are often configured to allow excessive implicit trust and unpatched vulnerabilities, leaving enterprises at risk for attack.
- Digital transformation requires systems, services, and applications to be accessible through multiple mechanisms anywhere, anytime, from any device. This expands the surface area for attackers to target.
- ZTNA (Zero-Trust Network Access) provides identity-aware access. Removing network location as a position of advantage eliminates excessive implicit trust, replacing it with explicit identity-based trust.
- ZTNA improves the flexibility, agility and scalability of application access, enabling digitally transformed businesses to function without exposing internal applications directly to the internet (they become invisible), reducing the risk of attack.
- Companies can have much more control over east-west traffic with fine grain application access without opening up the entire network. This idea of creating the least amount of privilege possible is consistent with the defensive approach of zero-trust.
- Secondarily, organizations rely on ZTNA to allow unmanaged devices and external partners to securely access applications without the need to trust the device connection.
- Recent movements to largely remote workforces have accelerated the adoption of ZTNA to address the hardware and bandwidth limitations of traditional VPN access.
- Firewall vendors saw an early boost from COVID as VPN capacity was ramped. While we think network-based firewalls will exist for a long time, we also believe over time some of those dollars could shift to support SASE and ZTNA strategies.

Conceptual Model of Endpoint-Initiated ZTNA



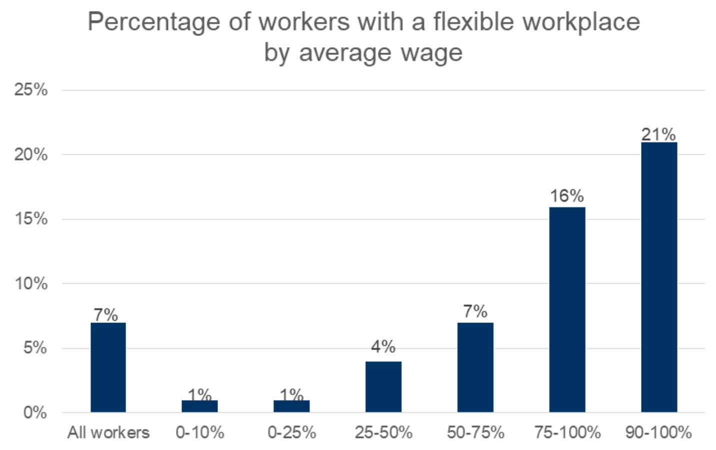
Conceptual Model of Service-Initiated ZTNA

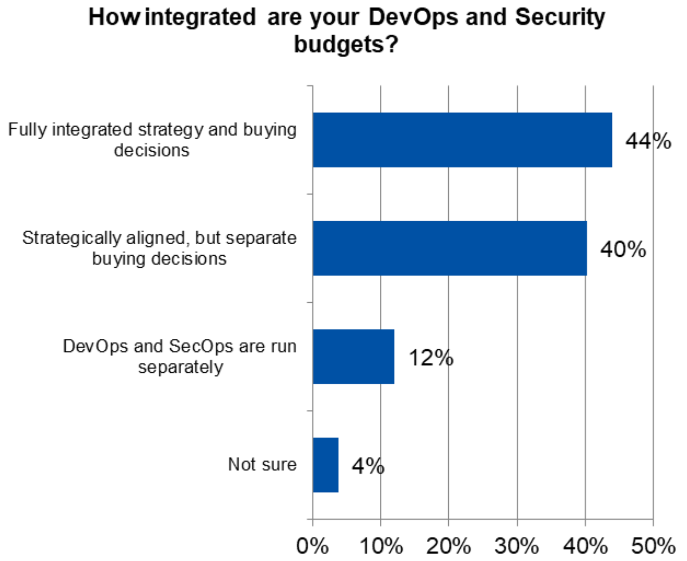


Source: RBC Capital Markets, Gartner, “Market Guide for Zero Trust Network Access” by Steve Riley, Neil MacDonald, Lawrence Orans on June 8, 2020

Is there a limit on workforce enablement in the balance of security?

- **Security as an enabler:** Security is now an enablement tool, built to find ways to say “yes”. We think security is going through a renaissance of turning traditional cost centers into sources of competitive differentiation. This is happening by moving beyond the original mission of creating a security organization to build walls to creating a security fabric to securely empower stakeholders.
- **Distributed work:** As seen on the right, at the highest salary levels (the 90-100% bucket), flexible work environments are already more normalized. We feel COVID could accelerate this trend showing that people at all levels can work efficiently remotely. To enable this, companies will need to embrace security that focuses on the user with zero-trust identity focused constructs. In doing so, we believe they could expand talent pools and increase retention without sacrificing security.
- **DevSecOps:** Looking at our 2020 IT Budget Survey of 186 CIOs, IT Directors, Architects, CTOs and developers, when considering the degree to which DevOps and Security budgets are integrated, 84% of respondents suggested they were either fully integrated or strategically aligned but separate buying decisions, while 12% said they were run separately. We feel this is a trend that will continue to increase, blurring the line between budgets creating new opportunities for integrated platforms leveraging common data sets with augmented algorithms.
- **Where is the limit?** We continue to view security and workforce enablement as a balancing act. What we have come to realize from conversations with vendors, customers and users is that the companies themselves don’t always get to control that balance. Not only does it benefit employee satisfaction and retention to let employees work from wherever and with whatever device and application they are most efficient, but it benefits security, because employees are likely to do these things anyway. The first step to securing a perimeter-less network is visibility. By embracing distributed workforces, unmanaged devices and business applications enterprises can gain a fuller network visibly and mitigate risk while driving efficiency. The key to this balance is context, identifying high-risk assets and access while enabling general work on a broader scale. This will accelerate the need for AI/ML as well as security at the new perimeter which is the user themselves.



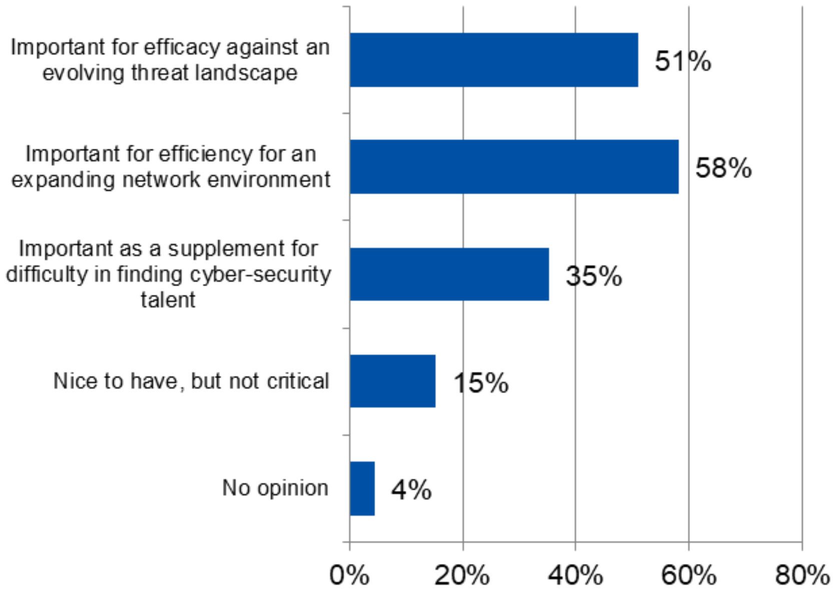


Source: RBC Capital Markets, company reports, 2019 National Compensation Survey, U.S Bureau of Labor Statistics

We need security software to do more of the heavy lifting

- **Large environments are being managed by fewer people:** We've seen consistent trends in our conversations with customers and security vendors toward automation and more managed security services. The shortage of cyber-security personnel has led to an increasingly competitive job market. This has led to fewer people managing expanding network environments. To do this we need more automation for repetitive tasks, more assistance for low-skilled workers and more efficiency for high-skilled workers.
- **Lack of talent:** According to a 2019 annual Cyber Security Workforce Study by (ISC)^2, the gap in cybersecurity talent has been widening and has reached a shortage of 4.07 million, meaning that the global workforce needs to grow by 145% to make up the gap. Within this study, 65% of organizations said to have a shortage of cybersecurity personnel with 51% saying their organization is at a moderate or extreme risk due to the shortage. When looking at graduation rates in computer science, we've seen relatively stable trends at 3-4% of bachelors degrees over the past decade. Given these trends, we feel it is unlikely more human resources are the answer in the near term.
- **AI/ML:** Looking at our 2020 IT Budget Survey of 186 CIOs, IT Directors, Architects, CTOs and developers, over half of respondents indicated AI/ML is important when evaluating security vendors to effectively deal with the evolving threat landscape (51%) and to deal with expanding network environments (58%). 35% suggested AI/ML was important to deal with the labor shortage in the security industry. Only 15% said AI/ML was nice to have, but not critical, when it came to evaluating security vendors.
- **Where these trends collide:** The idea around augmented intelligence is where we feel the security industry is moving. Increasing the amount of automation for low-skilled tasks like on-boarding and access provisioning as well as proactive defense for a better security posture, while increasing the efficiency of lower skilled workers to address low-risk and preemptive work while highly skilled tasks like threat hunting have better efficacy on alerts and assistance in remediation. Due to the shortage, cyber-security talent is more difficult to find and more expensive. The key is going to be making sure expensive assets are maximizing their time in the most important areas while software supplements for maintenance and low-skill tasks.

When evaluating security vendors, how important is AI/ML? (check all that apply)



Source: RBC Capital Markets, National Center for Education Statistics, (ISC)^2, company reports

What’s the role of public cloud vendors in security beyond 2025?

- **High level thoughts:**
  - We think public cloud providers will have an important role to play in securing cloud based workloads and applications…
  - …but will likely remain focused on increasing workloads and content as they could continue to leverage security partnerships.
  - For security vendors therefore, partnering and deep integration with Azure, AWS and GCP will likely gain increased importance over the next several years.
  - Additionally, while cloud providers may sell their own solutions, Microsoft is taking the lead here, we continue to believe enterprise customers will look to best of breed security providers as well as security platform vendors as a way to secure a multi-cloud compute and application landscape.

- **What do the public cloud vendors bring to the table?**
  - Massive scale in terms of global networks through built out point of presence (PoP)
  - Broad customer bases
  - ML/AI talent
  - Some of the best security engineers in the world
  - Reduced complexity and costs
  - A marketplace with security offerings from independent software vendors
  - Security learning/resources

- **What could change the game?** Following Microsoft’s lead, we believe AWS and GCP could add to their existing security posture, either organically or through acquisitions. It makes sense that basic security functions could be natively integrated into the various public cloud platforms, but feel enterprise customers will continue to pay for unique offerings that span multi-cloud environments while SMB vendors might standardize on a single cloud platform. To us the wildcard is GCP given their massive network scale and potential desire to leapfrog peers relative to existing security posture. The most logical areas of focus could be building out a ZTNA service.

Source: RBC Capital Markets, company reports

Potential security consolidators

- **Incumbency matters…but customers likely to look for what's best in the new landscape.** In addition to the likely continued investment in security by public cloud providers, we believe the following vendors could also be well positioned to consolidate aspects of security covered in this report including Cloud Security, Identity, Workload Security, and Security Monitoring. That said, we believe most large enterprise customers will continue to pursue best of breed security providers while the SMB market could likely see higher levels of spending consolidation. Potential consolidators likely include:

  - **Akamai.** The company has a disruptive security business today that could see them further leverage their global PoP network and internet traffic visibility. Their Enterprise Application Access service bears watching.
  - **Check Point.** As a core firewall vendor, we believe Check Point continues to push into growth areas beyond hardware-based firewalls. Outside of smaller tuck-in M&A deals, we would expect this to largely be an organic effort.
  - **Cisco.** The company has deep roots in security and has been aggressive in building out and acquiring additional security solutions, most recently Duo. We would expect additional investment in SASE and ZTNA.
  - **Cloudflare.** While the company isn't a classic security vendor, it is building out an impressive list of security solutions as we are most interested in Cloudflare for Teams.
  - **CrowdStrike.** We believe the company's cloud-based platform and intelligent agent is well suited to consolidate additional aspects of security and even DevOps spending.
  - **Fortinet.** As a core firewall vendor, we believe Fortinet continues to push into growth areas beyond hardware-based firewalls. We would expect a mix of M&A and organic investments as well as a focus on ZTNA to support their SD-WAN business.
  - **IBM.** The company has deep roots in security as we think it could look to add additional capabilities once Red Hat is fully integrated.
  - **Okta.** In addition to core SSO/MFA, we believe Okta could start to take share in Identity Governance and potentially PAM over time. This is most likely an opportunity in the SMB market.
  - **Palo Alto Networks.** Under new leadership, the company has been aggressively investing in M&A and organic development to build out a cloud-based platform. Of all the firewall vendors, we feel Palo Alto is further along this path via Prisma Access.
  - **Splunk.** We think the company has an opportunity to take share in the security monitoring market, which can help customers consolidate spend by leveraging Splunk's AI/ML capabilities.
  - **VMware.** The company is building out a wide range of security offering, largely via M&A, as we think the desire for additional security solutions is high. We would expect additional investment in SASE and ZTNA.
  - **Zscaler.** We believe the company is in a good position to consolidate levels of legacy network spend, most notably firewalls and VPNs via their early focus on ZTNA.

Source: RBC Capital Markets, company reports

ESG matters more

- **Environmental, Social and Governance (ESG)** criteria are a set of standards for a company's operations that socially conscious investors use to screen potential investments. Environmental criteria consider how a company performs as a steward of nature. Social criteria examine how it manages relationships with employees, suppliers, customers, and the communities where it operates. Governance deals with a company's leadership, executive pay, audits, internal controls, and shareholder rights.

- **We believe security companies will play an important role in ESG initiatives through 2025 and beyond.**
    - **Environmental:** We believe next generation security initiatives noted in this report such as secure remote application access (ZTNA) and a broad SASE strategy will help support higher levels of WFH, which can improve energy management and the reduction of carbon footprints, for example. Additionally, in terms of energy management, many security vendors work hard on reducing their energy consumption levels on a stand alone basis.
    - **Social:** This is likely the component that has the biggest ESG benefit through 2025 and beyond given many security companies noted in this report focus on customer privacy and overall data security. The Social aspect of ESG addresses management of risks related to collection, retention, and use of sensitive, confidential, and/or proprietary customer or user data. It also includes social issues that may arise from incidents such as data breaches in which personally identifiable information (PII) and other user or customer data may be exposed. It addresses a company's strategy, policies, and practices related to IT infrastructure, staff training, record keeping, cooperation with law enforcement, and other mechanisms used to ensure security of customer or user data.
    - **Governance:** In many regards tech companies including security vendors have also taken the lead in raising the awareness of corporate governance regarding issues. The category addresses a company's ability to ensure that its culture and hiring and promotion practices embrace the building of a diverse and inclusive workforce that reflects the makeup of local talent pools and its customer base. It addresses the issues of discriminatory practices on the bases of race, gender, ethnicity, religion, sexual orientation, and other factors.

- **ESG matters more:** In addition to all the direct benefits of being ESG aware and compliant, we believe that security vendors that follow and promote strong ESG standards could also be rewarded based on attracting new shareholders which will likely place an even higher importance on ESG through 2025 and beyond.

Source: RBC Capital Markets

Key components of the long-term security stack

Part 2

Key components of the long-term security stack

1. **Cloud security/application access and security:** As we look beyond 2025 and in the context of SASE and ZTNA, we believe the broad category of cloud security including application access & security takes on a new level of importance and expands sub-categories of spending such as application and data security while potentially cannibalizing or superseding existing categories such as infrastructure and network security. We believe this is being driven by the "perimeter" moving further out to the "edge" and closer to the user that could accelerate in a post COVID world with more distributed workforces.
   - **Key public vendors:** AKAM, CHKP, CSCO, FTNT, HPE, MSFT/Azure, NET, PANW, ZS as well as AWS and GCP
   - **Select private vendors:** Bitglass, Cato, CipherCloud, Darktrace, Forcepoint, iboss, Menlo Security, Netskope, Open Systems
   - **Legacy vendors:** On premise firewall and VPN solutions

2. **Identity:** Within the broad category of Identity, we think of three main sub-categories: 1) SSO/MFA, 2) Governance, and 3) PAM. Over the next five years as cloud security/SASE takes hold, adoption of Identity solutions is likely to increase as well as the potential to expand the overall Identity TAM. As such, we believe protecting identities of workers, customers, and increasingly APIs/bots will likely increase in importance.
   - **Key public vendors:** CYBR, MSFT, OKTA, PING and SAIL
   - **Key private vendors:** Auth0, BeyondTrust, Centrify, ForgeRock, OneLogin, One Identity (Quest) and Saviynt
   - **Legacy vendors:** CA/AVGO, IBM, ORCL and Micro Focus

3. **Protecting Workloads:** Historically we would have referred to this category as Endpoint Security or simply Anti-Virus but as we think in a post COVID world and as we look beyond 2025, the idea of endpoint security is limiting. As such, we believe the more important category will be protecting workloads. These workloads could certainly exist on traditional endpoint devices (laptop, etc.), but also increasingly exist in the public cloud as ephemeral workloads. As a result, we think with higher levels of WFH and a faster migration to public and hybrid compute, the broad category of workload security increases.
   - **Key public vendors:** CRWD, ESTC, MSFT, PANW, VMW/CBLK as well as AWS and GCP
   - **Key private vendors:** Cybereason, SentinelOne and Tanium
   - **Legacy vendors:** Traditional AV solutions

4. **Security Monitoring/Visibility:** We are bullish on monitoring/observability beyond 2025 and believe the sub-category of security monitoring (generally SIEM and SOAR) could be increasingly important given an evolving network/security landscape.
   - **Key public vendors:** DDOG, ESTC, MSFT, PANW, RPD and SPLK
   - **Key private vendors:** Exabeam, Forcepoint and LogRhythm
   - **Legacy vendors:** Dell, IBM and Micro Focus

5. **Other: 1) Data Security** (SAIL, VRNS); 2) **Email** (MIME, MSFT, PFPT); 3) **Vulnerability Management** (QLYS, RPD, TENB)

Source: RBC Capital Markets, company reports

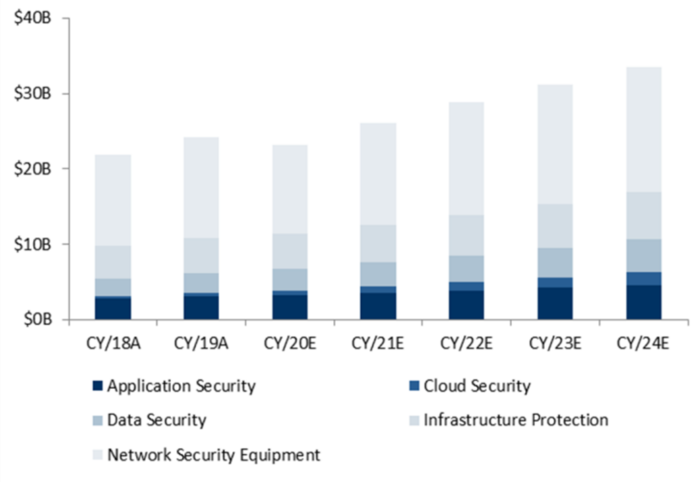
Key components of the long-term security stack: Cloud Security and Application Access/Security

Part 3

Capital Markets

Cloud Security in 2025 and beyond; the potential market opportunity

- **We believe the broad category of cloud security and application access/security could see large gains beyond 2025:** As we look beyond 2025 and in the context of SASE and ZTNA, we believe the broad category of cloud security including application access & security takes on a new level of importance and expands sub-categories of spending such as application and data security while potentially cannibalizing or superseding existing categories such as infrastructure and network security. We believe this is being driven by the “perimeter” moving further out to the “edge” and closer to the user that could accelerate in a post COVID world.
- **Expanding the market opportunity:** We looked at Gartner's estimates for various security categories and based on our own assumption and interpretation of the data, we believe the TAM could reach $35 billion by 2024, with an 8% CAGR. Within the various categories of spend, we believe the fastest growth could come from Cloud and Data Security while we believe the replacement cycle from Network and Infrastructure Security spending is high. Essentially we see cloud-based security as a TAM expansion opportunity primarily, but over time could shift security dollars away from traditional on premise/data center security spending.



- **The seismic shift:** We feel the long-term opportunity for securing the cloud is best represented by the shift in IT spending as a result of COVID. Gartner projects Data Center Systems to grow at a CAGR of 0.4% between 2018 and 2023 while Enterprise software grows at a CAGR of 9.8%. At the same time budgets are moving toward software, they are also moving toward the cloud going from 5.8% of IT budgets in 2017 to projections of 11.6% in 2023 or $194 billion to $497 billion. For context, all of software in 2019 was $482 billion, with security making up ~10% of that. As we look the future of cloud security, we feel it pushes the boundaries toward work force enablement as well as DevOps and cloud infrastructure management. Ultimately, the combination of these factors should lead to an increased focus on cloud security and application access/security.
- **The point is…** we believe in a post COVID world, while legacy firewall/VPN spending doesn’t go away, it becomes less relevant as we expect a significant increase in the TAM for cloud-based security over the next five years or more.

Source: Gartner “Forecast Analysis: IT Spending, Worldwide” by John David Lovelock and Linglan Wang on February 19, 2020, RBC Capital Markets

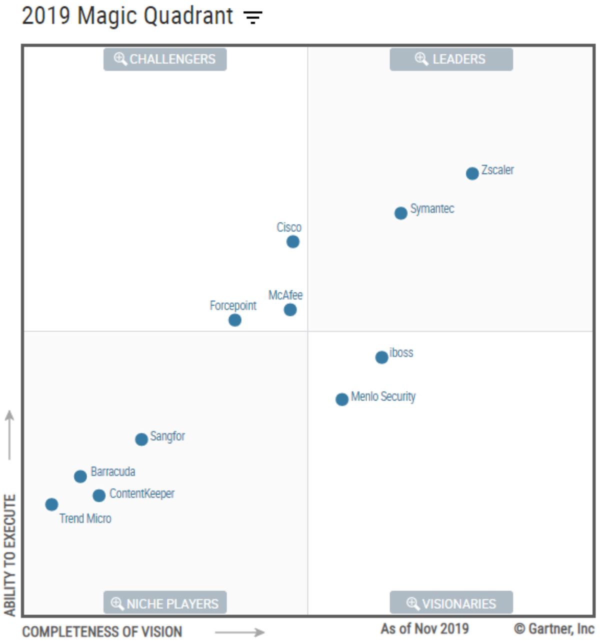
Cloud Security in 2025 and beyond; thinking through the landscape

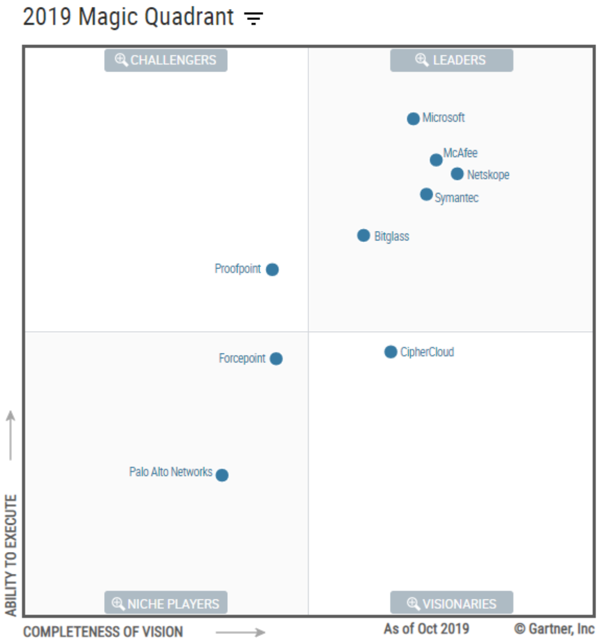
- **Relevant Magic Quadrants: Cloud security is an evolving market, but we feel the following product categories encompass relevant players building toward these new themes.**

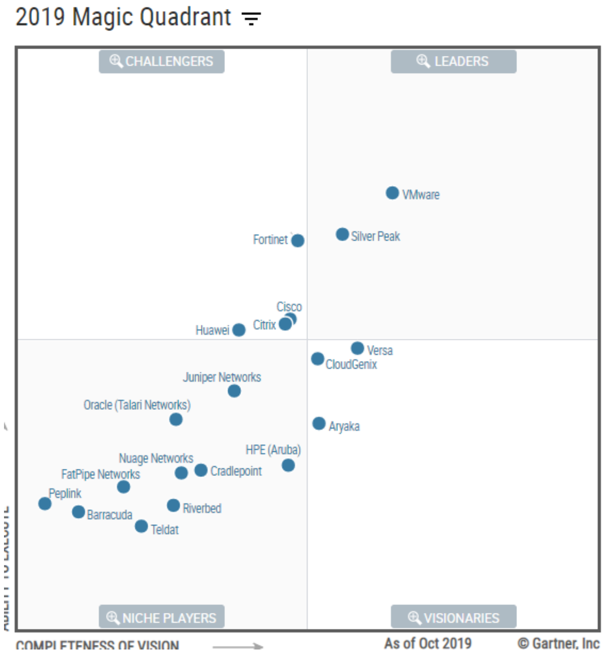
  - **Within Secure Web Gateway (first MQ below): Leaders**: Zscaler, Symantec; **Challengers**: Cisco, Forcepoint, McAfee; **Visionaries**: iboss, Menlo Security; **Niche**: Barracuda, ContentKeeper, Sangfor and Trend Micro.

  - **Within Cloud Access Security Brokers (second MQ below): Leaders:** Bitglass, McAfee, Netskope, Symantec; **Challengers:** Proofpoint; **Visionaries**: CipherCloud; **Niche**: Forcepoint, Palo Alto Networks.

  - **Within WAN (third MQ below): Leaders:** VMware, Silver Peak; **Challengers**: Fortinet, Cisco, Citrix, Huawei; **Visionaries**: Versa, PANW/CloudGenix, Aryaka; **Niche**: a whole host including Juniper, Oracle, HPE, Riverbed, Barracuda.







Source: Company reports, RBC Capital Markets, Gartner “Magic Quadrant for Secure Web Gateways” by Lawrence Orans, John Watts, Peter Firstbrook on November 11, 2019, “Magic Quadrant for Cloud Access Security Brokers” by Steve Riley and Craig Lawson on October 22, 2019 and “Magic Quadrant for WAN Edge Infrastructure” by Jonathan Forest, Mike Toussaint, Neil Rickardon on November 26, 2019

Cloud Security in 2025 and beyond; who might consolidate cloud security spend

- **Will the cloud secure the cloud?** We believe public cloud providers will likely have an important role to play in securing cloud based workloads and applications. That said, we continue to believe that at enterprise scale, hybrid and multi-cloud environments will lead to the adoption of best of breed as well as security platforms. Additionally, we believe the independence of best of breed security vendors that play a neutral role vs cloud providers is an advantage. To customers, we feel that the most important factor will be gaining a consolidated view of the health of workloads and applications against a multi-cloud backdrop. That said, if a public cloud vendor got deeper into ZTNA, for example, it could disrupt the industry.

- **Who seems best positioned to gain share?**
  - **Key public vendors: AKAM, CHKP, CSCO, FTNT, HPE, MSFT/Azure, NET, PANW, ZS as well as AWS and GCP**
    - **Zscaler**. We believe its web gateway/proxy technology should be well-positioned to gain share from an increase in edge focused spending. The company's ZIA offering helps secure public internet access while the ZPA offering helps secure access to private applications.
    - **Cloudflare**. We believe Cloudflare's visibility into internet traffic makes it a natural extension toward securing application and access. Cloudflare Teams includes Access that secures internal applications and Gateway that secures public internet traffic/apps.
    - **Palo Alto Networks.** Palo Alto may be the wildcard in the group as it likely transitions revenue away from on premise firewalls to cloud security offerings such as Prisma Access. While best of breed vendors may have an advantage, we believe Palo Alto could be better positioned relative to other firewall vendors due to aggressive investments in cloud security solutions and entrenched position as the incumbent.
  - **Select private vendors: Bitglass, Cato, CipherCloud, Darktrace, Forcepoint, iboss, Menlo Security, Netskope, Open Systems**
  - **Legacy vendors:** On premise firewall and VPN solutions

- **Who is likely to lose share?** While we think on premise firewall and VPN solutions will continue to play an important role in network security for many years, we do believe that spending could continue to shift to cloud-native solutions as more applications and workload shifts to the cloud. At this point we've seen Palo Alto shift aggressively to cloud-based security solutions such as Prisma Access and we'd expect other on premise firewall vendors to do the same and attempt to consolidate spending. Potentially aiding in this could be the importance of incumbency, which was an important factor in the early days of COVID with additional emergency VPN support. That said, we do believe CIOs see additional VPN access as a temporary fix as they move to more SASE and ZTNA architecture.

Source: RBC Capital Markets, company reports

Key components of the long-term security stack: Identity

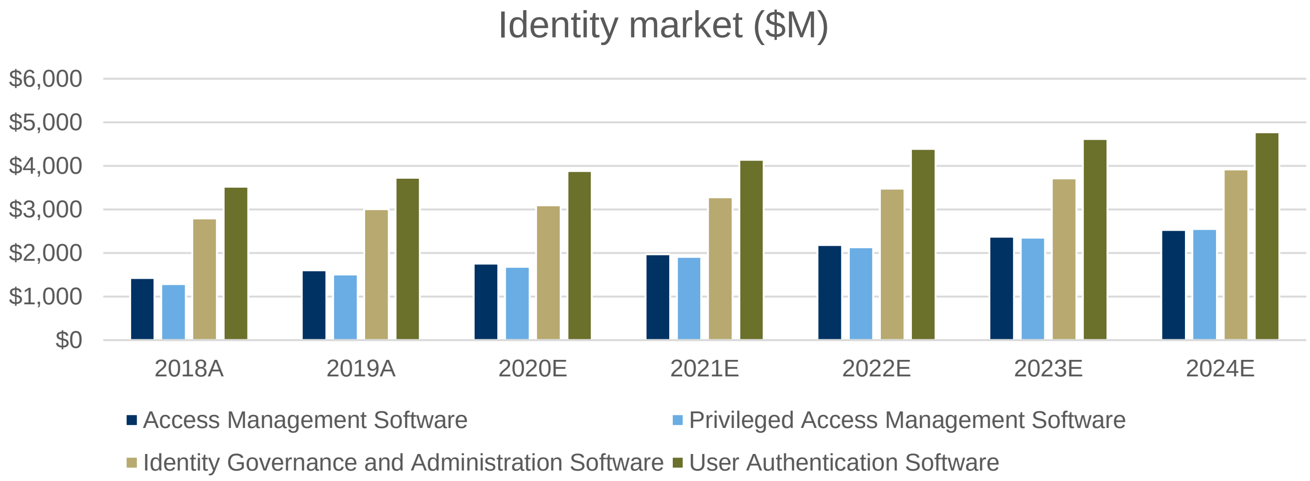
Part 4

Capital Markets

Identity in 2025 and beyond; the potential market opportunity

- **We believe the broad category of Identity could see large gains beyond 2025:** Within the broad category of Identity, we think of three main sub-categories: 1) SSO/MFA, 2) Governance, and 3) PAM. Over the next five years as cloud security/SASE takes hold, adoption of Identity solutions is likely to increase as well as the potential to expand the overall Identity TAM. As such, we believe protecting identities of workers, customers, and increasingly APIs/bots will likely increase in importance.

- **Expanding the market opportunity:** Gartner believes the identity market is $9.8 billion today and could expand to $13.8 billion by 2024.



	2018A	2019A	2020E	2021E	2022E	2023E	2024E	CAGR 2019-2024
Access Management Software	$1,426	$1,599	$1,756	$1,968	$2,180	$2,376	$2,531	9.6%
Privileged Access Management Software	$1,289	$1,505	$1,684	$1,911	$2,133	$2,354	$2,551	11.1%
Identity Governance and Administration Software	$2,792	$3,007	$3,093	$3,276	$3,478	$3,709	$3,918	5.4%
User Authentication Software	$3,520	$3,725	$3,878	$4,134	$4,387	$4,614	$4,769	5.1%

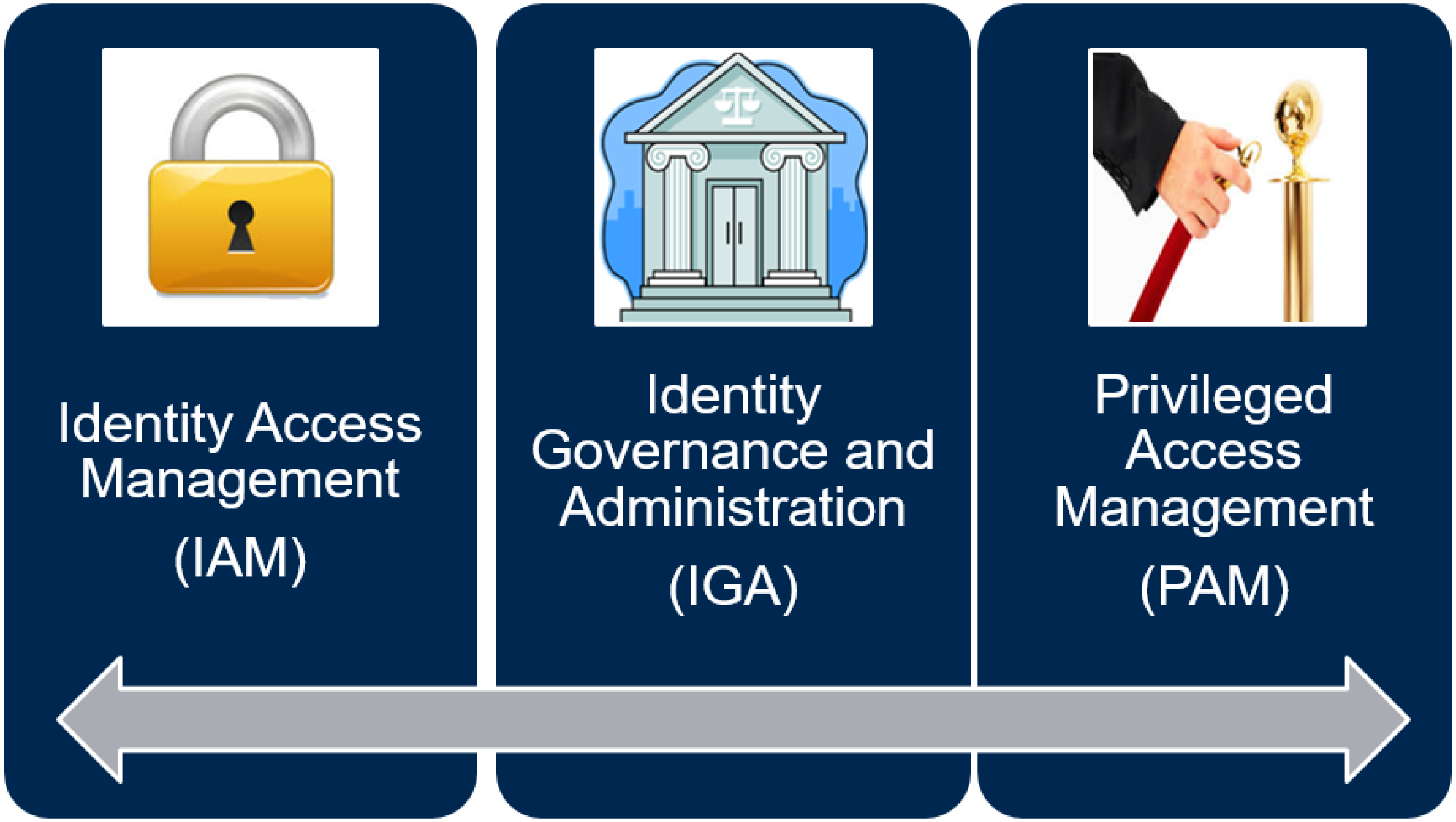
- **We believe the opportunity could be even larger:** We believe Gartner’s view of the Identity market is likely based more on a legacy on premise view and as cloud, mobile, remote/WFH trends increase, we believe the need for Identity-based solutions will increase.

- **The point is…** we believe in a post COVID world, Identity takes on a new level of importance with SASE and ZTNA architecture as we expect to see a significant increase in the TAM over the next five years.

Source: RBC Capital Markets, Gartner “Forecast: Information Security and Risk Management, Worldwide, 2018-2024, 1Q20 Update” by Rustam Malik, Mark Driver, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John A. Wheeler, Nat Smith and Christian Canales on May 20, 2020

Identity in 2025 and beyond; thinking through the landscape

- **Thinking through the landscape:**
  - **Within SSO/MFA primary vendors include** Okta, Microsoft, Ping Identity, IBM and Oracle while secondary competitors include AuthO, ForgeRock, OneLogin, Micro Focus, Broadcom/CA.
  - **Within Governance primary vendors include** SailPoint, Saviynt, IBM, Omada and One Identity while secondary vendors include Micro Focus, Oracle, Hitachi, SAP and Broadcom/CA.
  - **Within PAM primary vendors include** CyberArk, BeyondTrust, Centrify, and Broadcom/CA while secondary vendors include One Identity, Thycotic, Hitachi and Micro Focus.



Identity Access Management (IAM)

Identity Governance and Administration (IGA)

Privileged Access Management (PAM)

Source: RBC Capital Markets, company reports

Identity in 2025 and beyond; who might consolidate Identity spend

- **Will the Identity market consolidate?** We think consolidation in the SMB market is likely while at the Enterprise level, best of breed continues to win out. That said, we believe many Identity vendors will continue to expand the scope of their cloud-based Identity offerings and potentially move further into tangential markets.

- **Who seems best positioned to gain share?**
  - **Okta**. With a cloud-based model, we believe Okta is well positioned to continue share gains in its core SSO/MFA markets for both Workers and Customers, but we also believe it has the opportunity to consolidate some SBM spending within Governance and PAM over the next five years.
  - **Ping Identity.** We believe Ping remains well positioned in high-end Enterprise SSO/MFA spending and likely to gain share from legacy IAM vendors. We also like its opportunity to grow share of the emerging API security market. We do wonder over time if the company could look to other aspects of Identity.
  - **SailPoint**. We believe SailPoint remains well positioned in the Identity Governance market and would expect increasing share gains via SaaS-based offerings over the next five years. Similar to Ping, we do wonder over time if the company could look to other aspects of Identity.
  - **CyberArk** (not covered). While we don't cover CyberArk, our field work suggests it has a large advantage in PAM as it remains to be seen if the company leverages the recent acquisition of Idaptive to get into the SSO/MFA market.
  - **Microsoft** (covered by Alex Zukin). We believe Microsoft could be well positioned to gain share in SSO/MFA given the growing use of Office 365 and Active Directory.
  - **Select private vendors: Auth0, BeyondTrust, Centrify, ForgeRock, OneLogin, One Identity (Quest), Saviynt**

- **Who is likely to lose share?** We largely think legacy vendors such as IBM, Oracle, Broadcom/CA, and Micro Focus.

Source: RBC Capital Markets, company reports

Key components of the long-term security stack: Protecting Workloads

Part 5

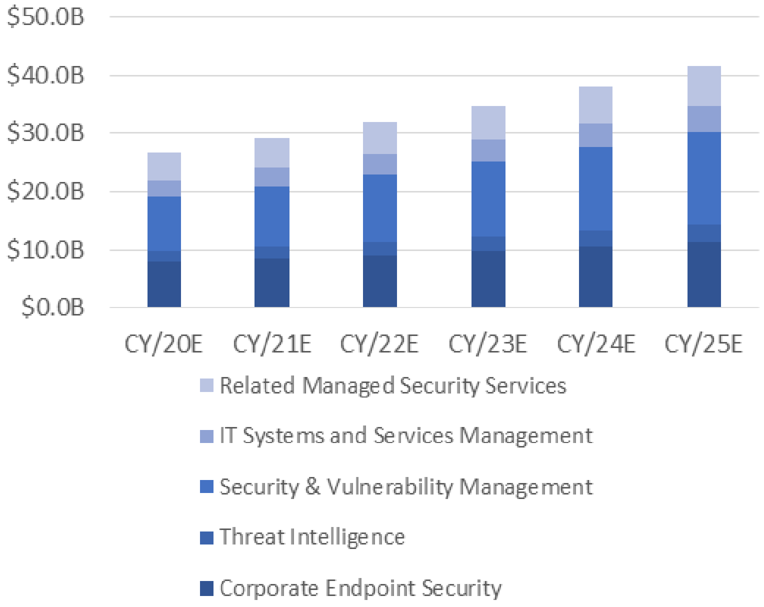
Capital Markets

Protecting Workloads in 2025 and beyond; the potential market opportunity

- **We believe the broad category of protecting workloads could see large gains beyond 2025:** Historically we would have referred to this category as Endpoint Security or simply Anti-Virus but as we think in a post COVID world and as we look beyond 2025, the idea of endpoint security is limiting. As such, we believe the more important category will be protecting workloads. These workloads could certainly exist on traditional endpoint devices (laptop, etc.), but also and increasingly exist in the public cloud as ephemeral workloads. As a result, we think with higher levels of WFH and a faster migration to public and hybrid compute, the broad category of workload security increases.

- **The endpoint market:**
  - Historically, the market has been viewed as the endpoint market, which is estimated at ~$8 billion in 2020 and could reach ~$11 billion in 2025 by our estimate.
  - Legacy vendors including Kaspersky Labs, McAfee, Sophos, Symantec and Trend Micro together have ~70% share.

- **Adjacencies to protect cloud workload provide an opportunity for significant TAM expansion:**
  - Overall we believe the TAM could be ~$41 billion in 2025.
  - This still likely underestimates the TAM as the real opportunity is to protect workloads wherever they may reside whether that be on a desktop/laptop, cloud or on premise environments, containerized applications, IoT and mobile.
  - We'd note that CRWD recently experienced a 75% q/q increase in ARR from AWS, a bullish trend around protecting workloads.
  - Potential adjacencies could include:
    - Threat intelligence estimated at ~$1.8 billion in 2020 and could reach ~$3.1 billion in 2025 by our estimate.
    - Security and Vulnerability Management estimated at ~$9.3 billion in 2020 and could reach $16.0 billion in 2025 by our estimate.
    - IT Systems and Services Management estimated at ~$2.8 billion in 2020 and could reach $4.4 billion in 2025 by our estimate.
    - Related Managed Security Services estimated at ~$4.7 billion in 2020 and could reach $6.9 billion in 2025 by our estimate.



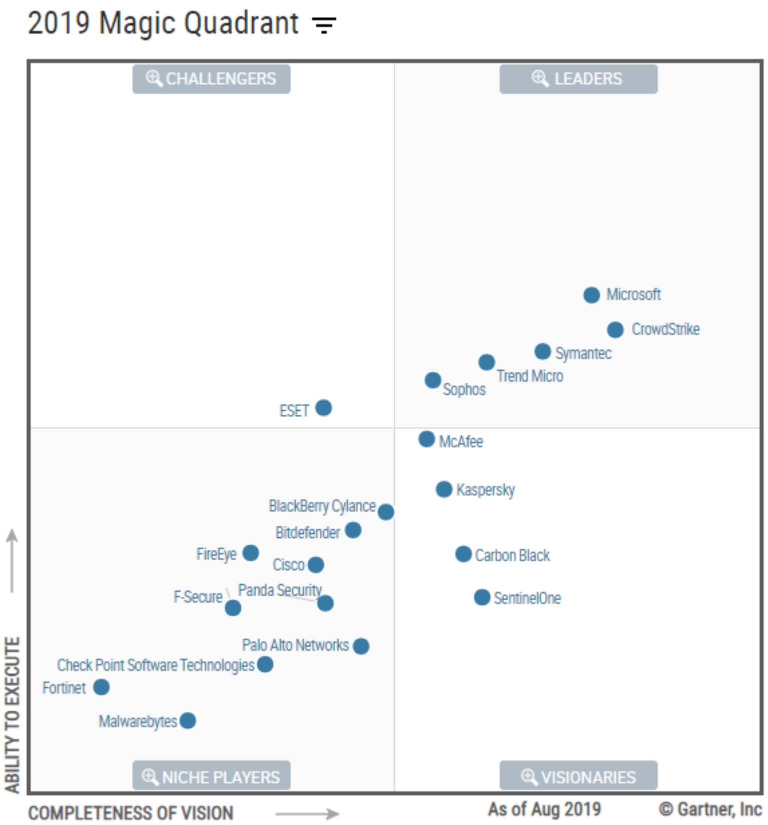
- **The point is…** we believe protecting workloads vs. just focusing on endpoints becomes the more important focus through 2025.

Source: CrowdStrike, Gartner "Prepare for Endpoint Protection Shifting to the Cloud" by Peter Firstbrook on February 28, 2019, RBC Capital Markets

Protecting Workloads in 2025 and beyond; thinking through the landscape

- **Thinking through the Endpoint landscape:** Gartner's Magic Quadrant for Endpoint Protection Platforms categorizes the landscape as follows:
  - **Leaders:** CrowdStrike, Microsoft, Sophos, Symantec, Trend Micro
  - **Visionaries:** Carbon Black, Kaspersky, McAfee, SentinelOne
  - **Challengers:** ESET
  - **Niche Players**: Bitdefender, BlackBerry Cylance, Check Point Software, Cisco, FireEye, Fortinet, F-Secure, Malwarebytes, Palo Alto Networks, Panda Security

- **But what about cloud vendors?** While vendors such as CrowdStrike have emerging opportunities to protect cloud-based workloads, we wonder over time might public cloud vendors start offering their own solutions, either build vs. buy? Even if that were to happen, we like the chances of best of breed security and security platform vendors to protect workloads.



- **Long-term drivers:**
  - An accelerated move to the cloud provides an opportunity for disruption.
  - EDR adds detection and investigation of security incidents, containment of the exploit at the endpoint and remediation guidance to traditional end point protection (EPP).
  - Gartner believes that by 2025, 70% of organizations with 5K+ seats will have EDR capabilities vs. 20% currently and cloud-delivered EDR will account for 95% of new deals vs. 20% today.
  - Automation adds AI/ML capabilities around remediation, response and threat intelligence, and SOAR (security orchestration, automation and response), and leverages existing staff.
  - Cloud scale better enables back-end compute and data analysis, collection and retention.
  - Endpoint is the new perimeter as securing the perimeter is no longer enough. Each endpoint must be secured from wherever it accesses the network.

Source: Gartner "Magic Quadrant for Endpoint Protection Platforms" by Peter Firstbrook, Dionisio Zumerle, Prateek Bhajanka, Lawrence Pingree and Paul Webber on August 20, 2019, Gartner "Prepare for Endpoint Protection Shifting to the Cloud" by Peter Firstbrook on February 28, 2019, RBC Capital Markets

Protecting Workloads in 2025 and beyond; who might consolidate spend?

- **Will the market consolidate?** We think consolidation likely benefits those better positioned for more challenging aspects of endpoint security, those able to protect all aspects around workloads and those with a modular, platform approach vs. those that fit more into the more traditional anti-virus oriented view of the endpoint market.

- **Who seems best positioned to gain share?**
  - **CrowdStrike**. Likely takes share from legacy endpoint vendors through a differentiated offering based on 1) a lightweight and smart agent, 2) a cloud-based Threat Graph database that allows for extensive ML/AI work, 3) a modular approach to the growing platform that enables a user to collect data once and use it for many purposes and 4) the CrowdStrike Store, which could further increase the halo-effect.
  - **Elastic**. Via their Endgame acquisition in 2019, the company could have an early, but differentiated approach to endpoint security, which is a natural extension of their platform.
  - **Microsoft**. The company has long been in the endpoint security market, but we think it could continue to take share by not only protecting traditional endpoints, but also Azure-based public cloud workloads.
  - **Palo Alto Networks.** The company has long been in the endpoint market via its Traps product, but we also believe the company could increasingly be looking at making a bigger play in protecting the broader category of workload security.
  - **VMware**. Carbon Black (acquired in August 2019) should benefit from tighter integration into VMware properties including NSX, vSAN and Workspace ONE as well as cross-selling into the broad Dell/VMware customer base.
  - **Select private vendors: Cybereason**, **SentinelOne** and **Tanium.**

- **Who is likely to lose share?**
  - Likely share donators include traditional AV vendors including Blackberry (Cylance), Kaspersky Labs, Sophos, Symantec and Trend Micro.
  - Legacy vendors combined have ~70% share in the legacy endpoint market.

Source: CrowdStrike company reports, Gartner “Prepare for Endpoint Protection Shifting to the Cloud” by Peter Firstbook on February 28, 2019, RBC Capital Markets

Protecting Workloads in 2025 and beyond; the desktop opportunity for security solutions

- **We believe the role of virtual desktops through increased levels of WFH gains importance and impacts security spending through 2025:** Over the next five years we believe as the “perimeter” moves further out to the “edge” and closer to the user through increased WFH levels, adoption of virtual desktops is likely to increase in importance, which should have an impact on security spending and posture.

- **Who seems best positioned to gain share in virtual desktops:**
  - **Microsoft.** Microsoft launched Windows Virtual Desktop (WVD), a solution hosted in Azure as WVD can deliver both multi-session (Windows 10) virtual desktops and if needed, dedicated VDI desktops. We think WVD could also create pull through for Microsoft’s growing security platform including Secure Remote Work, Zero Trust, IAM, Threat Protection, Information Protection and Cloud Security.
  - **VMware.** We believe the combination of Workspace ONE (digital/virtual workspace with Zero Trust capabilities) along with their emerging security portfolio of endpoint through Carbon Black, SD-WAN through VeloCloud and micro-segmentation through NSX could all position VMware for additional security gains through 2025.
  - **Citrix.** We believe Citrix’s Workspace solution application and desktop virtualization platform could continue to gain traction with elevated levels of WFH but we note Citrix doesn’t have a well defined internal security platform similar to Microsoft and VMware.

- **The biggest areas that could benefit are likely application access and identity:** We have talked to CIOs that note a combination of a virtual desktop and application access (we’ve heard a lot of references to ZS) and an IAM vendor like Okta, Ping or Microsoft will increasingly become strategic in a post COVID world.

Source: RBC Capital Markets, company reports

Key components of the long-term security stack: Security Monitoring and Visibility

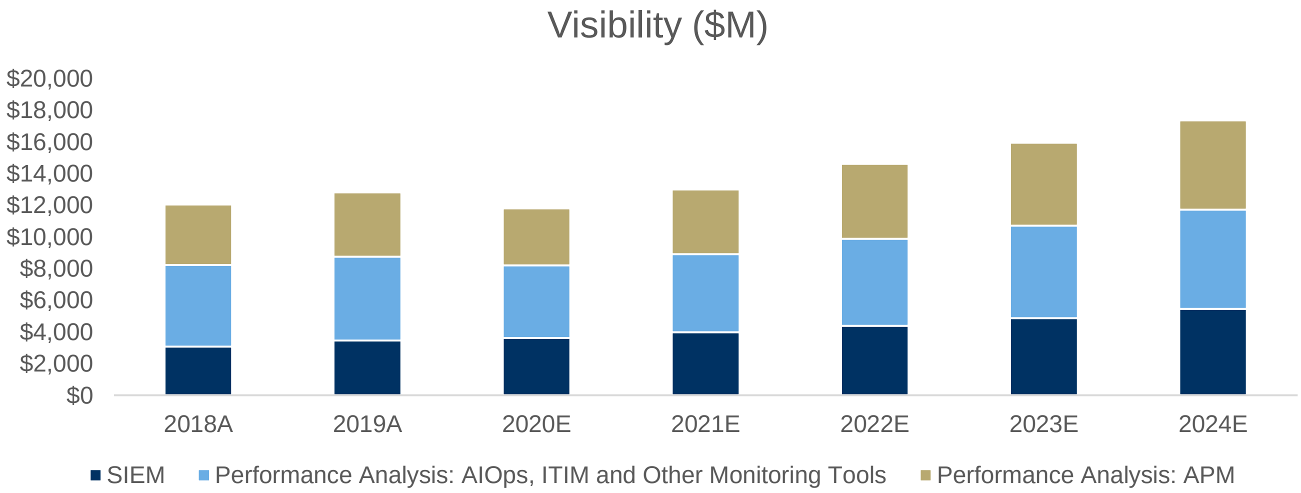
Part 6

Capital Markets

Security Monitoring/Visibility in 2025 and beyond; the potential market opportunity

- **We believe SIEM, SOAR, UEBA and monitoring converge around a common idea of visibility beyond 2025:** Essentially as networks become more complex and distributed in a post COVID world, being able to correlate data and security feeds quickly and increasingly automatically likely takes on a new level of importance. As the number of security solutions deployed by most organizations increases, being able to intelligently sift through this data is important; essentially helping organizations find the needle in the needle stack. The core of answering this question will be ML/AI technology as winners will be defined by who has the most data for their models.

- **Expanding the market opportunity for security monitoring:** Looking at estimates from Gartner, the SIEM market is expected to grow from $3.4 billion in 2019 to $5.5 billion in 2025, a CAGR of 9.5%, while monitoring for APM and ITIM is expected to grow from $9 billion to $12 billion, a CAGR of 5%. Over time we believe the security monitoring TAM could increase beyond these assumptions.



- **The conjunction of SecOps:** We feel the combination of these various markets is best defined by SecOps, or the meeting point of security and performance. Over time, the keys to this market are likely to revolve around the most comprehensive data sets feeding into ML/AI platforms helping to augment limited security, IT and developer resources.

- **The case for convergence:** The reason we view this market as likely to converge is the data. Security, IT and DevOps teams have common goals and often utilize common data sets. The idea that their tools are not communicating is not sustainable, in our opinion. While SIEM and SOAR solutions have primary goals around identifying and responding to security events, anomaly detection is a close cousin to identifying performance issues in applications. All can use UEBA to discover insider threats or performance issues used for security but also to manage user experience.

- **The point is…** we feel security monitoring and visibility takes on a new level of importance through 2025 in a post COVID world.

Source: RBC Capital Markets, Gartner “Forecast: Information Security and Risk Management, Worldwide, 2018-2024, 1Q20 Update” by Rustam Malik et. al. on May 20, 2020 and “Forecast: Enterprise Infrastructure Software, Worldwide, 2018-2024, April 2020 Update” by Vanitha Dsilva et.al on April 30, 2020

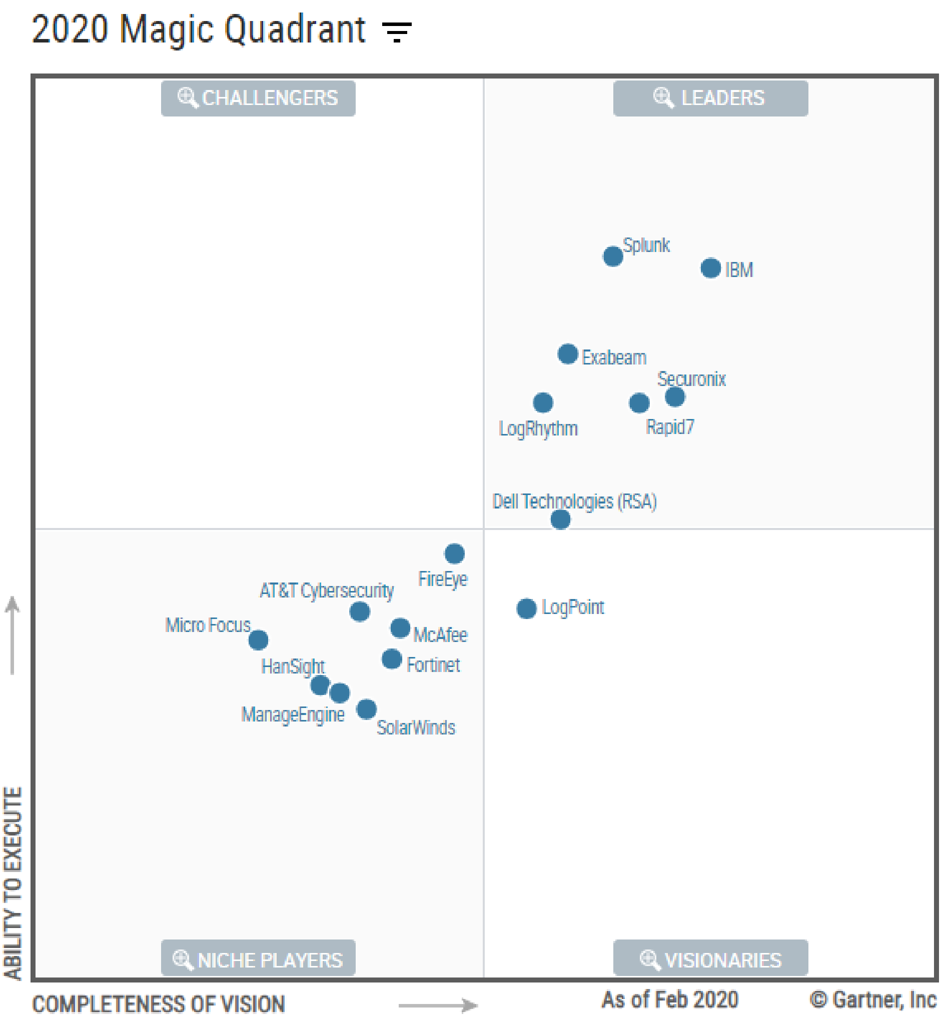
Security Monitoring/Visibility in 2025 and beyond; thinking through the landscape

- **Within the Magic Quadrant for SIEM (Security Information and Event Management); leaders per the exhibit to the right include:** Dell, Exabeam, IBM (Qradar), LogRhythm, Securonix, Splunk and Rapid7.

- **SOAR (Security Orchestration, Automation and Response):** Palo Alto Networks/Demisto, IBM, ServiceNow, Splunk and Rapid7

- **UEBA (User and Entity Behavior Analytics):** CyberArk, Exabeam, Forcepoint, HPE, LogRhythm, Microsoft, Netskope, Okta, Ping Identity, Rapid7, SailPoint, Splunk, Varonis

- **Monitoring tools:** Datadog, Dynatrace, Elastic, New Relic, Splunk



Source: Gartner "Magic Quadrant for Security Information and Event Management" by Kelly Kavanagh, Toby Bussa, Gorka Sadowski on February 18, 2020

Security Monitoring/Visibility in 2025 and beyond; who might consolidate Visibility spend

- **Will the Security Monitoring and Visibility market consolidate?** We believe the short answer is, yes. We are seeing traditional monitoring vendors such as Datadog and Elastic move into the security monitoring market while Splunk for example moved from security monitoring into APM. Additionally, Rapid7, which started as a vulnerability management vendor is moving into the broader security monitoring market. Over time we wouldn't be surprised to see additional consolidation in the market.
- **Who seems best positioned to gain share?**
  - **Splunk.** The company is a good example of convergence of ITOps and Security. With the addition of SignalFx, Splunk has a broad platform that we feel could consolidate spending in SOC products like the Splunk Mission Control and collaboration into the Next-Gen SOC.
  - **Rapid7.** The company is an early investor in automation across its cloud-based Insight platform moving beyond vulnerability management with InsightIDR for UEBA and SIEM and InsightConnect for orchestration and automation.
  - **Datadog.** Focused initially on the DevOps side of DevSecOps, we feel the recent entrance into the security monitoring market will be interesting to watch as the platform is broadened to full observability functionality.
  - **Elastic.** The company has been building its security capabilities starting with the acquisition of Endgame as well as launching SIEM capabilities in February.
  - **Public cloud vendors.** We believe public cloud vendors could continue to capture security monitoring spend, but focused on data that sits in their cloud, which is different than independent vendors that can monitor across multiple platforms. A good example of this is Microsoft Azure Sentinel, which is a cloud-native SIEM.
  - **Select private vendors: Exabeam, Forcepoint, LogRhythm**
- **Who is likely to lose share?** In core SIEM, Dell, IBM and Micro Focus seem to be losing share. That said, we believe SIEM/SOAR/UEBA could be more of a greenfield opportunity as more data, applications and workloads move to the cloud as well as increased levels of WFH post COVID.

Source: RBC Capital Markets, company reports

Key components of the long-term security stack: Other categories to consider

Part 7

Capital Markets

Other categories of security worth watching through 2025 and beyond

- **Data Security and Governance** (SAIL, VRNS)
  - When we built out our key pillars of security over the next several years we contemplated making Data Security a stand-alone category as we believe data security and governance takes on a new level of importance in a post-COVID world and with higher levels of WFH and collaboration which can expose an organization for sensitive data loss. We believe Varonis remains best positioned in the market as we see SailPoint as another candidate to benefit, but note its core market is Identity Governance.

- **Email Security** (MIME, MSFT, PFPT)
  - We believe Email Security will remain an important aspect of security spending especially when considering humans are often the weakest link in a security policy. That said, it will be important for email security vendors to continue to sell more products/upsell to their expanding base to help offset what might be more mature growth in core spam filtering. Both Proofpoint and Mimecast have a bundle strategy and could also benefit from underpenetrated international opportunities as well as share-shift from Symantec.

- **Vulnerability Management** (QLYS, RPD, TENB)
  - We believe Vulnerability Management is important from both a governance and security perspective given the proliferation in public and hybrid cloud adoption as well as elevated levels of WFH post COVID. That said, the core VM market won't likely see the same share gains and TAM expansion as other categories of security spending which is why we think it will be important for vendors like Qualys and Rapid7 to continue to add additional features beyond core VM.

Source: RBC Capital Markets, company reports

Companies mentioned

Akamai Technologies, Inc. (NASDAQ: AKAM US; $113.12; Sector Perform)
Cisco Systems, Inc. (NASDAQ: CSCO US; $45.63; Outperform)
Cloudflare, Inc. (NYSE: NET US; $36.47; Outperform)
CrowdStrike Holdings, Inc. (NASDAQ: CRWD US; $107.27; Outperform)
Okta Inc (NASDAQ: OKTA US; $207.76; Outperform)
Palo Alto Networks, Inc. (NYSE: PANW US; $230.53; Sector Perform)
Ping Identity Holding Corp. (NYSE: PING US; $32.49; Outperform)
SailPoint Technologies Holdings, Inc. (NYSE: SAIL US; $27.82; Outperform)
Splunk Inc. (NASDAQ: SPLK US; $199.91; Outperform)
VMware, Inc. (NYSE: VMW US; $149.88; Outperform)
Zscaler Inc (NASDAQ: ZS US; $110.21; Outperform)

Required disclosures

Conflicts disclosures

This product constitutes a compendium report (covers six or more subject companies). As such, RBC Capital Markets chooses to provide specific disclosures for the subject companies by reference. To access conflict of interest and other disclosures for the subject companies, clients should refer to https://www.rbccm.com/GLDisclosure/PublicWeb/DisclosureLookup.aspx?entityId=1. These disclosures are also available by sending a written request to RBC Capital Markets Research Publishing, P.O. Box 50, 200 Bay Street, Royal Bank Plaza, 29th Floor, South Tower, Toronto, Ontario M5J 2W7 or an email to rbcinsight@rbccm.com.

The analyst(s) responsible for preparing this research report received compensation that is based upon various factors, including total revenues of the member companies of RBC Capital Markets and its affiliates, a portion of which are or have been generated by investment banking activities of the member companies of RBC Capital Markets and its affiliates.

Distribution of ratings

For the purpose of ratings distributions, regulatory rules require member firms to assign ratings to one of three rating categories - Buy, Hold/Neutral, or Sell - regardless of a firm's own rating categories. Although RBC Capital Markets' ratings of Outperform (O), Sector Perform (SP), and Underperform (U) most closely correspond to Buy, Hold/Neutral and Sell, respectively, the meanings are not the same because our ratings are determined on a relative basis.

Distribution of ratings
RBC Capital Markets, Equity Research
As of 30-Jun-2020

			Investment Banking Serv./Past 12 Mos.	
Rating	**Count**	**Percent**	**Count**	**Percent**
BUY [Outperform]	**776**	**51.63**	**238**	**30.67**
HOLD [Sector Perform]	**635**	**42.25**	**130**	**20.47**
SELL [Underperform]	**92**	**6.12**	**12**	**13.04**

Conflicts policy

RBC Capital Markets Policy for Managing Conflicts of Interest in Relation to Investment Research is available from us on request. To access our current policy, clients should refer to
https://www.rbccm.com/global/file-414164.pdf
or send a request to RBC Capital Markets Research Publishing, P.O. Box 50, 200 Bay Street, Royal Bank Plaza, 29th Floor, South Tower, Toronto, Ontario M5J 2W7. We reserve the right to amend or supplement this policy at any time.

Dissemination of research and short-term trade ideas

RBC Capital Markets endeavors to make all reasonable efforts to provide research simultaneously to all eligible clients, having regard to local time zones in overseas jurisdictions. RBC Capital Markets' equity research is posted to our proprietary website to ensure eligible clients receive coverage initiations and changes in ratings, targets and opinions in a timely manner. Additional distribution may be done by the sales personnel via email, fax, or other electronic means, or regular mail. Clients may also receive our research via third party vendors. RBC Capital Markets also provides eligible clients with access to SPARC on the Firms proprietary INSIGHT website, via email and via third-party vendors. SPARC contains market color and commentary regarding subject companies on which the Firm currently provides equity research coverage. Research Analysts may, from time to time, include short-term trade ideas in research reports and / or in SPARC. A short-term trade idea offers a short-term view on how a security may trade, based on market and trading events, and the resulting trading opportunity that may be available. A short-term trade idea may differ from the price targets and recommendations in our published research reports reflecting the research analyst's views of the longer-term (one year) prospects of the subject company, as a result of the differing time horizons, methodologies and/or other factors. Thus, it is possible that a subject company's common equity that is considered a long-term 'Sector Perform' or even an 'Underperform' might present a short-term buying opportunity as a result of temporary selling pressure in the market; conversely, a subject company's common equity rated a long-term 'Outperform' could be considered susceptible to a short-term downward price correction. Short-term trade ideas are not ratings, nor are they part of any ratings system, and the firm generally does not intend, nor undertakes any obligation, to maintain or update short-term trade ideas. Short-term trade ideas may not be suitable for all investors and have not been tailored to individual investor circumstances and objectives, and investors should make their own independent decisions regarding any securities or strategies discussed herein. Please contact your investment advisor or institutional salesperson for more information regarding RBC Capital Markets' research.

For a list of all recommendations on the company that were disseminated during the prior 12-month period, please click on the following link: https://rbcnew.bluematrix.com/sellside/MAR.action

The 12 month history of SPARCs can be viewed at https://www.rbcinsightresearch.com.

Analyst certification

All of the views expressed in this report accurately reflect the personal views of the responsible analyst(s) about any and all of the subject securities or issuers. No part of the compensation of the responsible analyst(s) named herein is, or will be, directly or indirectly, related to the specific recommendations or views expressed by the responsible analyst(s) in this report.

Third-party-disclaimers

The Global Industry Classification Standard ("GICS") was developed by and is the exclusive property and a service mark of MSCI Inc. ("MSCI") and Standard & Poor's Financial Services LLC ("S&P") and is licensed for use by RBC. Neither MSCI, S&P, nor any other party involved in making or compiling the GICS or any GICS classifications makes any express or implied warranties or representations with respect to such standard or classification (or the results to be obtained by the use thereof), and all such parties hereby expressly disclaim all warranties of originality, accuracy, completeness, merchantability and fitness for a particular purpose with respect to any of such standard or classification. Without limiting any of the foregoing, in no event shall MSCI, S&P, any of their affiliates or any third party involved in making or compiling the GICS or any GICS classifications have any liability for any direct, indirect, special, punitive, consequential or any other damages (including lost profits) even if notified of the possibility of such damages.

RBC Capital Markets disclaims all warranties of originality, accuracy, completeness, merchantability or fitness for a particular purpose with respect to any statements made to the media or via social media that are in turn quoted in this report, or otherwise reproduced graphically for informational purposes.

References herein to "LIBOR", "LIBO Rate", "L" or other LIBOR abbreviations means the London interbank offered rate as administered by ICE Benchmark Administration (or any other person that takes over the administration of such rate).

Disclaimer

RBC Capital Markets is the business name used by certain branches and subsidiaries of the Royal Bank of Canada, including RBC Dominion Securities Inc., RBC Capital Markets, LLC, RBC Europe Limited, Royal Bank of Canada, Hong Kong Branch and Royal Bank of Canada, Sydney Branch. The information contained in this report has been compiled by RBC Capital Markets from sources believed to be reliable, but no representation or warranty, express or implied, is made by Royal Bank of Canada, RBC Capital Markets, its affiliates or any other person as to its accuracy, completeness or correctness. All opinions and estimates contained in this report constitute RBC Capital Markets' judgement as of the date of this report, are subject to change without notice and are provided in good faith but without legal responsibility. Nothing in this report constitutes legal, accounting or tax advice or individually tailored investment advice. This material is prepared for general circulation to clients and has been prepared without regard to the individual financial circumstances and objectives of persons who receive it. The investments or services contained in this report may not be suitable for you and it is recommended that you consult an independent investment advisor if you are in doubt about the suitability of such investments or services. This report is not an offer to sell or a solicitation of an offer to buy any securities. Past performance is not a guide to future performance, future returns are not guaranteed, and a loss of original capital may occur. RBC Capital Markets research analyst compensation is based in part on the overall profitability of RBC Capital Markets, which includes profits attributable to investment banking revenues. Every province in Canada, state in the U.S., and most countries throughout the world have their own laws regulating the types of securities and other investment products which may be offered to their residents, as well as the process for doing so. As a result, the securities discussed in this report may not be eligible for sale in some jurisdictions. RBC Capital Markets may be restricted from publishing research reports, from time to time, due to regulatory restrictions and/ or internal compliance policies. If this is the case, the latest published research reports available to clients may not reflect recent material changes in the applicable industry and/or applicable subject companies. RBC Capital Markets research reports are current only as of the date set forth on the research reports. This report is not, and under no circumstances should be construed as, a solicitation to act as securities broker or dealer in any jurisdiction by any person or company that is not legally permitted to carry on the business of a securities broker or dealer in that jurisdiction. To the full extent permitted by law neither RBC Capital Markets nor any of its affiliates, nor any other person, accepts any liability whatsoever for any direct, indirect or consequential loss arising from, or in connection with, any use of this report or the information contained herein. No matter contained in this document may be reproduced or copied by any means without the prior written consent of RBC Capital Markets in each instance.

Additional information is available on request.

To U.S. Residents:

This publication has been approved by RBC Capital Markets, LLC (member FINRA, NYSE, SIPC), which is a U.S. registered broker-dealer and which accepts responsibility for this report and its dissemination in the United States. Any U.S. recipient of this report that is not a registered broker-dealer or a bank acting in a broker or dealer capacity and that wishes further information regarding, or to effect any transaction in, any of the securities discussed in this report, should contact and place orders with RBC Capital Markets, LLC.

To Canadian Residents:

This publication has been approved by RBC Dominion Securities Inc.(member IIROC). Any Canadian recipient of this report that is not a Designated Institution in Ontario, an Accredited Investor in British Columbia or Alberta or a Sophisticated Purchaser in Quebec (or similar permitted purchaser in any other province) and that wishes further information regarding, or to effect any transaction in, any of the securities discussed in this report should contact and place orders with RBC Dominion Securities Inc., which, without in any way limiting the foregoing, accepts responsibility for this report and its dissemination in Canada.

To U.K. Residents:

This publication has been approved by RBC Europe Limited ('RBCEL') which is authorized by the Prudential Regulation Authority and regulated by the Financial Conduct Authority ('FCA') and the Prudential Regulation Authority, in connection with its distribution in the United Kingdom. This material is not for general distribution in the United Kingdom to retail clients, as defined under the rules of the FCA. RBCEL accepts responsibility for this report and its dissemination in the United Kingdom.

To German Residents:

This material is distributed in Germany by RBC Europe Limited, Frankfurt Branch which is regulated by the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

To Persons Receiving This Advice in Australia:

This material has been distributed in Australia by Royal Bank of Canada, Sydney Branch (ABN 86 076 940 880, AFSL No. 246521). This material has been prepared for general circulation and does not take into account the objectives, financial situation or needs of any recipient. Accordingly, any recipient should, before acting on this material, consider the appropriateness of this material having regard to their objectives, financial situation and needs. If this material relates to the acquisition or possible acquisition of a particular financial product, a recipient in Australia should obtain any relevant disclosure document prepared in respect of that product and consider that document before making any decision about whether to acquire the product. This research report is not for retail investors as defined in section 761G of the Corporations Act.

To Hong Kong Residents:

This publication is distributed in Hong Kong by Royal Bank of Canada, Hong Kong Branch, which is regulated by the Hong Kong Monetary Authority and the Securities and Futures Commission (SFC) in Hong Kong, RBC Investment Services (Asia) Limited and RBC Global Asset Management (Asia) Limited, both entities are regulated by the SFC. This material is not for general distribution in Hong Kong to persons who are not professional investors (as defined in the Securities and Futures Ordinance of Hong Kong (Cap. 571) and any rules made thereunder.

To Singapore Residents:

This publication is distributed in Singapore by the Royal Bank of Canada, Singapore Branch, a registered entity licensed by the Monetary Authority of Singapore. This material has been prepared for general circulation and does not take into account the objectives, financial situation, or needs of any recipient. You are advised to seek independent advice from a financial adviser before purchasing any product. If you do not obtain independent advice, you should consider whether the product is suitable for you. Past performance is not indicative of future performance. If you have any questions related to this publication, please contact the Royal Bank of Canada, Singapore Branch. Royal Bank of Canada, Singapore Branch accepts responsibility for this report and its dissemination in Singapore.

To Japanese Residents:

Unless otherwise exempted by Japanese law, this publication is distributed in Japan by or through RBC Capital Markets (Japan) Ltd. which is a Financial Instruments Firm registered with the Kanto Local Financial Bureau (Registered number 203) and a member of the Japan Securities Dealers Association (JSDA) and the Financial Futures Association of Japan (FFAJ).