GBH INSIGHTS

Technology Research
Industry Update
February 23, 2018

Cyber Security Spending Looks Strong for 2018; Threat Landscape Remains Front and Center

Daniel Ives, Head of Technology Research | 917.210.3220 | daniel.ives@gbhinsights.com

---

Based on our recent survey work to better gauge cyber security spending over the next 12 to 18 months, we forecast spending to increase 19% year over year in 2018 vs. 16% growth in cyber security spending in 2017, a very positive data point for the sector in our opinion. We have seen hundreds of examples of major cyber attacks (the vast majority go unreported) over the past few years with the recent Intel Meltdown/Spectre and Equifax credit hacking breach being the most recent examples that has gotten the attention of consumers, CIOs, board rooms, and other key IT decision makers. Cyber threats to enterprises and government networks/infrastructure remains a major pain point in today's landscape, especially as more organizations move proprietary data to the cloud with an ever growing mobile workforce. In addition, advanced persistent threats (APT) attacks on critical infrastructure such as power grids, nuclear facilities, and water supply are translating into significant increases in cyber security budgets both in the US and around the world to defend against these sophisticated cyber terrorist threats. Overall spending on cyber security should top $90 billion in 2018 according to our forecasts comprising overall software and services around protecting enterprises and governments worldwide from cyber attacks. Based on our analysis and survey work, we believe the top areas of security spending over the next year will be around cloud security, next generation firewall technology, email security, cyber asset and threat vulnerability, and identity access management (IAM). Today we estimate surprisingly less than 5% of total capex for enterprises worldwide is focused on security despite the rampant fears facing organizations as spending has significantly lagged the "talk of many CIOs" over the past few years. **Our favorite cyber security stocks for 2018 continue to be: Check Point, Palo Alto Networks, Fortinet, Qualys, Proofpoint, and FireEye**. In addition, overdue M&A could be another positive catalyst for the sector over the coming year with larger tech players looking to add cyber security capabilities to their converging technology product arsenal in our opinion.

- **Secular trends are forcing CIOs to spend more on security.** With a more mobile workforce, public/hybrid clouds, growing iOT ecosystem, and threatening global landscape, we are picking up an increased urgency to spend on proactive, advanced solutions to protect networks, IP/data,

endpoints over the coming years. With high threat levels and European privacy legislation (GPDR) in place, we believe the current cyber landscape will remain highly elevated with more sophisticated attacks, pervasive endpoints, and shift to cloud exposing more enterprises to potential cyber attacks over the coming years. As such, the cyber security industry is at a major inflection point with the next stage of spending underway that should benefit well positioned public and private cyber players with the right product portfolios, distribution, and value proposition in the field. To this point, one of the most pervasive threats facing enterprises and governments worldwide over the past decade is protecting the network and datacenter from cyber attacks and cyber crime. We estimate that cyber crime will cost enterprises over $2 trillion dollars by 2020, speaking to the critical need facing CIOs in today's evolving landscape. With trends such as IoT and BYOD, enterprises are facing increased endpoints, hybrid cloud architecture, and forms of data to protect in a threat environment that is growing by the day. Networks, endpoints, and applications are exposed to malicious attacks, ransomware, advanced persistent threats (APTs) and sophisticated cybercriminals looking to attack vulnerable networks and endpoints on a daily basis.

- **The massive cloud wave is a positive for cyber security players.** The shift towards the cloud has been a major trend for enterprises worldwide over the last few years. Public, private, and hybrid clouds have been secular trends driving CIOs and organizations as a more mobile workforce, ubiquitous data, lower costs, and changing IT architecture are defining a new landscape. That said, today the vast majority of data still resides on-premise as many enterprises and governments have been hesitant to trust a third-party provider with proprietary data, critical workloads, and sensitive IP. We have spoken to many CIOs and other IT decision makers that pointed to security, privacy issues, lack of one control points, compliance, and other corporate controls for reasons hindering broader cloud deployments and moving critical workloads to a public/hybrid cloud

Daniel H. Ives
917.210.3220
daniel.ives@gbhinsights.com

environment over the past year. That said, with Amazon (AWS) and especially Microsoft (Azure) having unprecedented customer success on their enterprise cloud initiatives, we believe the next potential beneficiary could be cloud cyber security players. We believe it is still early days in the move to cloud architectures across the enterprise world, with more CIOs and IT decision makers looking at this massive secular shift over the next 3 to 5 years. As such, with more sensitive data and critical information needing to be protected in these cloud deployments, we believe security vendors stand to benefit during the course of 2018 as more spending shifts towards broader cloud deployments. To this point, in our opinion there is a "land grab opportunity" over the next 12 to 18 months in cloud security for those security vendors that have the solution sets to protect critical cloud deployments and seamlessly work with on-premise and public/hybrid workloads through a unified and deep solution set.

Daniel H. Ives
917.210.3220
daniel.ives@gbhinsights.com