ClearBridge Investments

Cloud Breach Shows Security Software Still Critical

August 19, 2019

Key Takeaways

- Recent data breaches demonstrate the security benefits of the cloud are not fail-safe and that general fears about threats to third-party information security providers from the cloud are premature.
- As cloud workloads grow in number, tiers of importance and complexity, the security problem tends to grow beyond what hyperscale cloud providers can currently provide on their own.
- Against this backdrop of accelerating cloud adoption and recent market weakness in IT and software, information security stocks represent a compelling opportunity and one that could lead to consolidation.

Public Cloud Sees Challenges in Balancing Flexibility with Security

Recent data breaches highlight that the public cloud is not a panacea for security and could serve to slow the pace of enterprise and government willingness to jettison third-party information security solutions. Given relatively constrained valuations and skeptical investor sentiment, we believe this creates an intermediate-term opportunity in information security stocks.

Following a long period where corporations and governments feared (and even shunned) the public cloud due to security concerns, they have since started a full embrace of the cloud, first and foremost for the flexibility and agility it provides, but also on the idea that the public cloud can in fact be the most secure option.

While the processes an enterprise follows to set up a cloud workload tend to be inherently more secure than the mishmash of techniques and mechanisms employed within private data centers, like most things, cloud security is only as good as its weakest link. The "shell" of the public cloud is generally highly secure, but no cloud provider can be responsible for ensuring proper configuration of a plethora of data sets. Not only is this impractical, but it becomes a trade-off between the flexibility that makes public cloud infrastructure and platform services (IaaS and PaaS) so popular, and the enterprise-grade security that most corporations and governments seek for their more important workloads.

In the case of the Capital One data breach, the credit card issuer's IT team were considered relatively sophisticated cloud users and forerunners within financial services in moving customer data entirely to the public cloud. Other large banks have chosen a hybrid cloud strategy, with important customer data residing in private cloud servers. These banks use the public cloud for occasional tasks that require a lot of computing power but don't involve important customer information. As workloads grow in number, tiers of importance and complexity, the public cloud security problem also tends to grow.

The Capital One breach, while perpetrated by a former Amazon Web Services employee, exploited an at least somewhat known vulnerability involving misconfiguration of a simple web application firewall which a number of

hackers could have theoretically exploited. And therein lies the hallmark of most major, high profile attacks: it's not for a lack of alerts (in the case of Target), expertise or knowledge of the potential pitfalls that these continue to occur. Like security breaches from within and outside of an organization's four walls, the issues come down to the leg work of ensuring that all "i"s are dotted and all "T"s are crossed within increasingly complex and potentially ephemeral systems (in the case of container-based architectures).

Moreover, many organizations use public cloud storage as a place to park legacy data or data of less certain value, even customer data. The latest breach highlights the potential danger of leaving certain types of data within cloud storage unattended by a third-party security system, and often one which is consistent with the on-premise infrastructure they continue to run.

Adding in a layer of third-party security won't necessarily solve the problem, but it is a mechanism that companies may continue to rely on further out into the future to consolidate the system of notifications and alerts to which they have to respond in the event of a potential security compromise. By doing so, key actors within an organization's IT team may in fact be less likely to be fired (or under the fire of the Board of Directors or the board of public opinion) if and when a security compromise occurs. And they are theoretically more likely to avert such a compromise with a more consistent approach.

The recent data coming from traditional network security vendors (and the associated channel) has been relatively positive in recent months. Many, including Fortinet and Check Point Software, highlighted cloud security as a place of relative strength. Not all vendors will benefit, but against the growing drumbeat of investor belief that the public cloud will make security software obsolete in the very near future, our view is that this could and should take longer than expected.

The current spate of cyber attacks involve longer and more involved remediation engagements, unlike the preponderance of phishing attacks of the last 18 months, highlighting the ongoing need for third-party information security protection. Management of a leading security vendor serving hybrid cloud customers just this month called the current environment among the more robust they've seen for security remediation and security product uptake generally.

Amidst the backdrop of the current market selloff, tariffs and near-term headwinds related to business model transitions by some larger providers, information security companies continue to trade at some of the most attractive valuations relative to their history and other parts of the software space. In addition, we believe consolidation by a handful of major security providers will ensue in the intermediate term as it affords the best hope for control on the part of customers.

About the Author

Hilary Frisch, CFA
Director, Senior Research Analyst for Information Technology

- 25 years of investment industry experience
- Joined ClearBridge Investments in 2013
- Member of the CFA Institute
- BA in Economics/International Studies from University of North Carolina, Chapel Hill