Technology Brief...

March 1, 2022

J.Gold Associates LLC, 6 Valentine Road, Northborough, MA 01532, USA
www.jgoldassociates.com +1-508-393-5294
Research, Analysis, Strategy, Insight

Inside This Issue

"….Most organizations, especially those moving to a multi-cloud environment, face major challenges in ensuring all data and apps remain secure and meet increasing complex compliance requirements. But many enterprises have a plethora of disparate tools used by DevOps and SecOps ... The only efficient way to truly achieve a secure and private capability is to use an integrated "single pane of glass" approach that doesn't require excessive resources needed to manage and interpret a large number of standalone tools...."

Lacework Secures the Multicloud

With the rapid deployment of cloud technologies, both public and private, and enhanced enterprise apps built for the modern cloud-deployed environment (e.g., containers), it's become increasingly difficult and complex for organizations to ensure their corporate data assets remain secure. With the majority of enterprises moving to a multi-cloud environment over the next 1-2 years that includes public and private implementations, it's even more imperative they deploy a security infrastructure that is both cloud agnostic and enables uniform functionality across all clouds. This is something not readily available from the cloud providers (e.g., Microsoft, AWS, GCP), as they primarily concentrate their offerings within their own sphere of capabilities. And while some proprietary functions are available from the cloud providers, it leaves internal data center systems to find alternative and separately implemented/managed products.

To tackle this challenge, Lacework has created the Polygraph Data Platform to provide automated risk assessment in a multi-cloud environment. The goal is to move from a rules-based to a behavior-based approach that is cloud agnostic and uses data as an active part of the solution rather than specific cloud functions. The platform provides the ability to monitor workload and cloud activity from apps, networks, process and data access, and uses a Machine Learning (ML) capability to detect anomalous operations. The platform provides a unified "pane of glass" that can surface known and zero-day threat vectors, providing a consolidated alerting function that is typically provided in most organizations by a hodge-podge of different products. Lacework collects data and monitors accounts and workloads using both an agentless and agent based approach. It uses a unique application of agentless technology to collect activity logs and monitor cloud resources across the three largest hyperscaler clouds (AWS, Google Cloud and Microsoft Azure) for continuous configuration monitoring and compliance checks. Lacework also employs an agent technology to continuously collect data for cloud workload monitoring, intrusion detection and file integrity. This combination enables a more holistic approach to protection from build time to run time.

Both DevOps and SecOps require security tools optimized for their respective roles. DevOps needs to ensure monitoring and traceability of their code while engaging in vulnerability management and testing. SecOps must minimize the false positives and reduce time to discovery and remediation to maximize compliance and minimize the overall resources requirements that in most companies are in short supply.

Lacework offers functionality for DevOps teams to identify code and misconfigurations at the developer level before the code gets deployed. It includes infrastructure as code (IaC) security scans, and an inline scanner to identify

vulnerabilities at build time so they can be updated before they get deployed. It further provides a Kubernetes admission control to ensure each container meets security standards. And it provides a runtime vulnerability scoring mechanism plus correlation with exploits.

SecOps requirements are also supported. With many organizations having dozens or even hundreds of unique security products installed, it's incredibly difficult to extend uniform coverage across all workload instances on many different processing implementations. An ML-powered capability brings a unified analysis and identification of security threats that could easily get lost when using multiple stand alone tools.

By deploying a single uniform system that can consolidate all security operations, we estimate that organizations can increase security while also reducing resources by 25%-50% or more. Studies have shown it can take weeks or months to discover security infiltrations and/or data integrity breaches. Just removing false and/or repetitive alerts that need to be examined manually can not only speed remediation of any threats, but also significantly increase the orgainzation's security stance of the organization. Further, with many new regulatory requirements being imposed, some of which, like GDPR, can result in very substantial fines for noncompliance, enterprises must do all they can to reduce and/or eliminate security breaches.

Bottom Line: Most organizations, especially those moving to a multi-cloud environment, face major challenges in ensuring all data and apps remain secure and meet increasing complex compliance requirements. But many enterprises have a plethora of disparate tools used by DevOps and SecOps to try and create such an environment. The only efficient way to truly achieve a secure and private capability is to use an integrated "single pane of glass" approach that doesn't require excessive resources needed to manage and interpret a large number of standalone tools. Products like Lacework that incorporate a combined approach delivered from a single platform are something that all enterprises should be investigating in and moving to over the next 1-2 years.

There's Advantage to Nvidia and Arm Going their Separate Ways

"…We don't believe there was any real damage done to either company… We expect Nvidia will to continue on its growth path, and Arm will continue to license its IP to many companies that make a very large number of chips. But Arm does need to be looking over its shoulder at RISC-V as a potential competitor, although probably not in the short term (the next 3-4 years)…."

Nvidia's proposed acquisition of Arm is done. There were just too many obstacles for Nvidia to overcome to make this deal palatable to many agencies and countries. They tried hard to get the deal done but in the end there were just too many issues that couldn't be solved. Facing strong headwinds, the companies finally decided to move on. Is this good or bad for the companies? We believe it's a good move for both and a strong positive for Arm licensees.

This is a win for the Arm ecosystems of licensees.
Most of the major competitors to Nvidia and/or licensees of Arm IP (e.g., Qualcomm, Nvidia, Microsoft, Apple, Intel, etc.) were opposed to the merger, fearing that Nvidia could influence Arm technology to its advantage and to the detriment of licensees, or it could garner sensitive information about how the Nvidia's competitors were using the Arm IP. Even though Nvidia stated it would not do so and leave Arm as an independent operation, there was still a risk, even if it was through just subtle influence. So the Arm licensees, especially the major players like Apple, Qualcomm and even Intel, are all breathing a sigh of relief. And business expansion for Arm IP licensing will continue as a result.

We don't believe the abandonment of the acquisition is a negative for either company. Nvidia can still pursue the licensing of its IP, as it said it wanted to do

with ownership of the Arm IP licensing channel. It will just have to do it differently. Arm will still carry on with its massive market share in mobile and continue expanding to other areas like automotive and IoT. And Softbank can now do an IPO for Arm to recoup its investment. Although it's a more difficult transaction than an acquisition, Softbank should still be able to do well from the revenue generated and may actually do better financially than what would have been provided by the acquisition. It is possible that some other large company – not a direct chip competitor – could come along and try to acquire Arm, but after this extended battle, we don't expect many companies would be interested in re-trying an Arm acquisition. There has been some talk of potentially forming a consortium of other large companies to acquire Arm, but we believe this scenario is highly unlikely.

We expect this breakup to be good for Arm overall.
Had Nvidia acquired Arm, it would have pushed more of the Arm licensees to explore alternatives, pushing them aggressively into investments in RISC-V in particular. Although RISC-V is currently nowhere near as rich and compelling an IP environment as Arm, competitive pressures and worry about Nvidia gaining insights into business and tech use by the IP licensees would have pushed them in that direction. That would have been a boost for RISC-V's competitive market position which may not now happen, or at least not as quickly. As a result, Arm will retain more market share and RISC-V will remain behind it in capabilities, even though more companies are exploring the use of RISC-V as a hedge against sole supplier technology, including Intel who announced recently that it is making plans to produce RISC-V in its fabs.

Does this failed acquisition hurt Nvidia's reputation?
Nvidia's reputation is built on its products and market presence and right now Nvidia is firing on all cylinders. We don't think it really limits their desire or ability to license their technology – a primary stated purpose of the Arm deal. There are many other ways to do so, even potentially including doing a side deal with Arm to incorporate some of the Nvidia technology in Arm IP. We don't think this is the last acquisition that Nvidia will be making. They certainly have the resources to make more strategic deals and it's highly likely we'll see others come along. However they probably won't be of the magnitude of trying to acquire Arm.

Bottom line: We don't believe there was any real damage done to either company. Nvidia did spend a lot of time and money on trying to make this happen, and there is a penalty payment to Arm after the deal collapsed. We expect Nvidia will to continue on its growth path, and Arm will continue to license its IP to many companies that make a very large number of chips. But Arm does need to be looking over its shoulder at RISC-V as a potential competitor, although probably not in the short term (the next 3-4 years).

"….While Microsoft should be commended for trying to rationalize the needs for security across many different devices and vendors, Pluton should be seen as a feature improvement and not a major security enhancement. Any security improvement is a good thing, but this really is more of a uniformity extension than a true security upgrade….."

AMD's Embrace of Microsoft's Pluton: Real Security Advance or Just Marketing?

Recently, AMD announced that Ryzen™ 6000 series processors are the first x86 processors implementing the Microsoft Pluton Security Processor. Pluton technology is integrated directly into the PC's processor and embeds the hardware root-of trust on the same silicon substrate as the CPU. Further, Microsoft uses Pluton to offer a cloud-to-device upgrade capability for security firmware – something not currently available via Windows Update. Microsoft has garnered support from virtually every major chip vendor for Pluton (e.g., AMD, Intel, Qualcomm).

While security processors have been around for many years (e.g., TPM), they have generally been incorporated as standalone peripheral chips. Pluton being embedded on the processor chip eliminates a common weakness when the root-of-trust is located on another

discrete chip that operates over the internal bus and is therefore potentially subject to attack. Pluton supports the TPM 2.0 industry standard making it backwards compatible, so many of the current Windows security capabilities using TPM can immediately be used (e.g., BitLocker, Windows Hello, System Guard), as well as many third party products.

Tech with a Marketing Angle
Pluton is not really a major advance in processor security. Pluton is primarily just TPM built on the same silicon rather than employing a standalone chip. That helps with security as there is no exposed bus that can be compromised. And the ability to update via Windows Update and the cloud is a nice feature. But TPM capabilities have been around for some time, and often not fully implemented due to complexity, although that has improved over the past 2-3 years.

Pluton was an outgrowth of Microsoft's need for a security component on its custom chips powering its gaming consoles. So while it was important for Microsoft to add this capability to its gaming console, it's less clear how much of an improvement this really is in the PC space. All the major chip companies have the equivalent of Pluton already built into their processors (Intel, AMD, Qualcomm). Indeed, most chips are already well beyond Pluton in their security enhancements.

Market leadership has its privileges
Of course, all the major chip companies will adopt some form of Pluton so as not to anger Microsoft – a critical partner. But saying that Pluton is a major step forward in chip security is a stretch. It's more of a convenient evolutionary process than truly revolutionary. It's really more about the ability to update from a cloud connection, but there is no specific reason that couldn't be done with current security capabilities from Intel, AMD etc. Pluton does give Microsoft a unified interface to deal with so in that sense it's an improvement as Microsoft can update all PCs running Windows at the same time rather than wait for individual companies to do their own thing.

Should anyone buy a machine based on Pluton alone?
Probably not. It's not really that much of an enhancement, and in fact many of the chip companies already add security features in their hardware that go well beyond Pluton. But it's likely that all of the chip companies will announce Pluton compatibility for their products, since Pluton is a feature included in Windows 11 (and beyond) and that uses Windows Update to keep machines fully updated. It's also likely Microsoft will add additional OS and app features built on Pluton in the future, so compatibility/support is necessary to play in the Windows ecosystem.

Bottom line: While Microsoft should be commended for trying to rationalize the needs for security across many different devices and vendors, Pluton should be seen as a feature improvement and not a major security enhancement. Any security improvement is a good thing, but this really is more of a uniformity extension than a true security upgrade. Still, future devices will all support Pluton as a necessary capability to run Windows. But assuming this is a major security improvement beyond current best practice is an exaggeration.

About J.Gold Associates, LLC.

J.Gold Associates provides advisory services, syndicated research, strategic consulting and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies. We work with our clients to produce successful new product strategies and deployments through workshops and reviews, business and strategic plan coaching and reviews, assistance in product selection and vendor evaluations, needs analysis, competitive analysis, and ongoing expertise transfer.

J.Gold Associates provides its clients with insightful, meaningful and actionable analysis of trends in the computer and technology industries. We have acquired a broad based knowledge of the technology landscape and business deployment requirements, and bring that expertise to bear in our work. We cover the needs of business users in enterprise and SMB markets, plus focus on emerging consumer technologies that will quickly be re-purposed to business use.

We can provide your company with a trusted and expert resource to maximize your investments and minimize your risk. Please contact us to see how we can help you.

J.Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA

Phone:
+1-508-393-5294

Web:
www.jgoldassociates.com

Research, Analysis, Strategy, Insight