Guardicore

CASE STUDY

Openlink Strengthens Cloud Security with Guardicore

The Client

Openlink is the global leader in trading, treasury, and risk management solutions for energy, commodities, corporate, and financial services companies. More than 37,000 users from 600+ clients use the company's highly sophisticated software for activities such as hedging commodity prices, automating logistics, forecasting raw material needs, and trading derivatives.

The Challenge

Securing a Cloud Infrastructure - and Client Confidence

Like many enterprise software providers, Openlink is undergoing an IT transformation from on-premise delivery and support of its products to a public cloud deployment. Its Openlink Cloud platform, the first of its kind in the industry, launched in May 2017 via Microsoft Azure.

"There were two main drivers for us to move to the public cloud," explains Michael Lamberg, Vice President and Chief Information Security Officer with Openlink. "Because our software is processing intensive, clients typically build their computing environment for peak processing capacity, which carries an extremely high capital expenditure. By moving into the public cloud, we can auto-scale the application during times of peak demand, so the clients aren't paying for capacity they're not using. Second, our clients typically maintain several Dev Test (development) environments for testing new versions of our software and client add-ons. By using the public cloud, it's much easier for us to spin up an environment when they need it for their testing and remove it when they are done to minimize cost."

Of course, moving to the cloud brings a host of new security concerns. Openlink becomes responsible for protecting its clients' extremely sensitive and highly strategic data which could be targeted by malicious actors. Since cybersecurity in the public cloud operates under a shared responsibility model (where the cloud provider offers a finite spectrum of security measures subject to rigorous auditing and certification), the cloud customer (Openlink in this case) is ultimately responsible for securing its own data and processes.

openlink

"The tools we used to rely on to analyze how an infrastructure operates have changed [with the advent of the public cloud]."

- Michael Lamberg,
Vice President and Chief Information Security Officer, Openlink

"The major cloud providers have really come a long way in the last 5 years in terms of their ability to secure large infrastructures," says Lamberg. "They are actually doing a much better job than many organizations managing their own data centers. But everyone operates on a shared trust model. Azure may have the highest level of security certifications globally right now, but they're not going to protect us from our own implementations."

Openlink recognized the need to enhance Azure's security infrastructure with third-party solutions in order to provide the customized level of risk mitigation that Openlink and its clients require. "We have to be able to prove to our clients that, not only is Azure doing what they say they're doing, but also that we are adding a security layer on top of them, further strengthening the overall defense-in-depth controls of our clients' cloud-hosted data and environments."

The Solution

Guardicore Centra™ Security Platform

Lamberg was introduced to Guardicore about a year prior to the Openlink Cloud launch, and saw immediately how it could help augment the company's cloud security infrastructure. The Guardicore Centra™ Security Platform is designed to fill a critical blind spot in multiple infrastructures, namely lateral movements of intruders that have managed to get past firewalls and intrusion prevention systems. Focusing on detecting suspicious anomalies in east-west traffic, the Guardicore solution confirms and contains active breaches before they can do significant damage.

"A rude awaking moving to the public cloud is that everything you knew about networking and infrastructure might as well get thrown away," explains Lamberg. "It no longer applies from two perspectives: one is that you no longer have control over or access to lower layers of the infrastructure stack that's been virtualized by Azure. And the second is that the tools we used to rely on to analyze how an infrastructure operates have changed. So that's something you have to get your head around. All of your traditional networking skills and experience are not as helpful as they used to be. It's all new now."

Consequently, Guardicore has become one of Openlink's key security technologies Lamberg says. "It provides assurances that are we locking down the environment properly while validating that Azure is doing its job in a very efficient and effective way."

THE BENEFITS

Enhanced Visibility and Diagnosis

With the move to a virtualized, cloud-based infrastructure, Openlink's security team was challenged by the need to gain highly granular visibility into application activity. A key feature of the Guardicore Centra Security Platform is the ability to visualize all workloads, flows and processes within a compute environment.

"Although we're in the public cloud, we are not multi-tenant," Lamberg explains. "We build a single-tenant environment for each of our clients. As a result, I need to have a full understanding of what's going on horizontally within each client's infrastructure. Lamberg cites two key use cases that leverage Guardicore. The first involves DevTest which provides clients with a test environment that enables them to quickly and easily spin up virtual machines to test Openlink's application in various configurations before moving into production. In the event of an anomaly, Guardicore enables Lamberg's team to quickly and clearly analyze the situation from a host perspective by providing visibility into all flow processes. "It may not necessarily be a security issue," says Lamberg. "It may be a case of a design or configuration flaw or perhaps the client accidentally loaded some malware and suddenly I'm seeing a command and control connection attempting to go out. Guardicore gives me the ability to immediately isolate this anomaly and view it with unprecedented clarity."

The second use case involving Guardicore is Openlink's management of the clients' supported production environment. "While our application is complex, it's extremely deterministic," says Lamberg. "So, I know all of the flows and processes that are supposed to be running on each of our servers supporting the client. This allows a baseline to be generated of their environment. In the event Guardicore notes a process or flow outside of the baseline, I'm immediately alerted."

This ability to "triage and diagnose" problems very quickly is a core benefit of Guardicore, Lamberg points out. The appearance of an unknown process or flow — which would be exceedingly difficult, if not impossible, to isolate without a tool like Guardicore - could simply signal a problem with the software or something far worse. "It's highly unlikely that anyone can get into our environment, but I need assurance that we have a proactive mechanism in place to deal with that kind of situation. Guardicore provides me that."

Guardicore also caught Lamberg's attention with its micro-segmentation capabilities, which allow security operators to set security policies around individual or groups of applications and processes. "Attacks typically occur in a lateral fashion these days," he notes. "They get a foothold in one machine and laterally jump to others. Having appropriate controls on all your machines, and being able to monitor the interaction of those machines, is the only way you're going to get ahead of that problem." Should Openlink decide to implement micro-segmentation in the future, Lamberg believes Guardicore's capabilities could put the company in a better position to do so successfully.

"Guardicore gives me the ability to immediately isolate process flow or connection-based anomalies and view them with unprecedented clarity."

- Michael Lamberg,
  Vice President and Chief Information Security Officer, Openlink

"Guardicore has been a terrific partner."

- Michael Lamberg,
  Vice President and Chief Information Security Officer, Openlink

Partners in Protection

While Openlink is benefitting from Guardicore's technology today, Lamberg also sees value in the ongoing working relationship with the people behind the solution. "I only do business with companies that are willing to partner," he says. "I don't just buy commoditized products. And Guardicore has been a terrific partner. They listen to our feedback and what we need, and they have continually refined the solution based on that."

Because public clouds are by nature dynamic, Openlink counts on Guardicore to help ensure that the company is optimizing its environments as the cloud infrastructure evolves. "They understand that to solve problems, they're going to have to work very closely with the cloud provider as well. Guardicore's steady communication with Azure ensures they are staying on top of any changes that may impact how their product operates."

As a result, Guardicore - the company and the solution - have become integral to Openlink's mission to safeguard its clients' critical assets in the public cloud. "I never want to get into a situation where I call a vendor about an issue, and they tell me, 'Well, it's a Microsoft issue, go talk to Azure.' I've never heard that from Guardicore. They acknowledge that shared responsibility efforts are required to safeguard our clients' most critical assets."

About Guardicore

Guardicore is an innovator in data center and cloud security focused on delivering more accurate and effective ways to stop advanced threats through real-time breach detection and response. Developed by the top cyber security experts in their field, the Guardicore Centra Security Platform is changing the way organizations fight cyber attacks.

More information is available at **www.guardicore.com**