CLOUDVISORY

CASE STUDY 02 | GLOBAL HEALTHCARE COMPANY

Cloudvisory detected security violations driven by potentially malicious code, allowing us to shut down the threat before any damage was done.

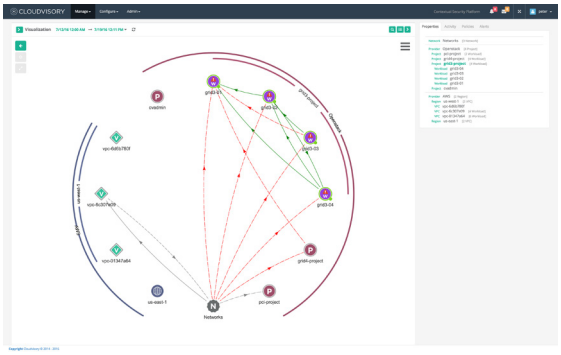
This Fortune 100 company, focused on Pharmaceutical, consumer health and medical devices is undergoing a radical modernization to their computing approach in order to be more agile, more partner and customer focused. This calls for a re-architecting of their applications with a Big-Data focus to be deployed in public and private clouds. Moving away from a traditional data center architecture, applications from Finance to HR to supply chain and even clinical data applications are migrating to this new arena. Customer centricity, business speed and agility followed by reduction in costs, are the main drivers behind this transformation.

Traditional datacenters have been difficult enough to secure. Nation State hackers have found their way into and across so many traditional network environments. Realizing this hybrid landscape of virtual machines, public and private clouds, would be subject to the same threats, the company wanted to make sure the risks associated with lateral attacks were buttoned up. Equally, they had concerns that managing security policies across various providers, environments and lines of business could quickly create bottlenecks to the very business agility they were looking to gain from the initiative.

As part of their detailed architecture re-vamp they made sure to put forth design considerations for security:

- Solutions must leverage native security controls available from public and private cloud providers
- Automated, granular, micro-segmentation of the environments to halt the East/West threat
- Auto-provisioning of security policy whenever possible
- Real-time, dynamic adjustment of policies to environmental changes, for speed and accuracy
- Real time monitoring and policy enforcement to alert on and block rogue activity.

Hence they went to the market in search of potential companies to partner with. Their analysis turned up Cloudvisory. Deployed quickly and in an early testing phase, Cloudvisory proved its worth by detecting, alerting on and blocking a very granular data-flow violation. A new virtual machine, part of a private cloud deployment, was attempting to contact the internet. The attempt was blocked, server was taken offline and forensics indicated rogue code had been inserted into the machine.



Key architecture elements of Cloudvisory Contextual Security Platform (CSP) stood out for them:

1. Cloudvisory was architected from the ground up to deal with Hybrid Cloud deployments
2. Cloudvisory utlizies cloud-native security controls of the various provider environments, streamlining security automation
3. CSP can auto-discover all native infrastructure objects and data flows using this information to automate policy provisioning
4. CSP has the most advanced approach to micro-segmentation, based on Context, which allows for highly granular and dynamic controls with minimal effort

The project is in high-gear. Cloudvisory has become a key partner in all future state architecture and design discussions as a result of fast deployment and quick detection of malicious activity.

Reach out today for a demo and a test drive of Cloudvisory's Cloud Security Platform

WWW.CLOUDVISORY.COM