



Multinational
Telecommunications and
Media Company

Business Challenge

Not long ago, a multinational telecommunications organization embarked on a massive digital transformation project in support of its strategic business evolution. As part of this initiative, the organization adopted multiple public cloud providers, containerization technologies such as Docker and Kubernetes. It implemented CICD capabilities to support many DevOps teams.

Similarly, its security tools and processes needed to evolve along with the underlying application infrastructure and delivery strategy. Perimeter-centric approaches, network hardware appliances, heavy traditional agents, and legacy vulnerability scanning tools were not going to be effective in the new environment. In addition, the security also needed to address ephemeral and elastic workload environments since the organization added IaaS and containerization solutions to the mix.

Ultimately, the organization needed to move security from the perimeter to a workload-based model that could support multiple public and private cloud environments simultaneously. The solution required:



Scalability



Automation



Integration

- Transparent elasticity and extremely high scalability (millions of assets simultaneously protected across thousands of application environments)
- Extensive automation to ensure efficiency, prevent the need for significant.
- Integrations to leverage existing technologies.

The Solution: Fidelis CloudPassage Halo®

The global telecommunications leader evaluated numerous vendors who claimed to provide agile cloud security. It eventually narrowed the field to two. After the final evaluations and proof-of-concept (PoC) testing, the organization chose the Fidelis CloudPassage Halo® platform, purchasing two unified cloud security services-Fidelis CloudPassage Halo Server SecureTt.1 and Fidelis CloudPassage Halo Container Secure™.

There were several key features that separated Fidelis Halo from the competition.

First, Fidelis Server Secure automatically protects workloads anywhere, anytime, regardless of the location or IP address. This automated and comprehensive cloud security is important to a geographically diverse enterprise organization that needed a unified defense to keep up with its growing number of workloads.

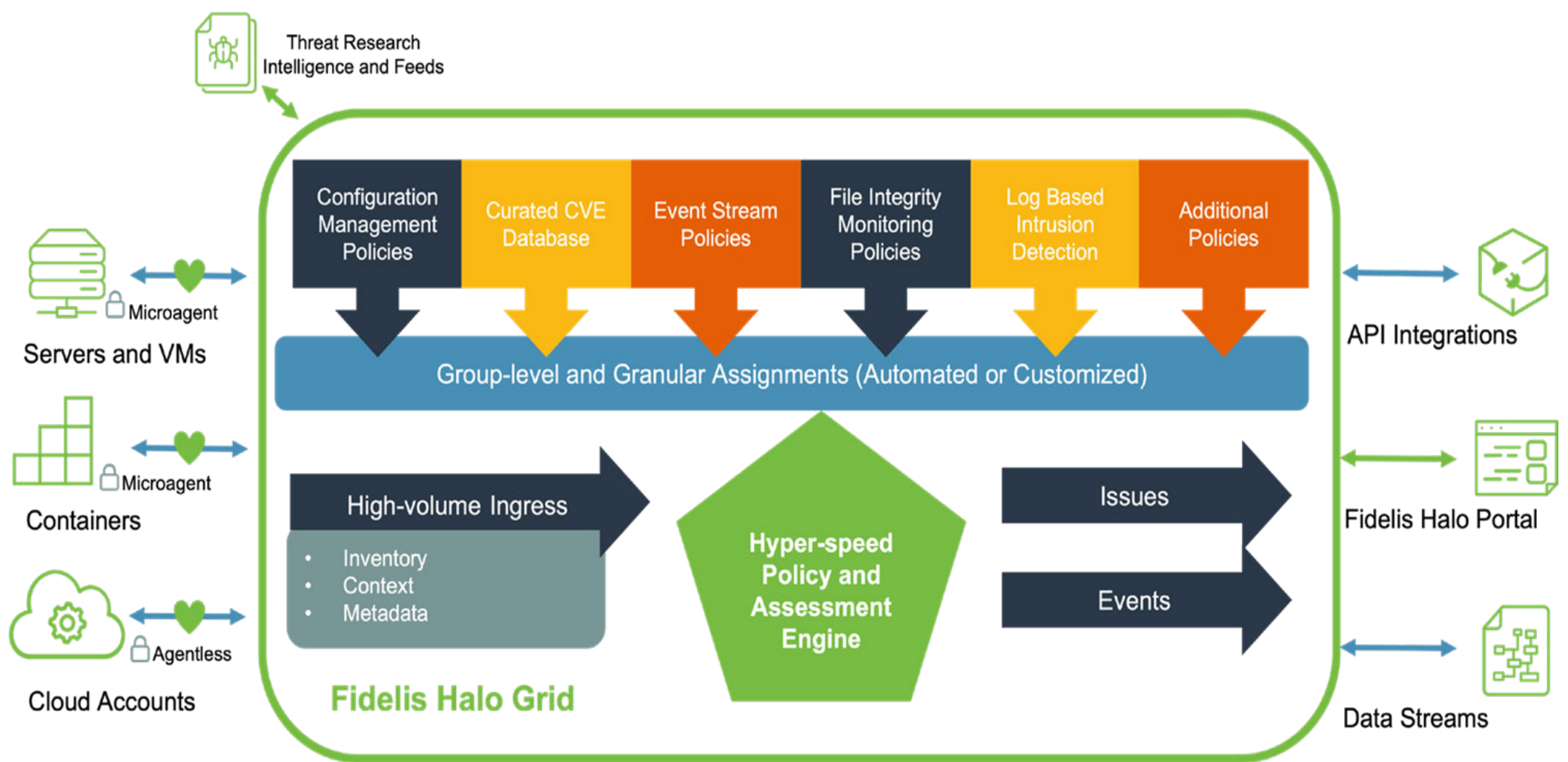
Scalability was another advantage. The organization wanted to be able to implement consistent cloud security across tens of thousands of public and private servers in use, quickly, without needing to deploy additional security products on-site.

In anticipation of rapid adoption of container technologies, the company also wanted rapidly deployable security for thousands of container hosts, tens of thousands of images, and an almost immeasurable number of container instances. Fidelis Container Secure scales dynamically and automatically with a cloud footprint, staying ahead of new assets and workloads, configuration changes, and containerized environments.

Fidelis Halo also provides visibility into security and compliance functions such as workload protection, micro segmentation, and compromise detection. Using Fidelis Halo, the organization has stayed ahead of configuration changes that violate policies and rules-both innocent and malicious-with real-time alerting on configurations that put an enterprise at risk.

The organization's security team appreciates that Fidelis Halo's lightweight agents enable fast deployments, quick set up, and easy maintenance. Its patented micro agent architecture is compact and efficient. It has only two agents-one for Windows-based kernels, and one for Linux-based kernels that only consume around 2 MB in memory.

Finally, Fidelis Halo's comprehensive bi-directional REST API was flexible enough to allow the organization to easily integrate it into its various other security tools. This accelerated workflows and streamlined communication and compliance with DevOps teams, helping to recover precious staff hours from menial administrative efforts.



Results

Once the organization's security team implemented the Fidelis Halo platform, they had the visibility into their cloud environments and workloads they needed. Fidelis Service Secure automates a broad range of security and compliance needs along with delivering protection for legacy virtual machines and bare-metal hosts. The organization monitors its fleet of more than 100,000 workloads for configuration compliance, vulnerabilities, exposures, and threats based on its internal company security policies.

The organization also implements Fidelis Halo's extensive network traffic monitoring and host-based firewall policy orchestration in support of a datacenter microsegmentation initiative.

The organization continues to ramp up the services by integrating them with projects and using the APIs to pull information and feed it into multiple security stacks and other internal systems. Most recently the organization began work on an expanded implementation that includes Fidelis Container Secure to defend containers in a new network cloud environment in support of its mobile business.

Fidelis Halo platform helps the organization leverage the inherent efficiency of the cloud environment by distributing security for workloads across its networks and servers. This allows the organization to freely innovate and rapidly deploy new technologies and capabilities. It unifies and simplifies security, enhances productivity, lowers total cost of ownership, and reduces the security barriers the team previously faced when distributing new technology into the enterprise. Vendors and developers now can confidently introduce new capabilities into the telecommunications cloud environment quickly, safely, and securely.

Benefits

- Immediate cloud asset and risk visibility
- Deeper, more actionable cloud security intelligence
- Improved operational and financial benefits of cloud computing through scalability
- Minimal load on protected servers with lightweight microagent
- Saved time with automated, bi-directional REST API

About Fidelis Security

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms. Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure. Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.

