CASE STUDY

Large Government Contractor Extends Security to AWS Public Cloud

Small team efficiently manages hybrid physical, virtual, and cloud infrastructure

Large Government Contractor

Customer Profile
Business process provider to government health and human services agencies

Industry
Technology, government

IT Environment
35,000 endpoints across physical infrastructure, as well as private and public cloud

By adding McAfee Cloud Workload Security to its existing McAfee®-integrated security architecture, this company can now reap the benefits of leveraging the public cloud. And, thanks to McAfee® ePolicy Orchestrator® (McAfee ePO™) software, deploying and managing cloud security is easy and adds minimal additional overhead.

Connect With Us

A large, for-profit government contractor based in the eastern corridor of Washington, D.C. provides business services to government agencies in the US and other countries. Employing more than 15,000 professionals, the organization administers programs of all sizes, from enormous federal programs to smaller state and local programs that directly assist a broad sector of the population.

Biggest Challenge of Adopting the Cloud isn't Technical

Increasingly the organization's clients had begun asking about the possibility of receiving cloud-based services because of lower TCO. Internally, the company also realized that it could reap significant benefits from providing services using the public cloud. Like its customers, the organization could take advantage of reduced TCO. Using the public cloud, it could also quickly ramp up or scale down the number of users—a huge benefit for a company with so many contracted projects.

Clearly, the cloud belonged in the government contractor's future, so the system analyst and his colleagues set out to figure out how best to secure it. In the process, they discovered that, as he puts it: "The biggest challenge of the public cloud isn't technical." Rather, it is overcoming the perception that the cloud can't be secured.

"We have had to educate both internally and externally that we can extend our existing threat defenses beyond our physical infrastructure to the public cloud," says the system analyst. "Education is ongoing, but our success thus far at securely leveraging the public cloud is converting the naysayers."

Easy Deployment of Cloud Protection for AWS

After carefully researching cloud security options, the company decided to implement McAfee Cloud Workload Security before launching its first contracted project using Amazon Web Services (AWS). They already relied on the McAfee integrated security platform and a variety of McAfee solutions to secure its physical and virtual infrastructure of 35,000 endpoints (including servers). These products are all managed using the McAfee ePO central console—as is McAfee Cloud Workload Security.

"Adding the public cloud to our McAfee infrastructure was simple," notes the system analyst. "We spun out the cloud side in less than a week. With McAfee ePO software, it was easy to implement McAfee Cloud Workload Security and set security policies for the project."

As part of the McAfee Cloud Workload Security solution, they deployed the Data Center Connector for AWS, Cloud Usage Metering, Data Protection for Cloud, Data Center Visualization, and Data Center Assessment components. With this functionality, the organization has

Challenges

- Securely take advantage of the benefits of the public cloud
- Provide robust defenses for hybrid environment
- Enforce multitenancy security policies for endpoints in the cloud
- Overcome perception that the cloud can't be secured

McAfee Solution

- McAfee® Cloud Workload Security
- McAfee® Server Security Suite Essentials
- McAfee® Endpoint Security
- McAfee® ePO™

Results

- Flexibility, scalability, and TCO benefits of leveraging the public cloud
- Easy management of hybrid environment by small team
- Faster time to compliance and remediation with automated reports and responses
- Foundation laid for expanded use of the public cloud in the future

end-to-end visibility into all cloud workloads and their underlying platforms and insights into weak security controls, unsafe firewall and encryption settings, and indicators of compromise (IoCs). In addition, the same McAfee Endpoint Security, which protects its physical and virtual endpoints, protects the company's endpoints within the AWS cloud.

Flexibility and Bandwidth to Accommodate Volatility in Server Volume

The company's first AWS-based project serves a handful of US federal government agencies with a combined total of 1,500 endpoints. As part of the project, the company created a web-based portal where authorized users from these agencies can review aspects of their program's infrastructure, request changes, and exchange information. "Portal traffic is very fluid," explains the system analyst. "The number of servers can increase or contract sometimes daily; five to 20 instances come online very week. The public cloud is the perfect vehicle to handle such fluctuations in bandwidth requirements."

For this multiple-agency project, the workloads that run in the public cloud are generated by:

- SQL and Oracle databases
- Imaging software, since a huge volume of documents need to be stored digitally for years
- Agency- or contract-specific applications

Small Team Able to Manage Security Across Hybrid Environment

For this project, 95% of the security policies for the endpoints within the AWS public cloud are the same as for the company's physical endpoints, but 5% are unique to the project. "We run a base set of policies for every project, to meet ISO requirements and so on, but with McAfee ePO software, we can easily add or customize policies to meet the security needs of each specific contract and project," notes the system analyst.

Thanks to the intuitive McAfee ePO management console, the company's information security team of five, spread across three locations, can effectively and efficiently manage a host of McAfee solutions and even some non-McAfee solutions, across a widely dispersed physical and virtual infrastructure that includes private and public cloud. "As a small but dispersed team, we must have tools that work well together and enable us to work efficiently with one another," says the system analyst. "McAfee ePO software is basically our eyes and ears across the entire environment. We use it for day-to-day management as well as to remediate threats quickly in conjunction with our McAfee SIEM."

Custom Reports and Automated Responses Speed Compliance and Resolution

Using McAfee ePO software, the system analyst and his colleagues have also created customized reports and automated responses as an added cloud defense measure. "To us, whether the endpoint is in the public cloud or on premises, it doesn't matter," he says. "We use McAfee ePO software the same way, to manage as well as accelerate time to compliance and resolution."

For example, in McAfee ePO software, he created an agent access report, which runs frequently. The report details which endpoint agents are not reporting back on a regular basis. If an agent doesn't respond within a set number of minutes—the number is set in the project contract—then the information security team will automatically be notified to investigate. The team also receives automatic notifications if file integrity monitoring queries discover that certain thresholds are reached, such as a user accessing an executable file a certain number of times within a certain number of minutes.

"Full Speed Ahead" for AWS Expansion

The government contractor has built a hardy, multilayered defense with a McAfee integrated security infrastructure backbone that protects its widely dispersed, hybrid environment and numerous, global government customers. With the addition of McAfee Cloud Workload Security, they have extended that defense and laid the foundation for securely leveraging the public cloud even more in the future, to the benefit of both the company and its customers.

"Now that we can extend robust security to the public cloud, it's not a question of if we'll put more projects in AWS, but how many," says the system analyst. "It's full speed ahead."

> "... Adding the public cloud to our McAfee infrastructure was simple. We spun out the cloud side in less than a week. With McAfee ePO software, it was easy to implement and set security policies for the project."
>
> —System Analyst, Large Government Contractor

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com