Securing the Cloud: Simple deployment of empow on the major cloud providers

As the number of employees working from home continues to grow, coupled with the movement to cloud computing for financial flexibility, the importance of effectively securing critical cloud infrastructure grows. Each cloud has specific and unique requirements (see our AWS and Azure Integration Tech Notes). However, one of the simplest ways to fully integrate cloud security is through a cost-effective deployment of empow's i-SIEM in cloud environments.

empow supports a range of virtualized hardware resources for deployment on cloud providers.

empow's i-SIEM instance configurations are deployed on Amazon EC2 (AWS), Google Cloud Platform (GCP) and Microsoft Azure. For each of these cloud providers, empow provides a sizing guide and a recommendation for instance types or custom machine types.

empow resource usage optimization allows reduction of the overall cost of cloud management both in terms of storage and memory usage. At the same time, empow's sizing methodology is volume focused and supports heavy logging, monitoring and security analysis operations.

Prior to deployment, empow provides a customized deployment strategy based on estimated data flow (events per second), data retention requirements, network topology and security goals.

With empow deployment in the cloud, all basic logs and plugin connectors are supported out of the box, including cloud applications APIs, firewall logs, Windows logs, endpoint logs and others.

Secure access to empow in the cloud

Regardless of the chosen deployment option, empow secures the data in motion and at rest. All communication to empow's i-SIEM cloud deployment is protected with SSL / TLS data encryption and credentials for access control. empow's database is password protected and all user credentials are encrypted and stored securely behind empow's proxy. In addition, empow supports single sign-on authentication to allow integration with identity and access management solutions.

Additional security measures for data ingestion include minimizing the open ports from outside data sources, as well as using queue messaging technologies to isolate the data storage from the ingestion nodes.

Monitoring cloud from the cloud

As organizations move their applications to the cloud, monitoring those applications and platforms requires access outside of corporate network perimeters. Remote employees connected via a cloud access security broker (CASB), as well as directly to the various cloud

services and applications generate vital data for security that is not accessible through typical endpoint solutions or Windows logs.

empow's cloud deployment supports multiple cloud applications and CASB solutions and adds User Event Behavior Analytics (UEBA) modules to cloud solutions such as Azure AD, O365, Web Proxy and application layer Firewalls. Read more:

- Securing the cloud – Integrating into AWS
- Securing the cloud – Integrating into Azure