direktiv

CASE STUDY

Server-Side Email Encryption

Customer

Dell Technologies Managed Services (DTMS)

DELL Technologies

Problem Background

As a managed service provider, DTMS is responsible for the health, capacity and availability of the customer environment. DTMS leverages a combination of on-site engineering and off-site 1st & 2nd level support. As with many service providers, data and information regarding the systems need to be sent (via email) from the server-side components to the engineering and support teams. The server-side components do not have the ability to encrypt emails or event notifications.

Problem Statement

Prevent data leakage from the internal customer environments to the managed service provider (email, SNMP traps or external API calls).

Problem Impact

Data leakage has a financial impact (financial institutions can incur fines from regulatory bodies), reputational damage, legal action or loss of sensitive data.

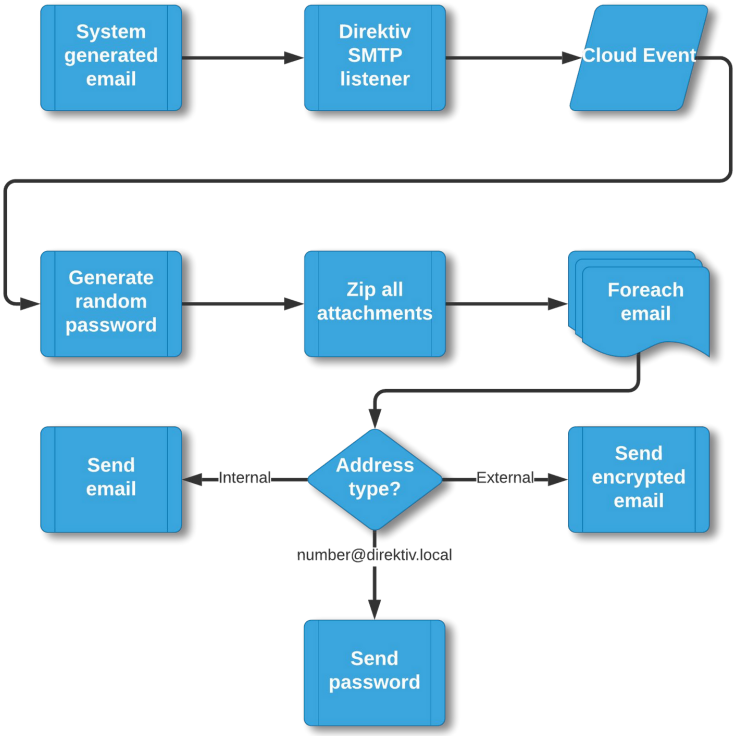
Solution

Using **Direktiv** as an email server (leveraging the basic **Direktiv** SMTP listener), emails from all server-side sources are intercepted and deconstructed into objects.

The DTMS team has the ability to encrypt and compress any component of the deconstructed email object. The workflow is a simple YAML definition, and all the plugins and extensions are containers developed and owned by the DTMS team.

This ensures that the code-level is maintained at a secure level without any external code artifacts or plugins being used.

All changes to the workflow is self-maintained by the DTMS team, whilst offering the API endpoint to the customer as a service.



Business Outcome

Effort estimation savings 1.5 FTEs and guaranteed delivery of encrypted emails according to security policy requirements.

Read more about Direktiv.io