Seguridad Cloud Native

By **Antonio Juanilla**(Specter)

HACK &BEERS

$Whoami

Antonio Juanilla

1. Autodidacta.
2. DevSecOps.
3. Co-Organizador de HackMadrid%27 y Co-Fundador de HackBarcelona%27
4. Miembro del equipo de FlagHunters
5. Amante de la tecnología.
6. Defensor de la democratización de la tecnología para la mejora de la sociedad.

Redes

Twitter: **@spectertj**

Linkendin: https://www.linkedin.com/in/spectertj

Github: **spectertj**

HACK &BEERS

Empezamos hablando de:

CLOUD

Cloud Computing

Conocida también como **servicios en la nube**, **informática en la nube**, **nube de cómputo**, **nube de conceptos** o simplemente «**la nube**», es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.
Wikipedia

Empezamos hablando de:

CLOUD NATIVE

Cloud Native

Cloud Native (nube nativa) es un patrón de arquitectura de software para desarrollar aplicaciones usando principios esenciales de cloud computing como la escalabilidad, elasticidad y agilidad.

Y tambien integrando conceptos como Continuous Delivery/integration/deployment o CI-CD, DevOps, microservicion, serverless, y contenedores.

Diferencias entre Cloud y Datacenter

Datacenters(on premise)

1. Parcheo manual y mantenimiento
2. On premise(tu responsabilidad)
3. Maquinas físicas(hierro)
4. Corre en tu propia red(Intranet)
5. Se necesitan elementos para suplir de corriente a los equipos, energía de respaldo por si se va la electricidad, maquinas de respaldo(backups)
6. Se necesita personal operativo(Ops) disponible 24/7
7. Despliegue de aplicaciones en servidores especificos

Cloud

1. Off premise (no es tu responsabilidad)
2. Auto escalado, no se necesita comprar nada en el progreso
3. Siempre basado en la disponibilidad del internet
4. Infrastructure as a Service(IaaS)
5. Las aplicaciones pueden estar en diferentes y cualquier servidor
6. El mantenimiento no es tu problema
7. Manejo centralizado y visibilidad
8. Disponibilidad geográfica o geográficamente distribuido

Hablemos de lo que nos gusta xD

CLOUD NATIVE SECURITY

Cloud native security

- Zero trust.
- Automatización de parcheos y manejo de parcheos.
- Automatizacio de la seguridad en el ciclo de desarrollo software(SSDLC).
- Visibilidad total y monitoreo de amenazas.
- Seguridad como código.

Cloud native security

- DevSecOps.
- Escribir playbook para automatizar respuestas de seguridad.
- Usar herramientas de Cloud Native, como SIEM en la nube.
- Application Gateway.
- WAF nativos.

Seguridad entre Cloud y Datacenter

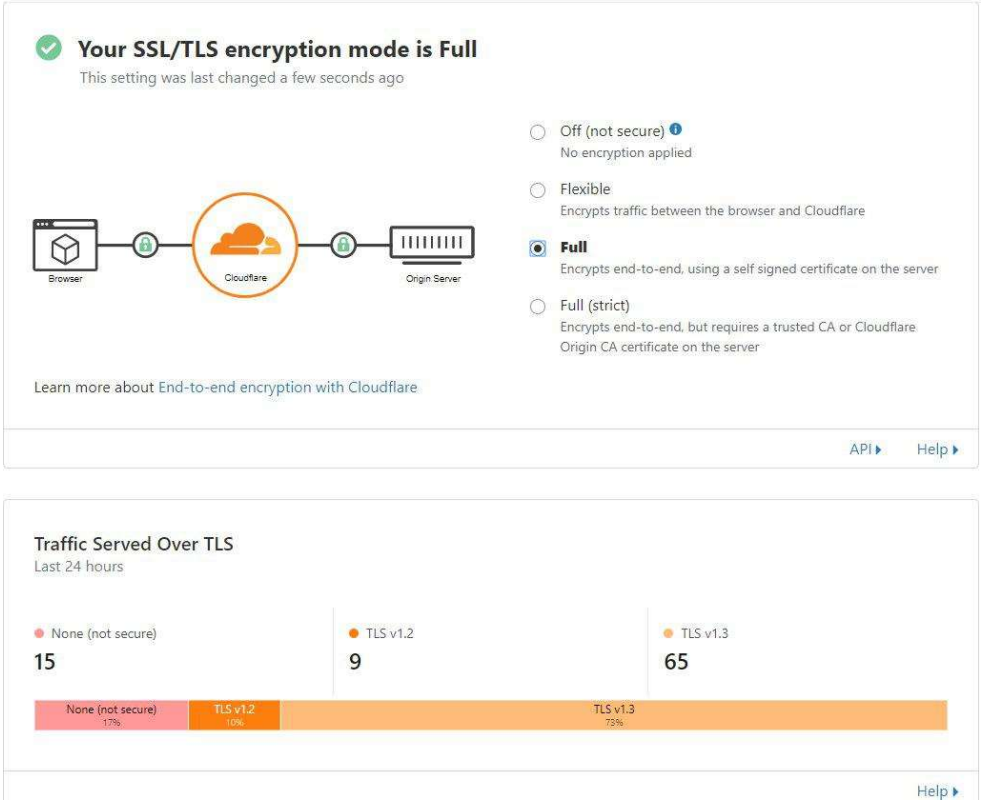
Datacenters(on premise)

1. Zona
2. Parcheo manual y mantenimiento de los parches
3. Seguridad física

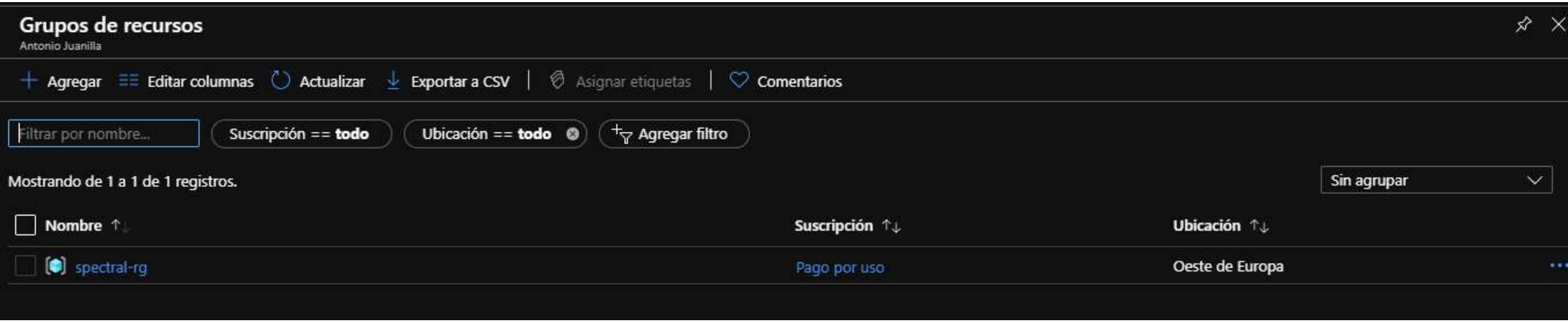
Cloud

1. Off premise (no es tu responsabilidad)
2. Auto escalado, no se necesita comprar nada en el progreso
3. Siempre basado en la disponibilidad del internet
4. Infrastructure as a Service(IaaS)
5. Las aplicaciones pueden estar en diferentes y cualquier servidor
6. El mantenimiento no es tu problema
7. Manejo centralizado y visibilidad
8. Disponibilidad geográfica o geográficamente distribuido

Ejemplo


Your SSL/TLS encryption mode is Full
This setting was last changed a few seconds ago
Browser
Cloudflare
Origin Server
Off (not secure)
No encryption applied
Flexible
Encrypts traffic between the browser and Cloudflare
Full
Encrypts end-to-end, using a self signed certificate on the server
Full (strict)
Encrypts end-to-end, but requires a trusted CA or Cloudflare Origin CA certificate on the server
Learn more about End-to-end encryption with Cloudflare
API
Help
Traffic Served Over TLS
Last 24 hours
None (not secure)
15
TLS v1.2
9
TLS v1.3
65
None (not secure) 17%
TLS v1.2 10%
TLS v1.3 73%
Help

Ejemplo


Grupos de recursos
Antonio Juanilla
Agregar
Editar columnas
Actualizar
Exportar a CSV
Asignar etiquetas
Comentarios
Filtrar por nombre...
Suscripción == todo
Ubicación == todo
Agregar filtro
Mostrando de 1 a 1 de 1 registros.
Sin agrupar
Nombre
Suscripción
Ubicación
spectral-rg
Pago por uso
Oeste de Europa