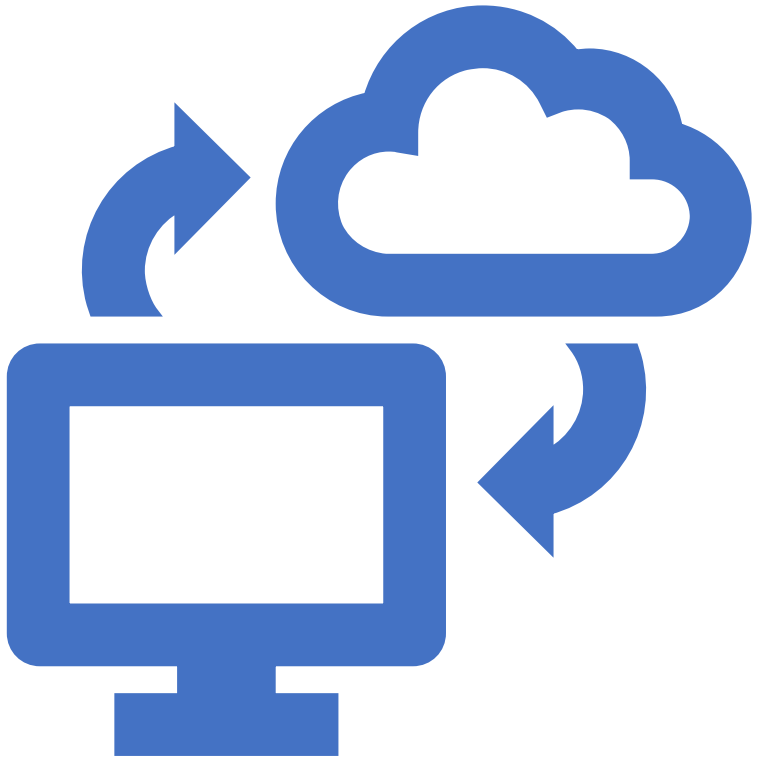


Data protection per aziende e studi professionali: un approccio essenziale alla sicurezza dei dati e delle informazioni

A cura di Ugo LOPEZ

Chi sono

- Ingegnere informatico (forense)
- Docente incaricato di informatica forense (Uniba-Sicurezza Informatica)
- Trainer LinkedIn (cybersecurity)
- Consigliere direttivo ONIF
- Membro gruppo Cybersecurity/C3i
- Telegram/Twitter/Matrix: @ugolopez
- LinkedIn: ugolopez.link/LinkedIn

Gli asset da proteggere/analizzare

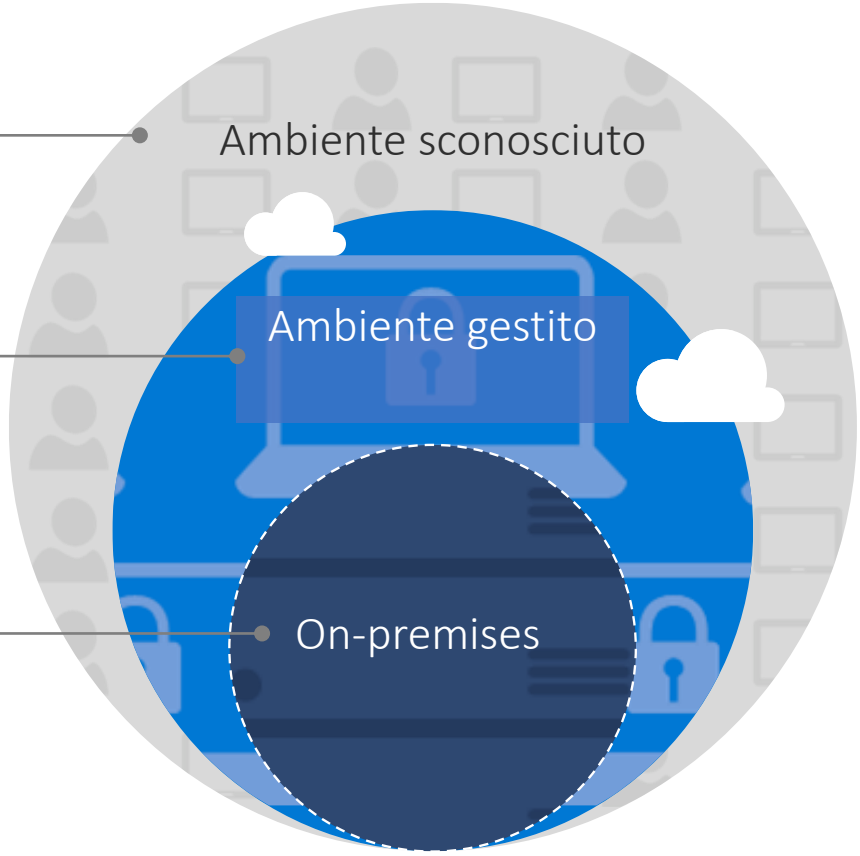
- Identità
- Periferiche
- Applicazioni
- Dati

Evoluzione del concetto di perimetro

Mondo esterno (dati ibridi)

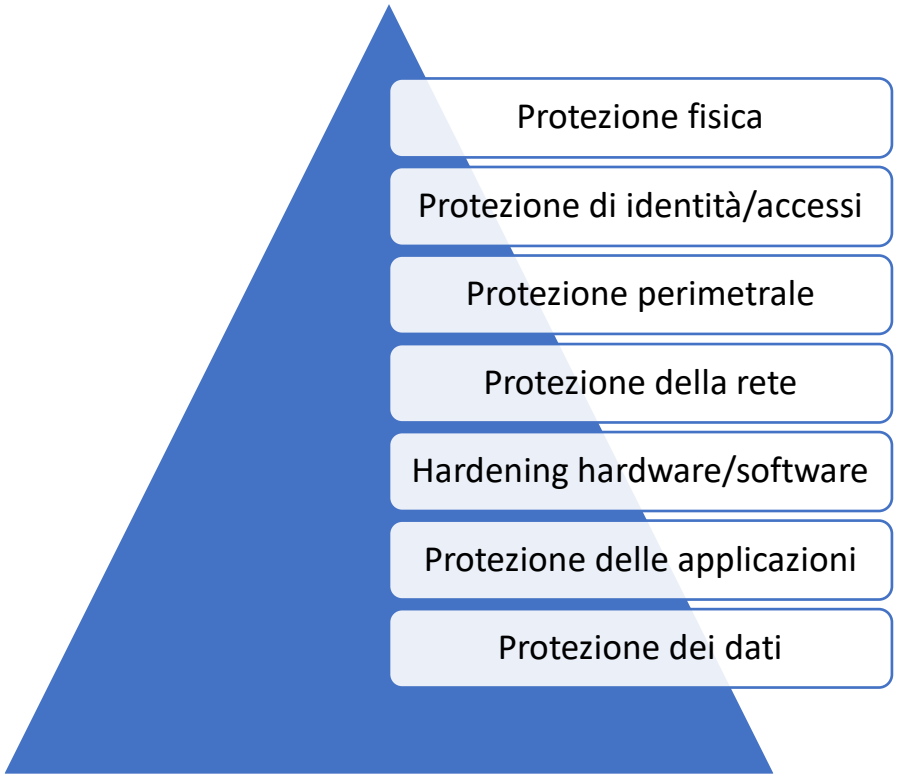
Protezione e gestione delle identità e delle periferiche

Protezione perimetrale



Le strategie di protezione

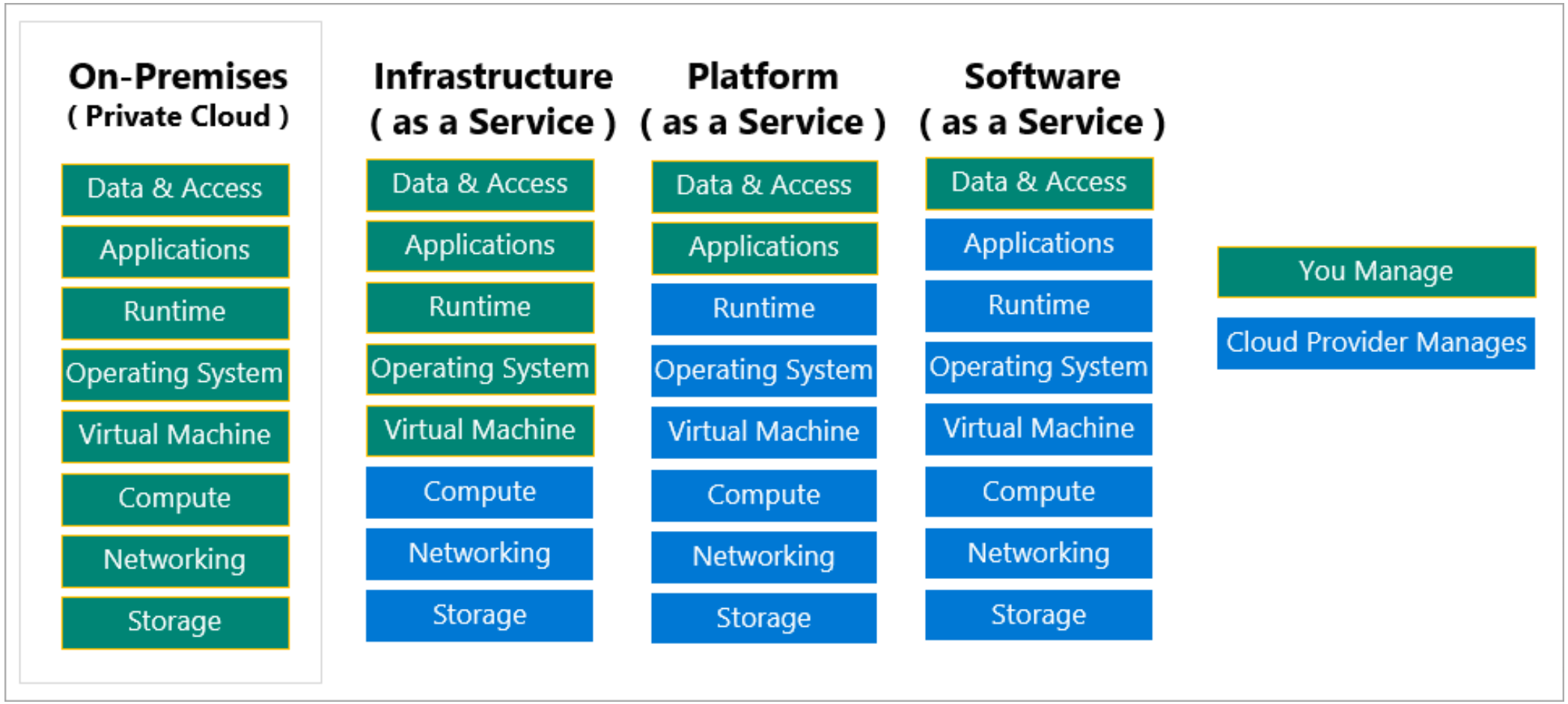
Defense-in-depth



Zero Trust

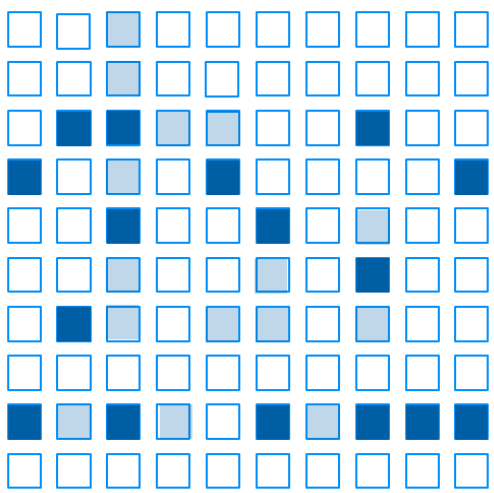
- “Trust no one, verify everything”
- Verifica esplicita di tutti gli asset
- Least privilege
- Least administrative effort
- Approccio “assume breach”

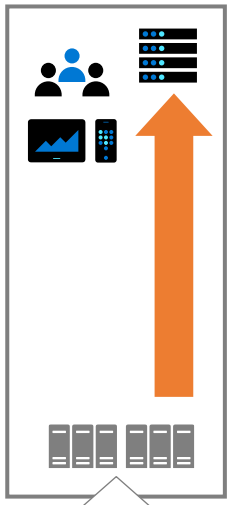
Modello a responsabilità condivisa



Sicurezza cloud-enabled

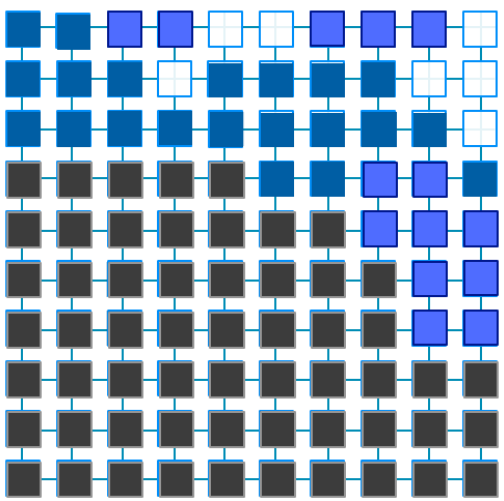
Approccio tradizionale





Asset da proteggere

Sicurezza cloud enabled



Responsabilità ora assegnate al cloud provider con lo stesso livello di efficienza (risorse riallocabili)

Responsabilità ora assegnate al cloud provider con aggiore livello di efficienza (risorse riallocabili)

Responsabilità gestate attraverso IA/ML

La sicurezza è un processo sfidante e, spesso, povero di risorse

Responsabilità assegnata | Responsabilità non assegnata | Responsabilità parzialmente assegnata | Responsabilità del cloud provider

Protezione delle identità

- Il modello Just-in-Time/Just-Enough
- Sistemi di access review
- Identity/Access protection (identità sensibili)
- Sign-in risk/User risk
- MFA
- Autenticazione frictionless/passwordless
- Accesso condizionale
- SSPR (no domande di sicurezza)

Autenticazione “portatile” – standard FIDO/2

Condivisione di password

Utilizzare mezzi alternativi (e.g. caselle di posta condivise)	• Riduce la possibilità di accountability
Mai attraverso mail	
Possibilmente mai attraverso applicazioni di messaggistica	• Qualora utilizzata, preferire chat cifrate end-to-end • Eliminare **per tutti** non appena terminata la necessità
Utilizzare sistemi specifici (e.g. Kpaste, gratuito), meglio se dedicati aziendali	

ToDo

Ridurre accesso SSO delle app terze parti (e.g. giochi Facebook)

Protezione dei dati

- Il modello RBAC
- Il metodo etichette → policy
  - Automatizzate
  - Suggerite
  - Modificabili
  - Manuali
- Crittografia mista (interna o esterna)
  - Pubblica
  - Privata
  - Hash
- DLP
- DRM/IRM

DLP

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. Learn more about DLP policy templates

gdpr

All countries or regions

Categories

Privacy

Templates

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR)

Helps detect the presence of personal information for individuals inside the European Union (EU) to assist in meeting GDPR privacy obligations.

Protect this information:

- EU Debit Card Number
- EU Driver's License Number
- EU National Identification Number
- EU Passport Number
- EU Social Security Number (SSN) or Equivalent ID
- EU Tax Identification Number (TIN)

Sensitivity label

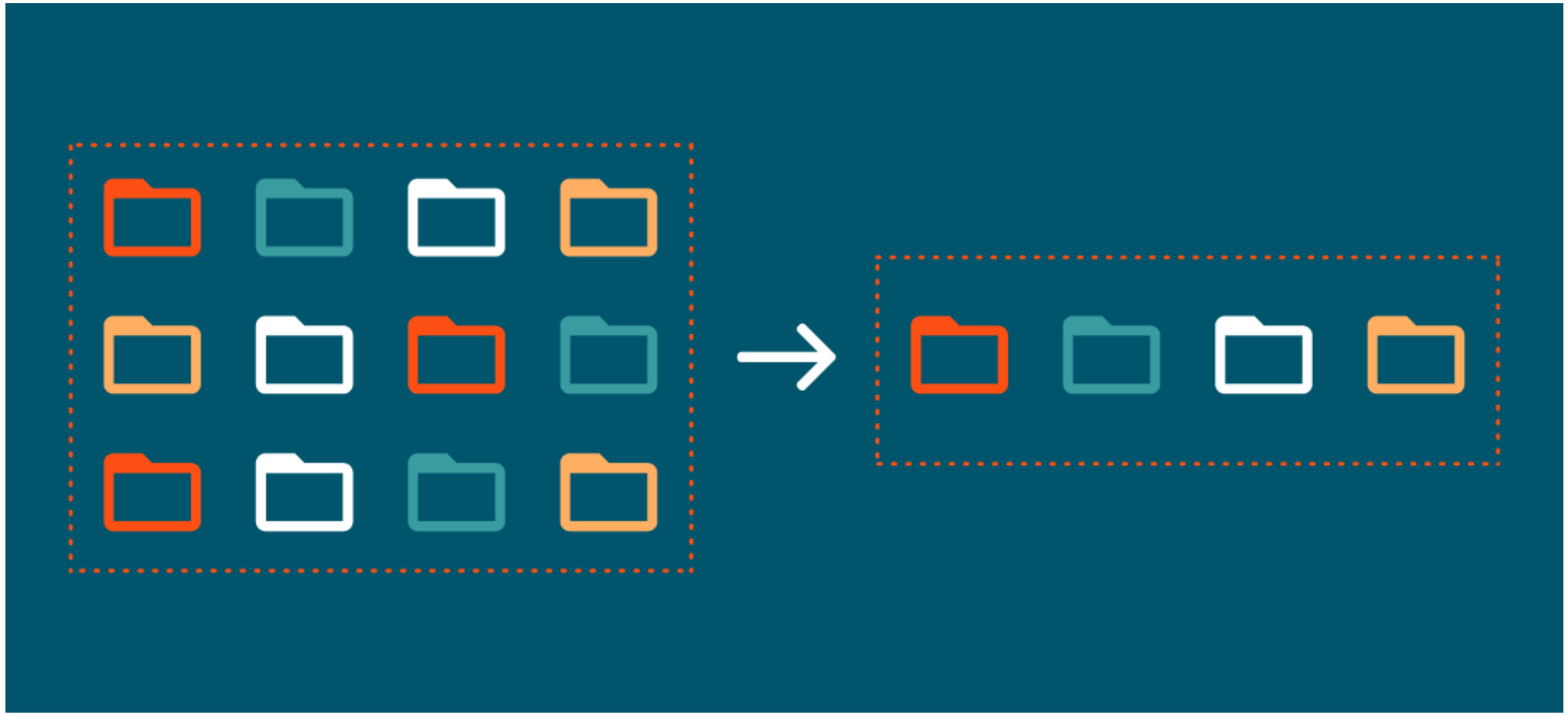
Choose protection settings for labeled items

Configure encryption and content marking settings to protect labeled items.

☐ **Apply or remove encryption**
Control who can access items that have this label applied.

☐ **Apply content marking**
Add custom headers, footers, and watermarks to items that have this label applied.

Deduplicazione dei dati



https://blog.quest.com/what-is-data-deduplication-and-how-can-my-organization-benefit-from-using-it/

BLOCK STORAGE

OBJECT STORAGE

FILE STORAGE

https://qumulo.com/blog/block-storage-vs-object-storage-vs-file-storage/

Alert

Alert policies

Create alert policies to notify you when certain email-related events occur. You can create policies for domain loops, new users forwarding emails, slow mail flow, new domains being forwarded emails, delayed or rejected messages, and more. Learn more about alert policies

Export | New alert policy | 3 items | Filter | Search

Alert name	Severity	Status	Type	Last modified
Reply-all storm detected	High	Active	System	3 months ago
Priority accounts' mail flow is unhealthy	High	Active	System	2 years ago
Messages have been delayed	High	Active	System	4 years ago

Monitoraggio delle app

Sistemi di cloud app protection

Reverse proxy (app LoB)

Protezione delle periferiche

- MAM
- MDM
- Integrazione con accesso condizionale

Protezione avanzata dalle minacce

Link analysis/rewriting

- Click-time analysis

Analisi degli allegati

- Può lavorare assieme alla link analysis
- ZAP
- Sandbox per malware analysis

شكراً جزيلاً
ngiyabonga
рахмат
danke
謝謝
spas
teşekkür ederim
Баярлалаа
mersi
kia ora
barka
welalin
tack
mahalo
tapadh leat
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
kiitos
dankie
nanni
nandri
dhanyavad
thank you
gracias
хвала
asante
manana
obrigada
tenki
bedankt
bayarlalaa
gràcie
hvala
maururu
köszönöm
aciu
dankon
akun
djiere dieuf
tau
mochchakkeram
murakoze
enkosi
dziękuję
дякую
mamnun
chnorakaloutioun
gracies
sulpáy
go raibh maith agat
chokrane
sobodi
dēkuji
sagolun
sukriya
kop khun krap
taiku
obrigado
mèsi
ありがとう
tanemirt
grazie
arigatô
takk
dakujem
trugarez
didi madloba
najis tuke
terima kasih
rahmet
diolch
dhanyavadagalu
shukriya
merce
мерси
kam sah hamnida
rahmat
감사합니다
xièxie
ευχαριστώ
merci