

SOPHOS

La journée du CLOUD

LA PROTECTION DES DONNÉES DANS LE CLOUD

Gilles SARQUIZ

Benjamin MERCUSOT

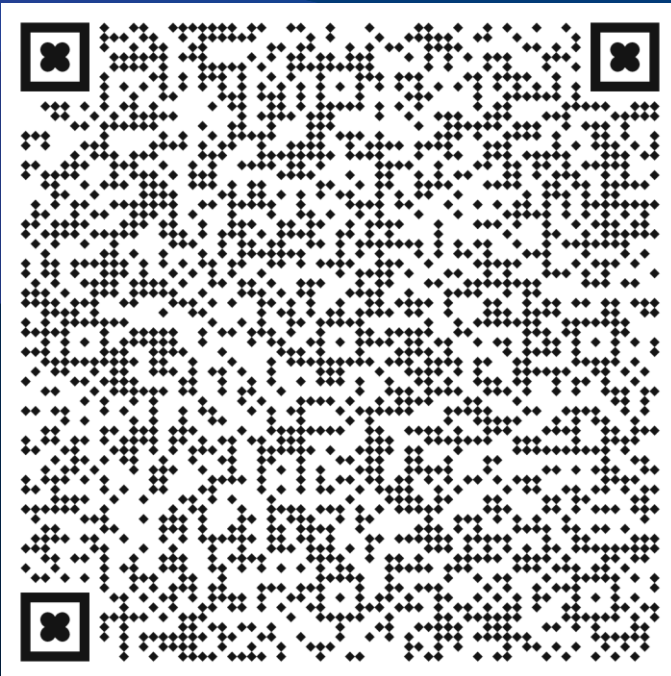
jeudi 4 février 2021

70%

*Des entreprises
hébergeant des données
dans le cloud ont
rencontré un 'incident'
de sécurité **durant**
l'année écoulée.*

Ça fait l'actualité, c'est de plus en plus sophistiqué.

<https://tinyurl.com/Cloud-accounts-hijacked>



SOPHOS



NEWSREVIEWSIN DEPTHEVENTSRESOURCE LIBRARYSC SECURITY OPS CENTERSC UK

THE CYBERSECURITY SOURCE SINCE 1989

SC Media > Home > Security News > APTs/cyberespionage > Hackers hijacked cloud accounts of high-tech and aviation firms, hid in systems for years

January 21, 2021

Hackers hijacked cloud accounts of high-tech and aviation firms, hid in systems for years



Bradley Barth
Follow @bbb1216bbb

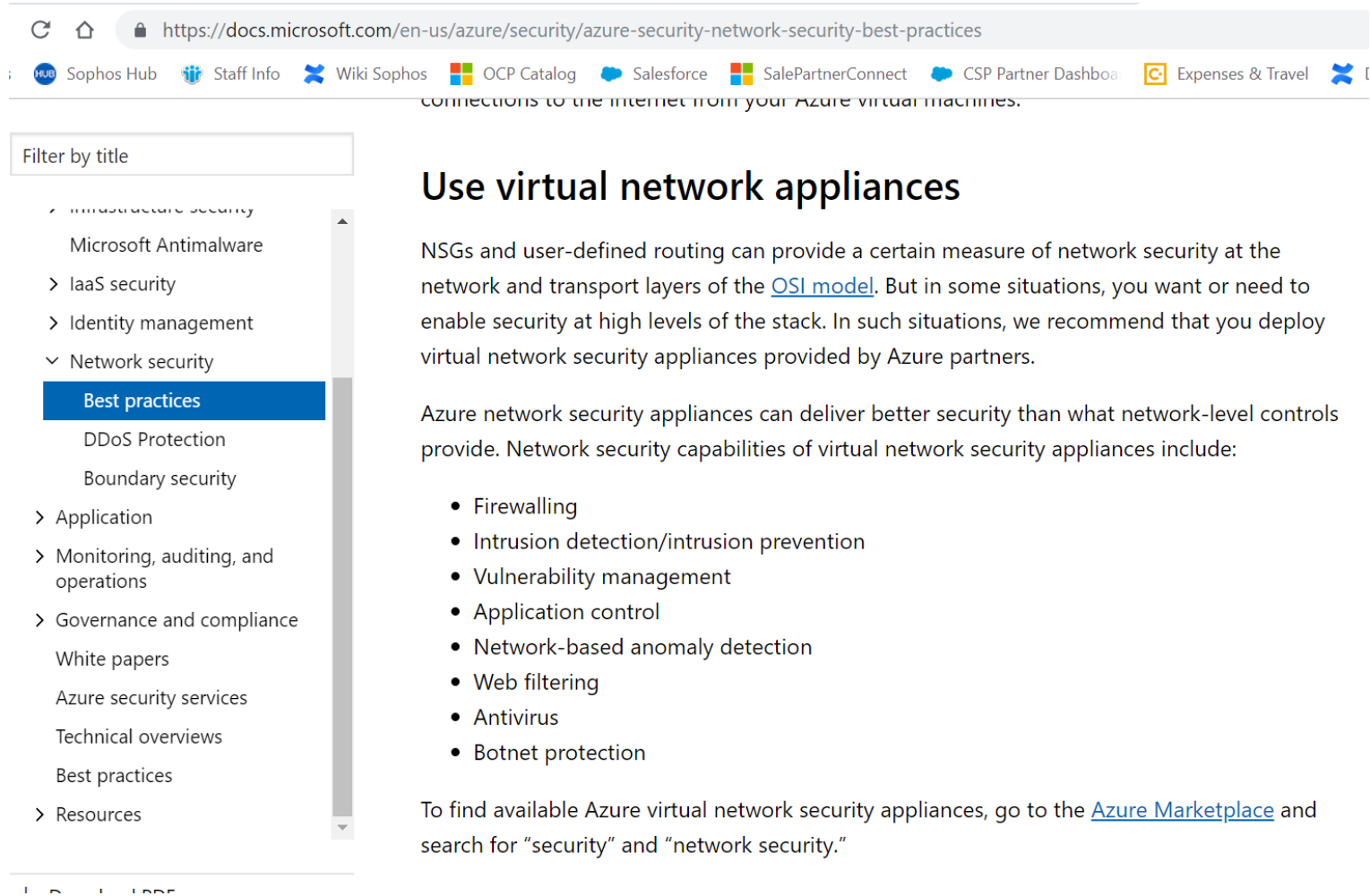


Entries now open for 2021 SC Awards, celebrating cybersecurity's best and brightest

Cybersecurity Collaborative introduces \$1M grant program for new members

Modèle de sécurité partagé

Security Best Practices



The screenshot shows a web browser window with the URL <https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices>. The browser's address bar and tabs are visible at the top. Below the browser window, a sidebar on the left contains a navigation menu with the following items: Infrastructure security, Microsoft Antimalware, IaaS security, Identity management, Network security (expanded), Best practices (highlighted in blue), DDoS Protection, Boundary security, Application, Monitoring, auditing, and operations, Governance and compliance, White papers, Azure security services, Technical overviews, Best practices, and Resources. The main content area on the right features the heading "Use virtual network appliances" in a large, bold font. Below this heading, a paragraph explains that NSGs and user-defined routing provide network security at the network and transport layers of the OSI model, but in some situations, virtual network security appliances provided by Azure partners are recommended. A second paragraph states that these appliances can deliver better security than network-level controls and lists their capabilities: Firewalling, Intrusion detection/intrusion prevention, Vulnerability management, Application control, Network-based anomaly detection, Web filtering, Antivirus, and Botnet protection. The final paragraph advises users to find available Azure virtual network security appliances by going to the Azure Marketplace and searching for "security" and "network security."

connections to the internet from your Azure virtual machines.

Use virtual network appliances

NSGs and user-defined routing can provide a certain measure of network security at the network and transport layers of the [OSI model](#). But in some situations, you want or need to enable security at high levels of the stack. In such situations, we recommend that you deploy virtual network security appliances provided by Azure partners.

Azure network security appliances can deliver better security than what network-level controls provide. Network security capabilities of virtual network security appliances include:

- Firewalling
- Intrusion detection/intrusion prevention
- Vulnerability management
- Application control
- Network-based anomaly detection
- Web filtering
- Antivirus
- Botnet protection

To find available Azure virtual network security appliances, go to the [Azure Marketplace](#) and search for "security" and "network security."

Your Responsibilities

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability				
Client & end-point protection				
Identity & access management				
Application level controls				
Network controls				
Host infrastructure				
Physical security				
	 Cloud Customer	 Cloud Provider		

The **Customer** is responsible for the **security** of **each asset layer**

The **Customer** is responsible for providing **host** security

The **Customer** is responsible for **authenticating user/service access**

The **Customer** is responsible for securing application infrastructure

The **Customer** is responsible for securing and inspecting network traffic

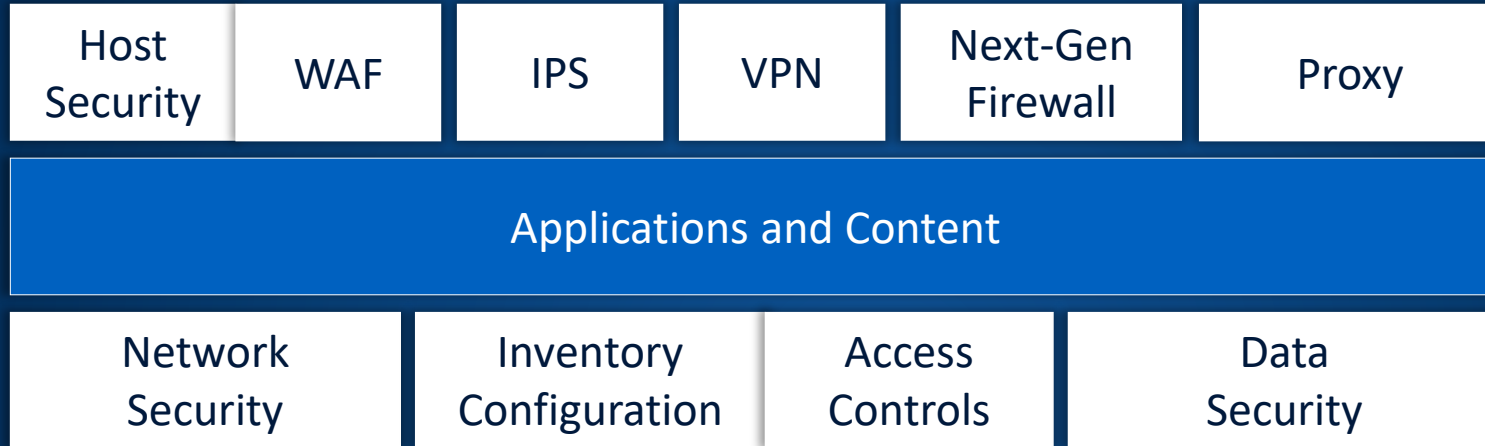
Customer/Microsoft is responsible for the security *'of'* the Cloud

Microsoft is responsible for the Physical Security *'of'* the Cloud

Source: Microsoft TechNet – Shared Responsibilities for Cloud Computing

La sécurité du cloud est une responsabilité partagée

Sécurité
DANS le
Cloud



**Votre
responsabilité**

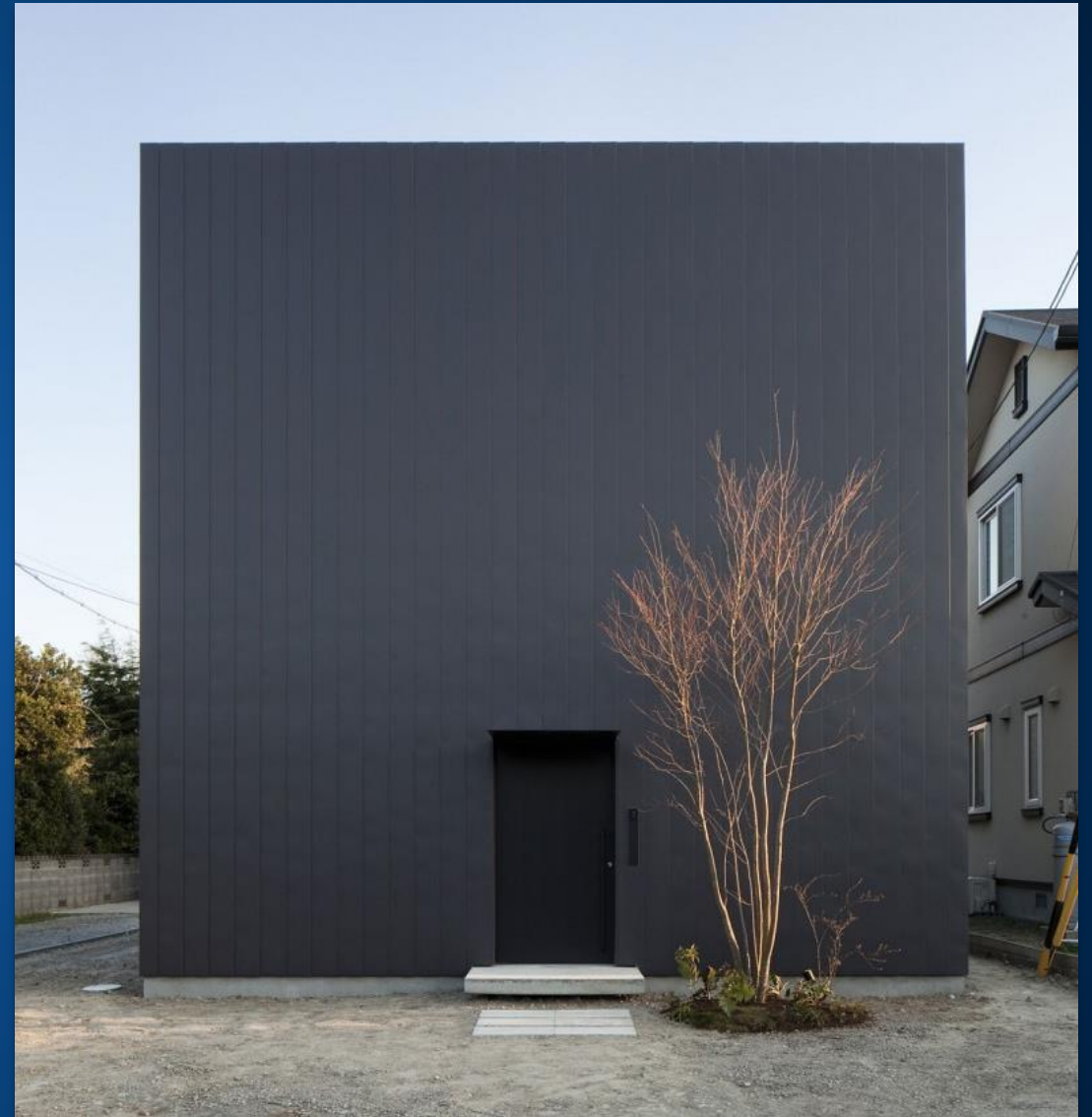
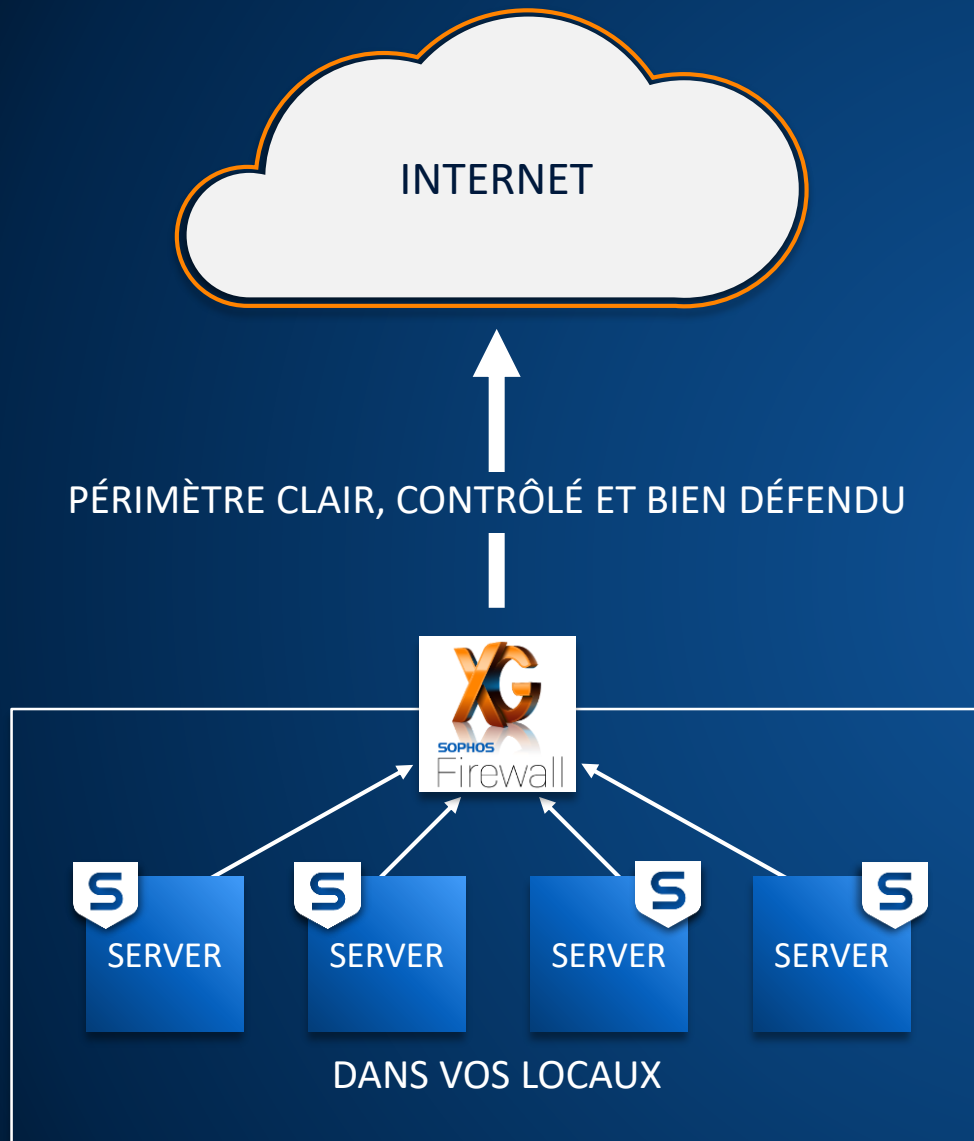
Sécurité
DU Cloud



**Responsabilité
du CSP**
AWS, Azure, Google

Le Cloud c'est pareil... mais différent.

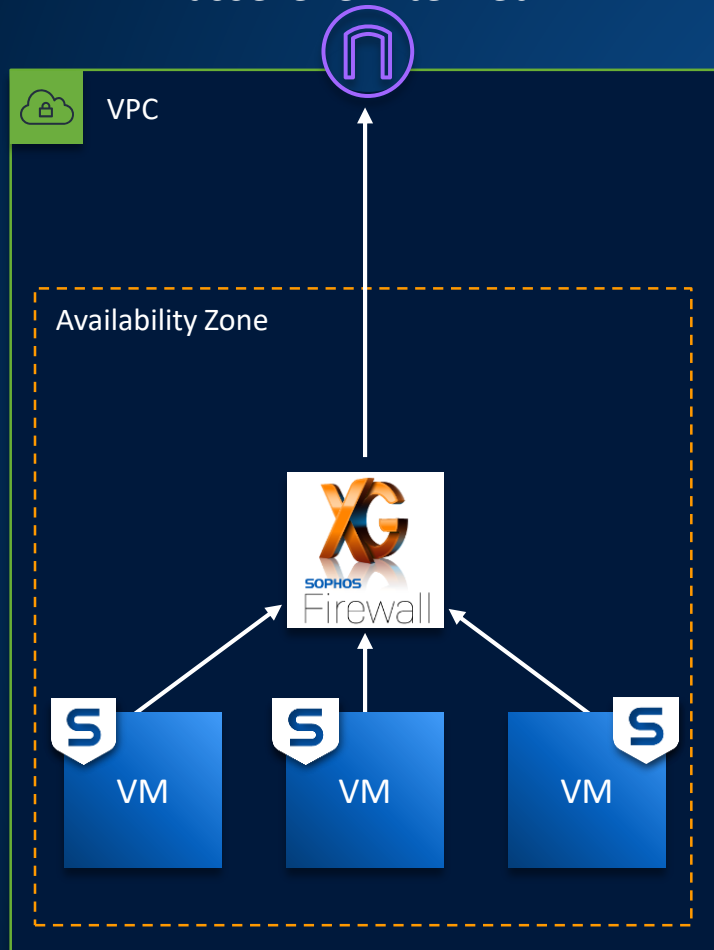
SOPHOS





AWS CLOUD

Passerelle Internet





AWS CLOUD

Passerelle Internet



VPC



Availability Zone



SOPHOS
Firewall



VM



VM



VM



Amazon Simple
Storage Service (S3)



Amazon Elastic
Kubernetes Service



Amazon
Dynamo DB



AWS Lambda

INTERNET

Votre responsabilité

Sécurité DANS le Cloud



– XG Firewall



– Intercept X



– Le client fait les MAJ des OS et des applications



– Sophos Cloud Optix

Une gamme complète de solutions

- *Une offre fonctionnelle modulaire : firewall, protection serveurs*
- *Sophos Central (SaaS) :*
 - *Console d'administration unifiée et ergonomique,*
 - *Alertes corrélées,*
 - *Rapports,*
 - *API RESTful*



INTERCEPT X avec EDR



XG FIREWALL

Protection et gestion de la position de sécurité



Découverte d'actifs et analyse



Sécurité des accès



Détection des menaces et réponses assistées



Optimisation des coûts



Scan de conformité et de sécurité



Intégration du CI/CD



Google Cloud



Un service d'analyse à la demande pour sécuriser vos applications

- *Intelix sur le MarketPlace d'AWS.*



Challenges

SOPHOS

Principales préoccupations des Professionnels de l'informatique quant au déploiement en mode CLOUD.

Menaces

Identifier et répondre aux incidents de sécurité est un sujet critique.

41%

Des entreprises interrogées.

Coûts

Identifier les variations de coûts d'exploitation des environnements CLOUD est un sujet important.

26%

Des entreprises interrogées

Conformité

Rester conforme aux règles et normes est un sujet d'inquiétude.

27%

Des entreprises interrogées

Evolution de la surveillance / monitoring



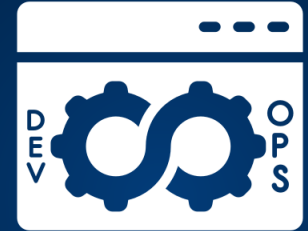
Expérience
Utilisateur (UX)



Ressources à courte
durée de vie



Davantage de
périphériques
davantage de données



Vélocité
Cycle de publication
plus rapide

Évolution de la Sécurité Synchronisée du CLOUD.

Notre volonté est de fournir la meilleure protection et visibilité sur l'ensemble de vos données.



Restons en contact

Écrivez-nous



Livre blanc



SOPHOS