Cybersécurité : les nouveaux enjeux

Marc GUEROULT
Security Partner Account Manager
mgueroul@cisco.com

L’ère de la transformation numérique…

Induit une ère de nouveaux challenges de sécurité

50 milliards d’objets connectés d’ici 2020

Surface d’attaque exponentielle

Infrastructure critique & applications cloud

Manque de contrôle

Utilisateurs mobiles partout tout le temps

Manque de visibilité

Complexité & nombre d’attaques

Probabilité de subir une attaque

D’ici 2022…

89%

des PME seront confrontées a une attaque avancée

76%

des grandes entreprises seront confrontées à une attaque avancée

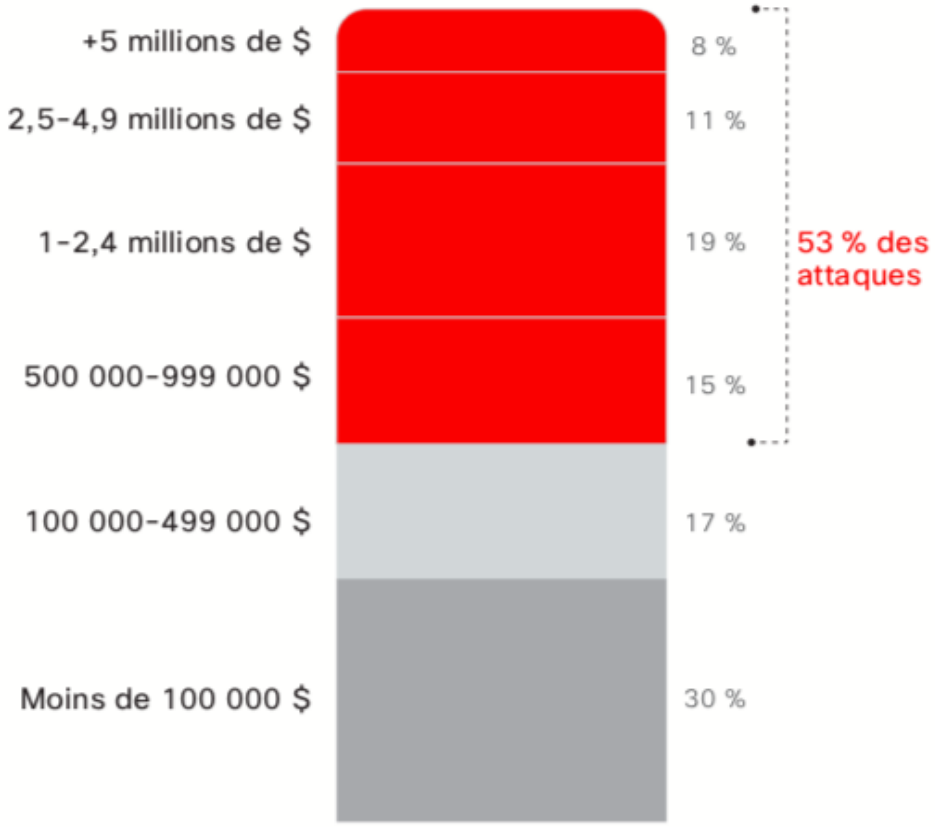
**** Source: Gartner, 2018***

Le coût des attaques

La crainte des failles de sécurité repose sur le coût financier des attaques, qui n'est plus hypothétique. Les failles de sécurité ont des conséquences économiques désastreuses pour les entreprises, dont elles peuvent mettre des mois voire des années à se remettre.

Selon les participants à l'étude, plus de la moitié soit 53 % de toutes les attaques ont entraîné des pertes financières de plus de 500 000 dollars (pertes de chiffre d'affaires, de clients et d'opportunités commerciales ou coûts directs)

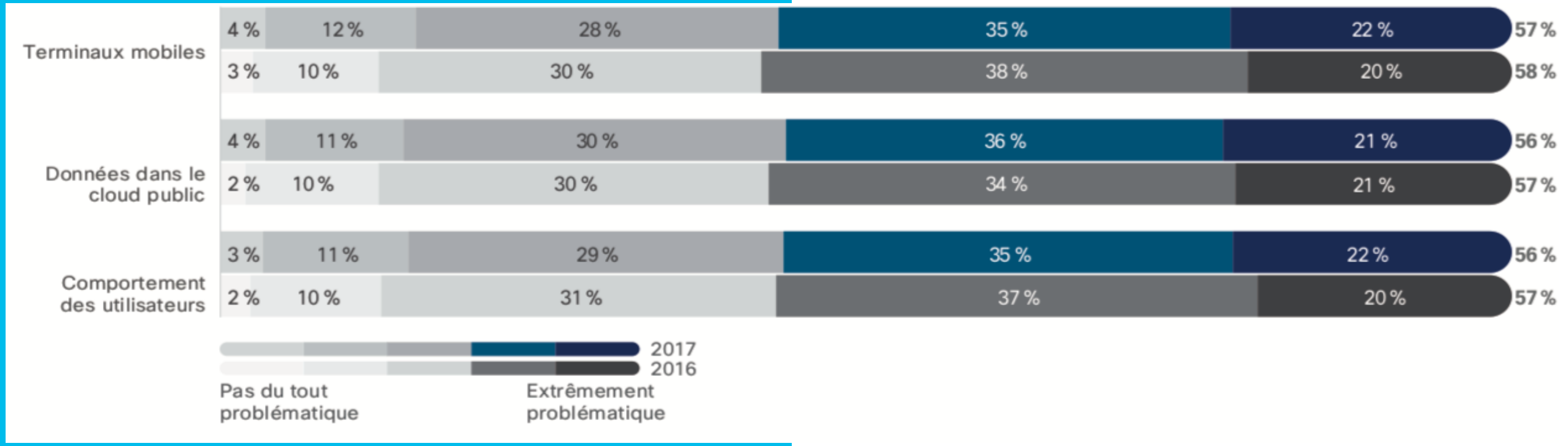
Figure 40 53 % des attaques causent au moins 500 000 $ de dégâts



Défis et enjeux

Dans leurs efforts pour protéger leurs entreprises, les équipes de sécurité font face à de nombreux obstacles.

Les **appareils mobiles**, les données dans le **cloud public** et le **comportement des utilisateurs** présentent les plus grands risques et sont les plus difficiles à protéger.

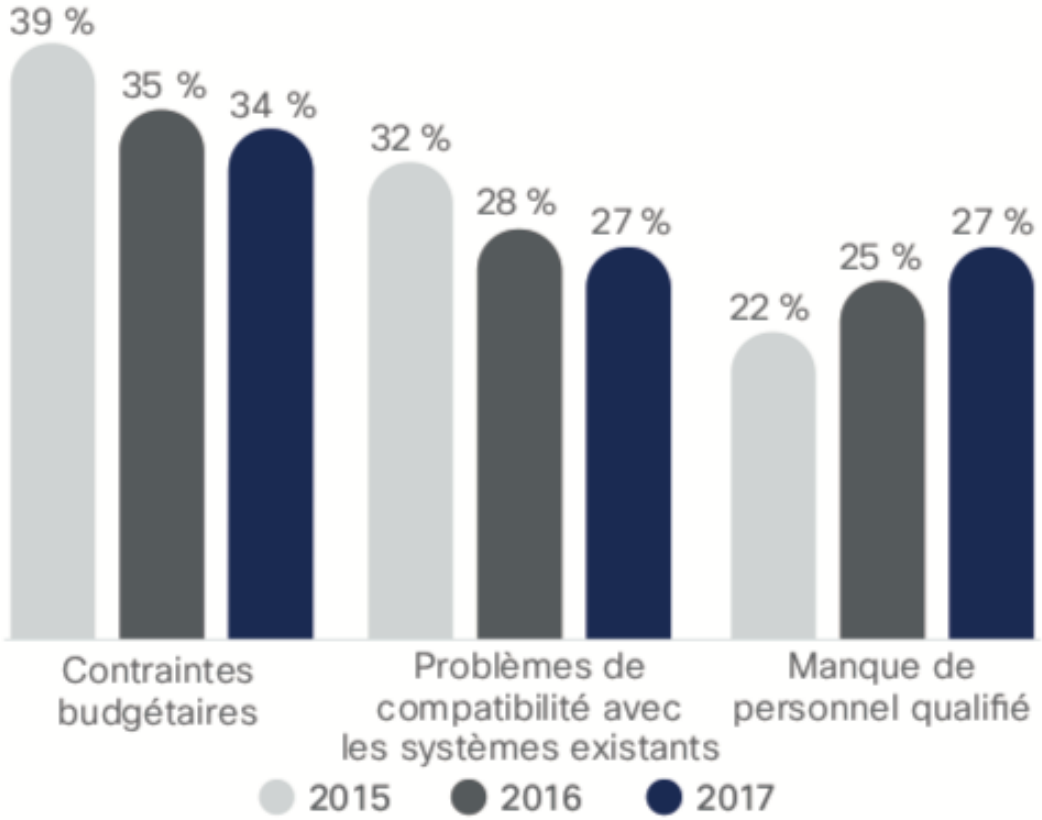


Les plus grands obstacles à la sécurité

Les responsables sécurité citent le budget, l'interopérabilité et le personnel comme principales contraintes pour gérer la sécurité.

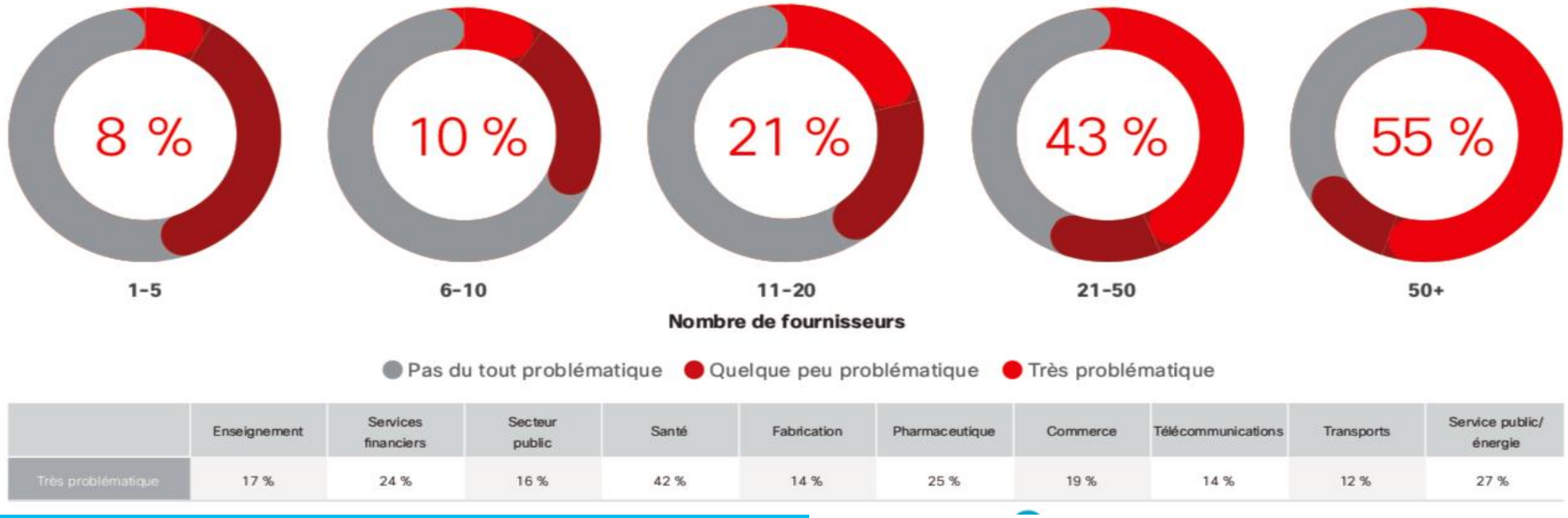
Le manque de personnel qualifié est également cité comme un obstacle à l'adoption de processus et de technologies de sécurité avancés.

En 2017, 27% des personnes interrogées ont indiqué que le manque de personnel qualifié était un obstacle, comparé à 25% en 2016 et 22% en 2015.



Complexité et orchestration

Plus il y a de fournisseurs de solutions de sécurité, plus l'orchestration des alertes est complexe



	Enseignement	Services financiers	Secteur public	Santé	Fabrication	Pharmaceutique	Commerce	Télécommunications	Transports	Service public/ énergie
Très problématique	17 %	24 %	16 %	42 %	14 %	25 %	19 %	14 %	12 %	27 %

De nombreuses alertes non traitées

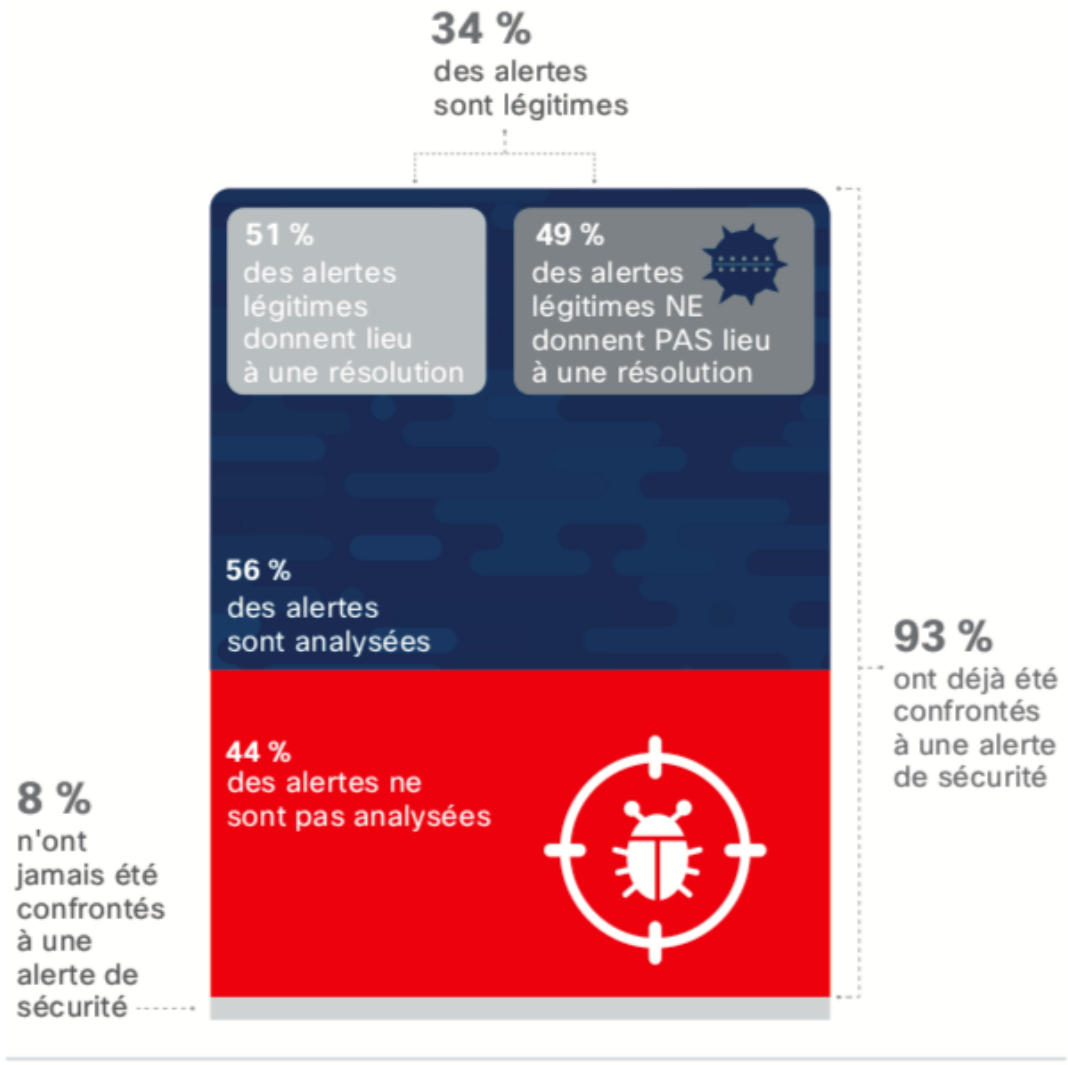
Dans les entreprises qui reçoivent des alertes de sécurité quotidiennes, une moyenne de 44 % de ces alertes ne sont pas analysées.

Parmi ces alertes analysées 34 % sont considérées comme légitimes.

Parmi ces alertes légitimes, 51 % donnent lieu à une résolution.

Près de la moitié (49 %) des alertes légitimes ne donnent pas lieu à une résolution.

Par conséquent, de nombreuses alertes ne sont pas traitées.



Un impact : la méfiance du public

Bien que les entreprises tentent de relever les défis de la sécurité de demain avec une préparation adéquate, les responsables sécurité s'attendent à ce qu'elles soient victimes d'une faille qui entraînera la méfiance du public à leur égard.

55 % des personnes interrogées ont indiqué que leur entreprise a du faire face à la méfiance du public suite à une faille

Les tendances façonnant la sécurité

Tendance n°1

Le périmètre de l’identité

Les attaques ciblent les employés indépendamment de leur position, au sein ou en dehors du réseau

Tendance n° 2

Le périmètre Cloud

Les utilisateurs nomades accèdent directement aux applications dans des environnements multi-cloud

Tendance n° 3

La pénurie de ressources

Les PME doivent faire face a un manque d’experts

Les points stratégiques

Réseau

Cloud

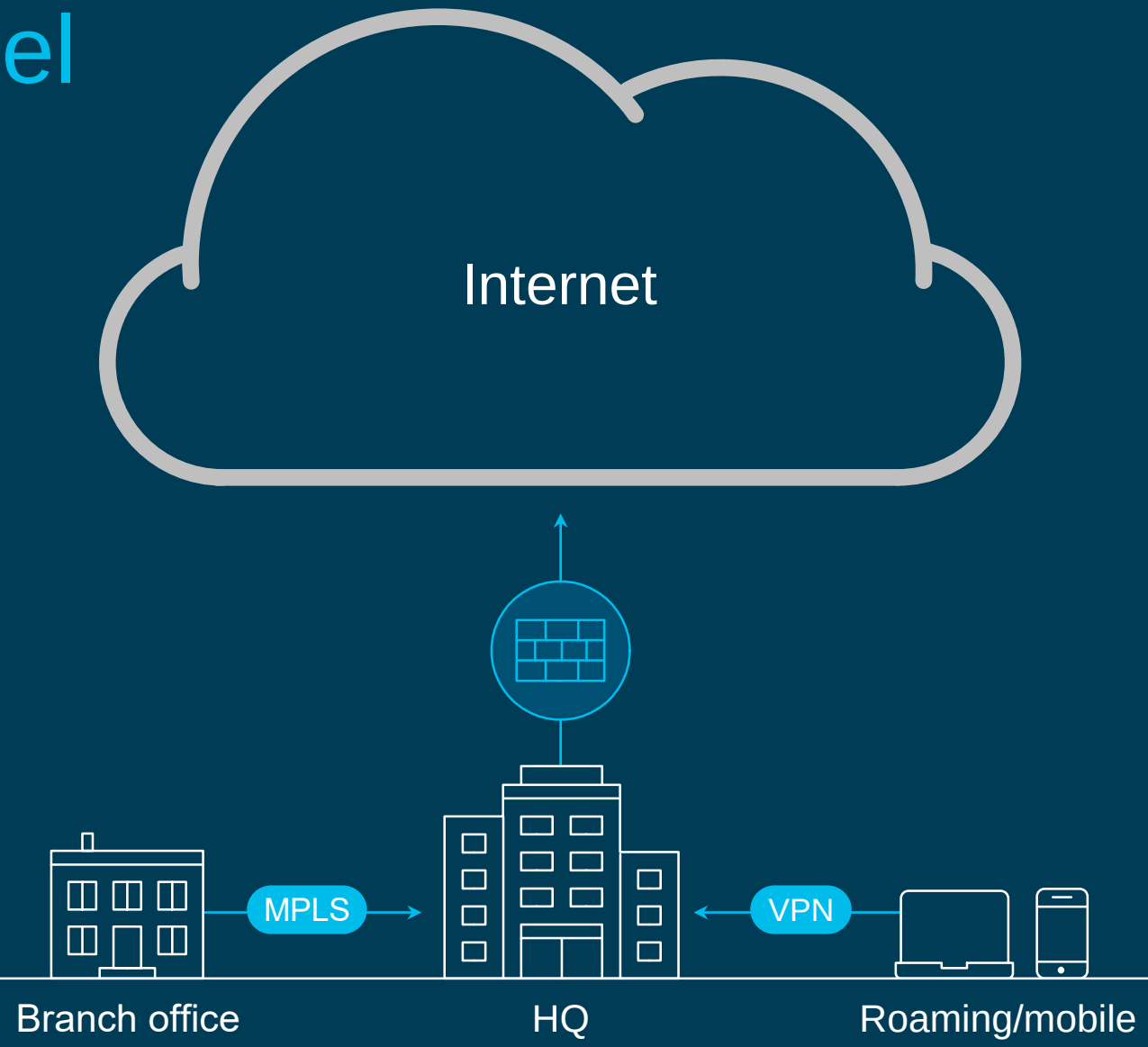
Endpoint

Cloud

Le modèle traditionnel

Réseau:
Centralisé

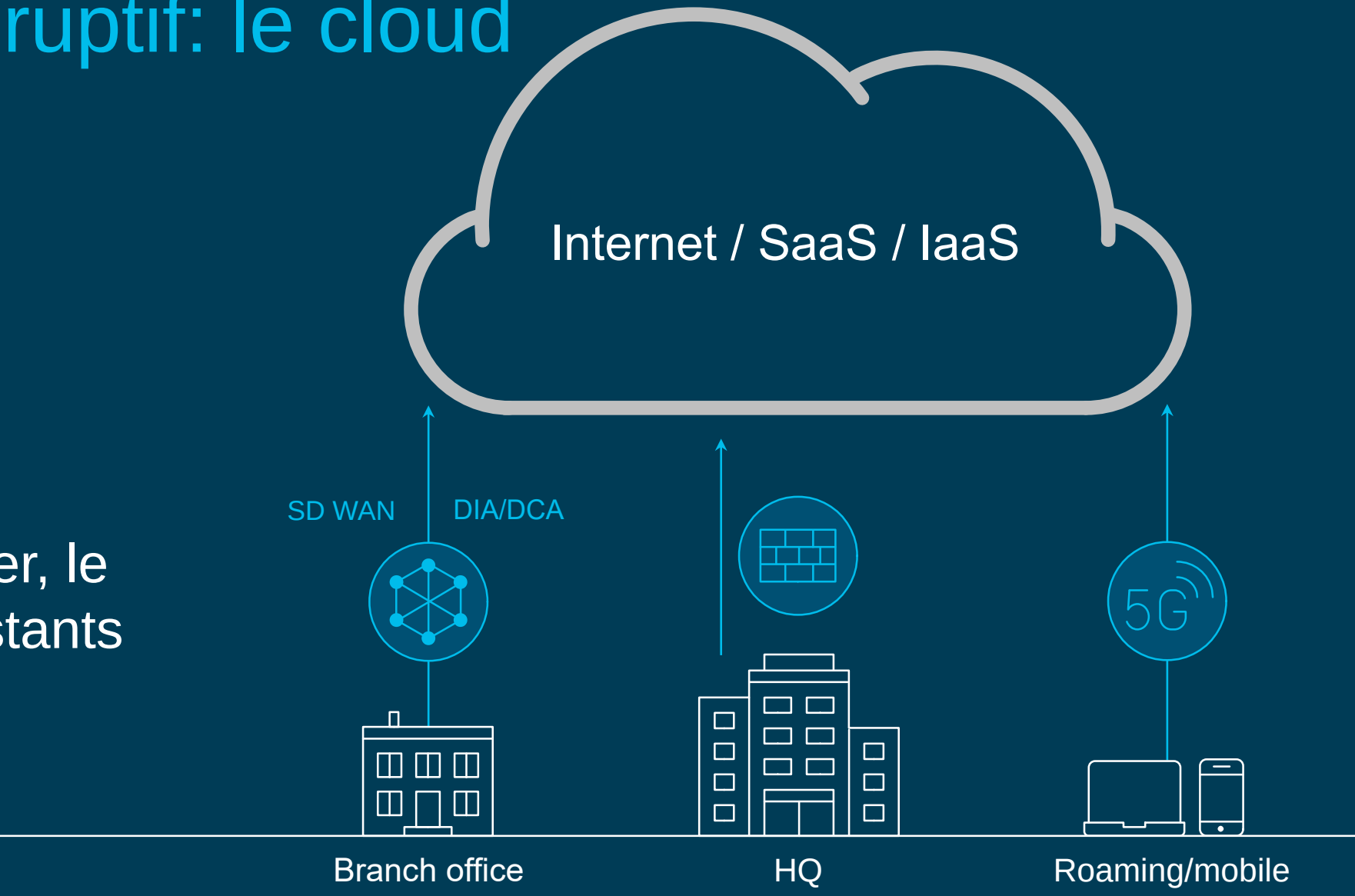
Sécurité:
Point unique de protection et d'application de la politique

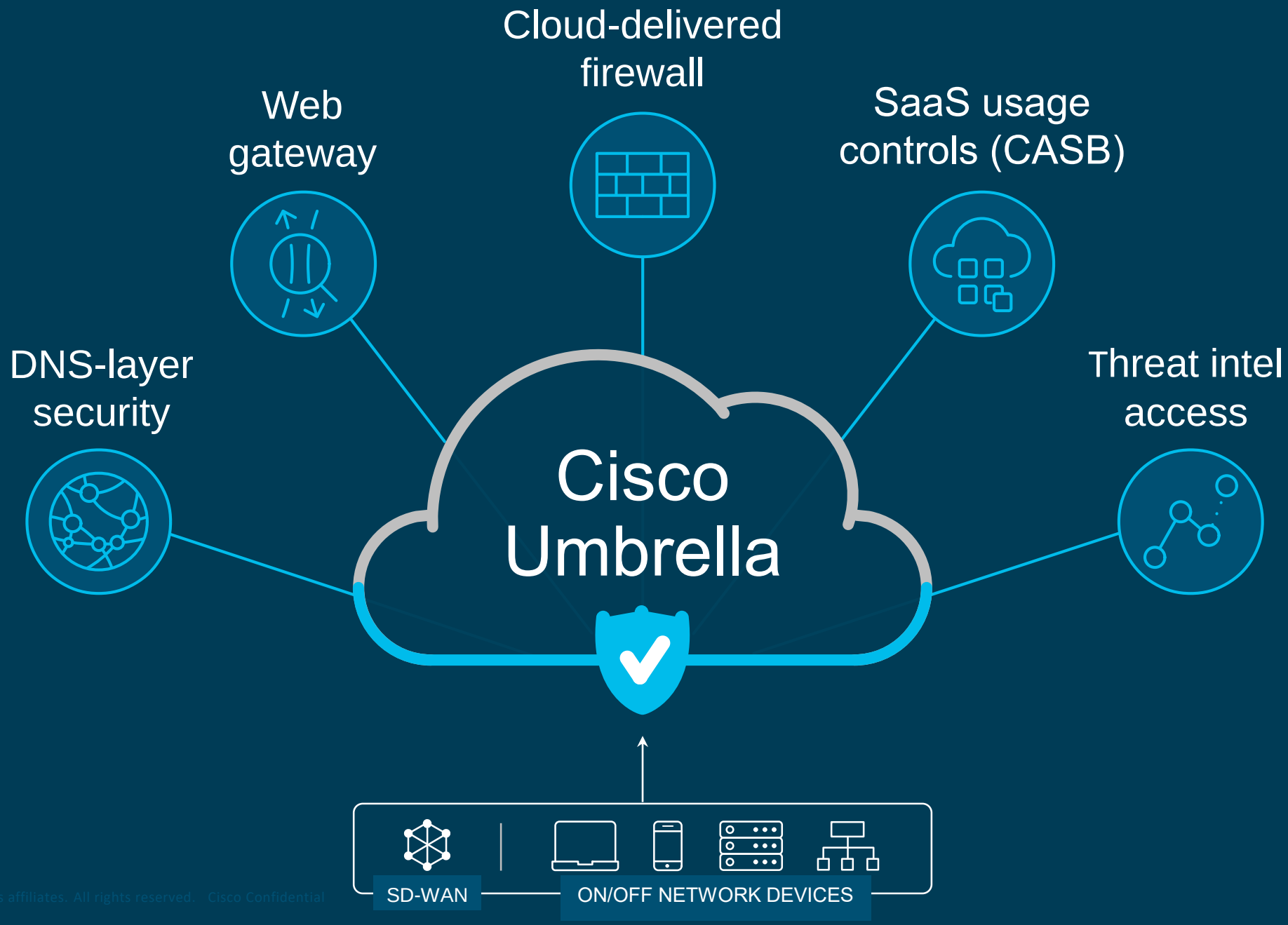


Le modèle disruptif: le cloud

Réseau:
Décentralisé

Sécurité:
Protège le data center, le cloud, et les sites distants





Email Security & Cloudlock protègent Office 365

Cisco Cloud Email Security avec AMP

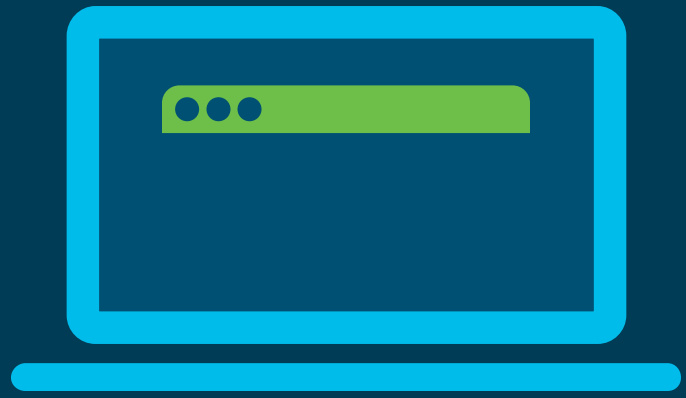
Office 365

Cisco Cloudlock

- Avoir une visibilité sur les attaques Internet et les bloquer – Réputation, AS, AV, AMP, Réputation Web, URL Sandboxing
- Sécurité rétrospective
- DLP
- Chiffrement des données en transit

- Identifier les comptes compromis
- Détecter les extractions malicieuses d'informations provenant de l'interne
- Voir ce que les utilisateurs uploadent et partagent

Endpoint



Protégez vos terminaux

Cisco Any Connet - Accès simple et sécurisé

Donnez les moyens à vos collaborateurs de travailler à tout moment aussi bien sur les ordinateurs portables que vous mettez à leur disposition que sur leurs terminaux mobiles personnels, et ce, où qu'ils se trouvent. Bénéficiez d'une visibilité sur vos terminaux à l'échelle de l'entreprise.
Protégez vos collaborateurs sur le réseau et en dehors. Mettez en œuvre des politiques de gestion de l'état des terminaux connectés.

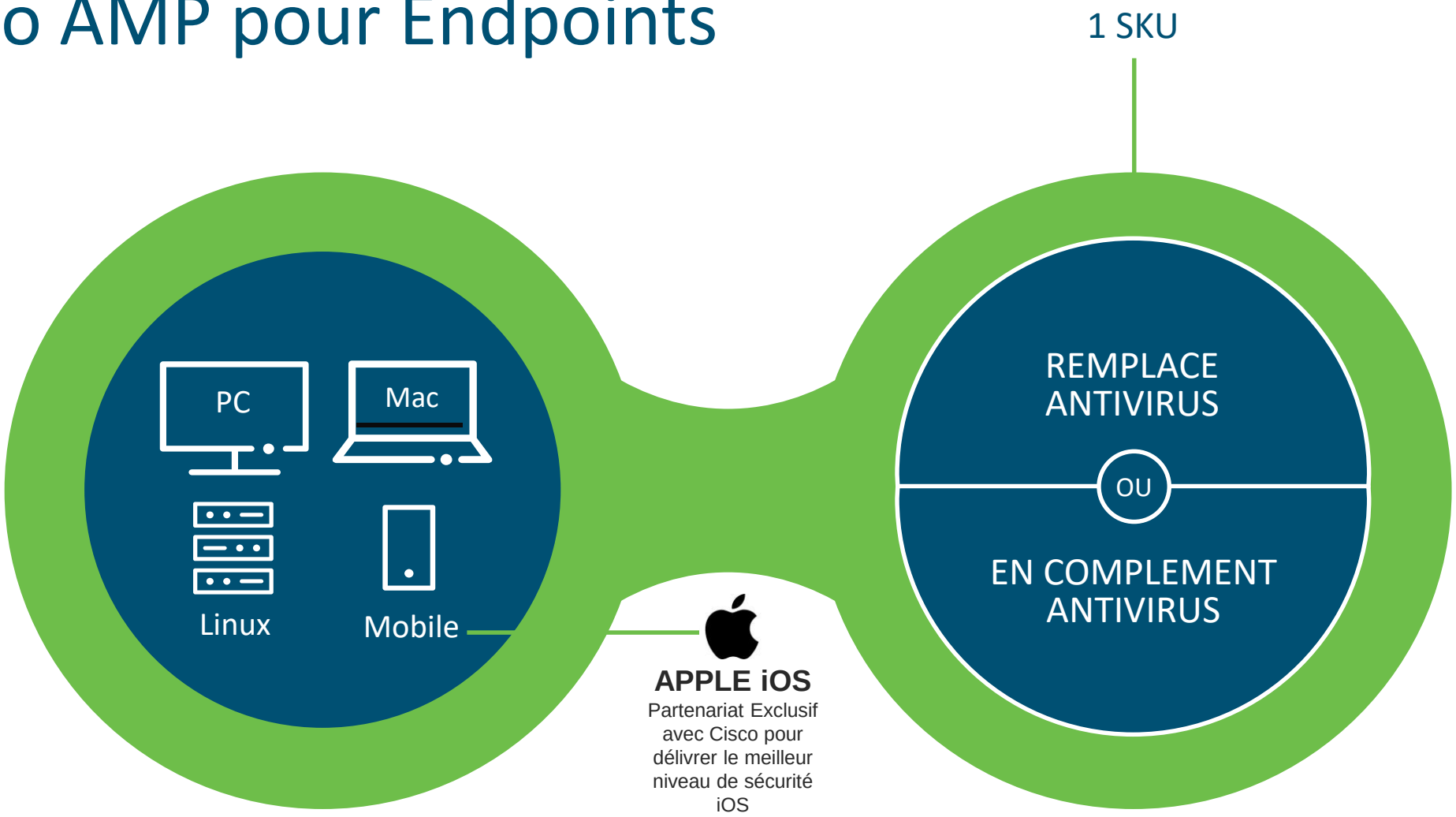
AMP pour Endpoints - Visibilité, données contextuelles et contrôle

Prévenez les failles de sécurité. Surveillez en continu le comportement de tous vos fichiers afin de repérer les attaques furtives. Détectez, bloquez et éliminez les malwares avancés sur tous vos terminaux, rapidement et automatiquement.

UMBRELLA - Sécurité en dehors du réseau privé virtuel (VPN)

Protégez vos collaborateurs même lorsqu'ils ne sont pas connectés au VPN. Il vous suffit d'activer la fonctionnalité Umbrella dans le client Cisco AnyConnect. Vous pouvez mettre en place, facilement, une protection contre les programmes malveillants, le phishing et les instructions de type contrôle-commande (C&C), où que se trouvent vos utilisateurs.

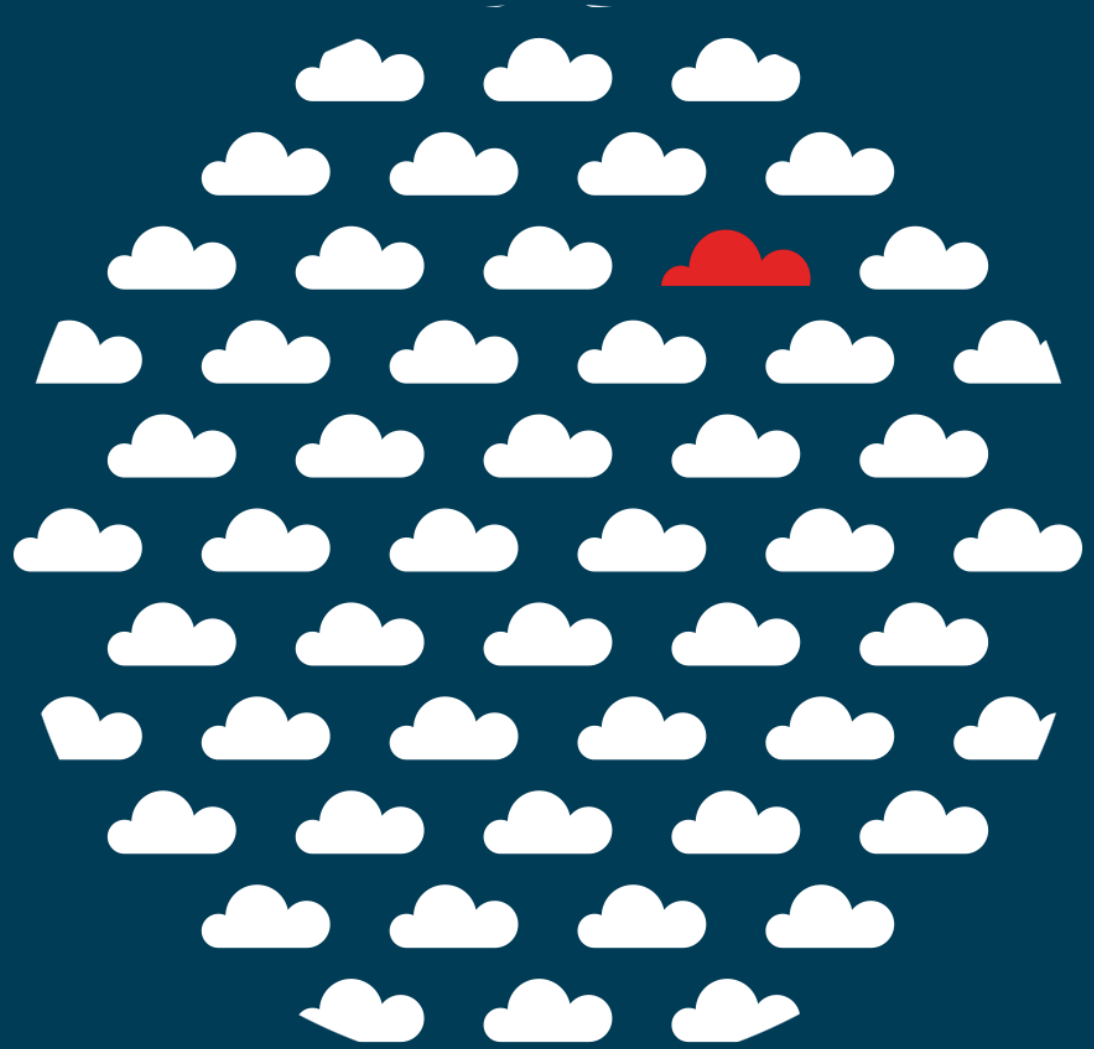
Cisco AMP pour Endpoints



Cisco Security Vision et Strategie

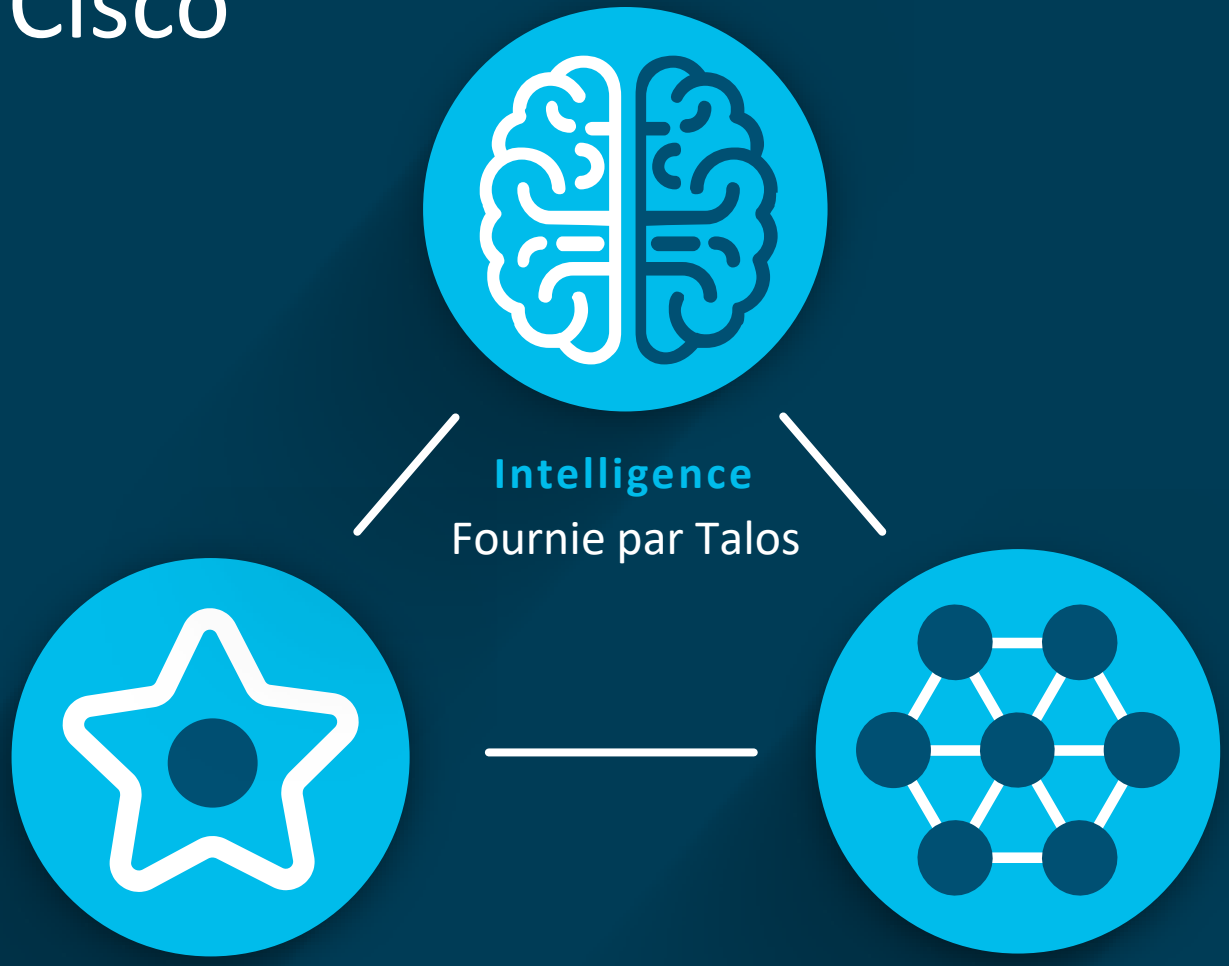
Marc Guéroult
Cyber Security Partner Account Manager

mgueroul@cisco.com



Security above everything.

La stratégie Cisco



Intelligence

Fournie par Talos

Cloud, Firewall, Email, Endpoint

Produits Best of Breed

Automatisation & Visibilité

Architecture intégrée

TALOS

Web/URL

Network Analysis

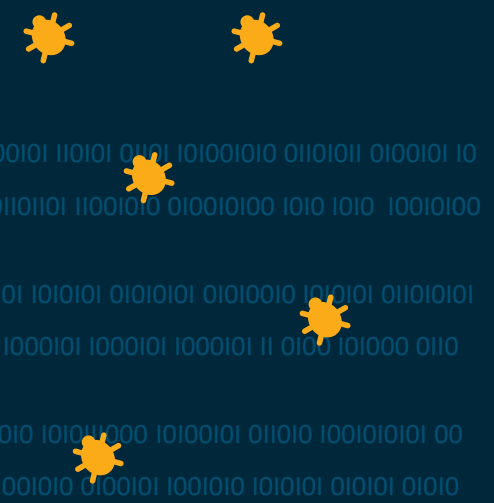
Email

Malware/Endpoint

DNS/IP

Network Intrusions

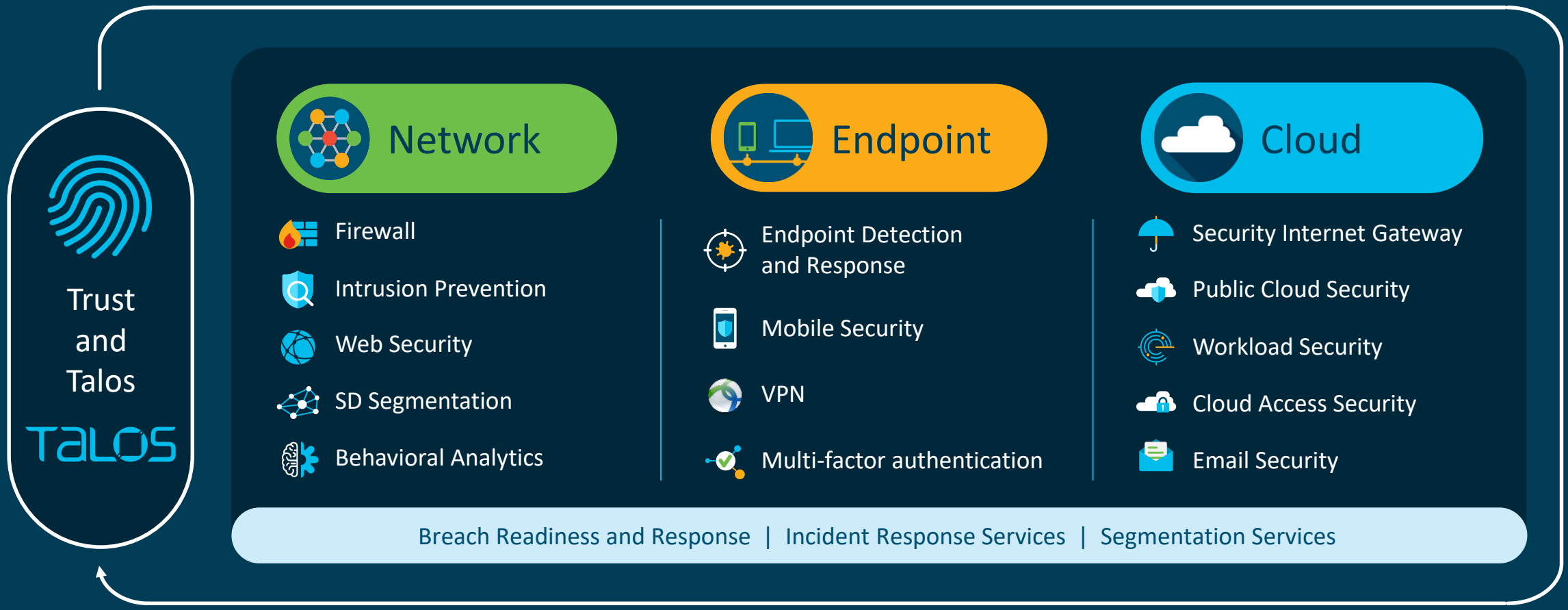
- 100 TB de data / jour
- 1.6 millions de sensors
- Plus de150 millions de endpoints déployés
- 300 chercheurs dédiés sur l'évolution des menaces
- 35% du traffic mail mondial
- IntelligenceAMP Threat Grid
- Analyse dynamique AMP Threat Grid : 10 millions de fichiers par mois



- 16 milliards de requêtes Web
- 24x7x365
- 4.3 milliards de sites web bloqués par jour
- 40+ langues
- 1.5 millions de samples de malware par jour
- Communauté AMP
- Private/public threat feeds
- Communautés Open source Snort et ClamAV
- AEGIS Program

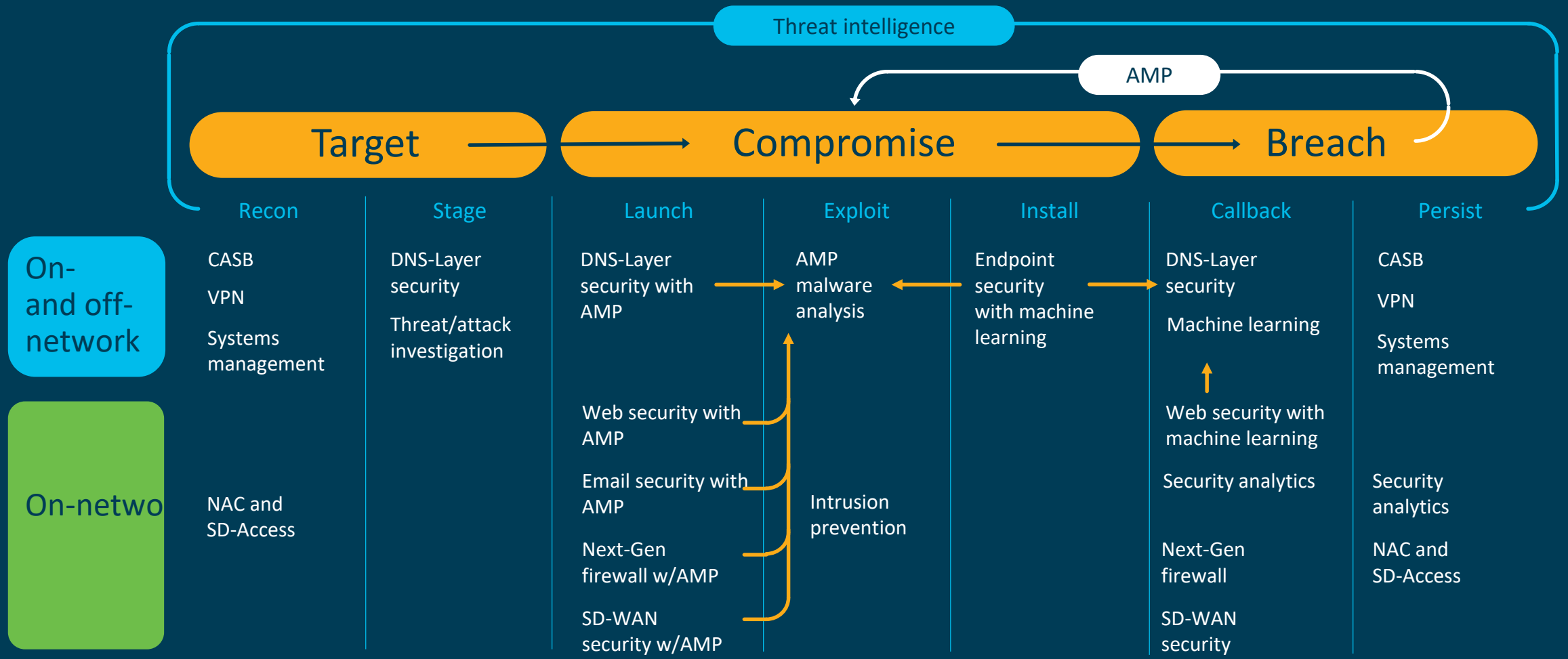
Le portfolio sécurité

Renforcez vos systèmes de défense



*Slide with specific Cisco products in appendix

Une ligne de defense durant la chaîne d'attaque



AMP: Advanced Malware Protection

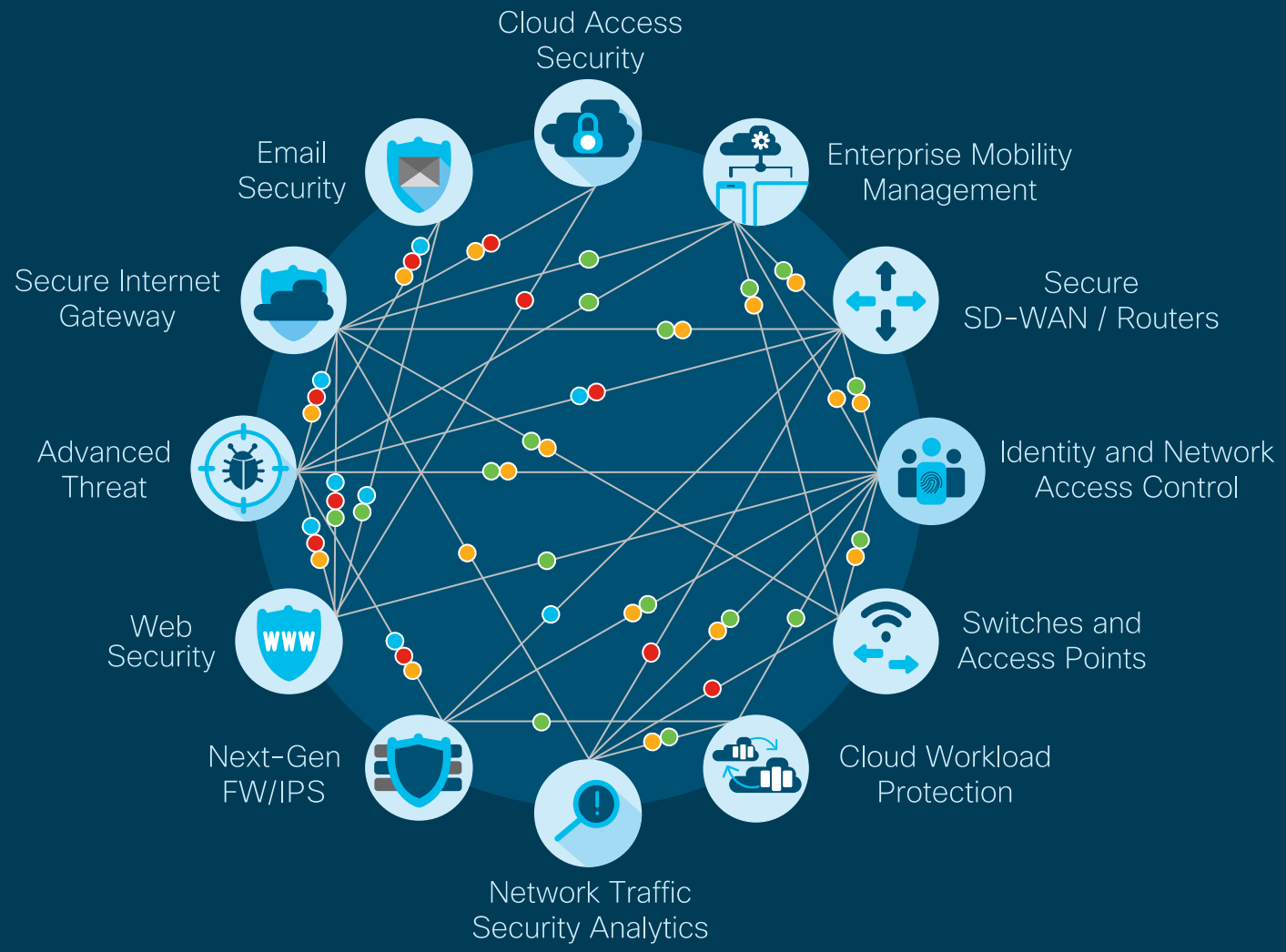
Une architecture intégrée et automatisée

Threat Intelligence
Optimise la prévention d'intrusions

Visibilité des évènements
Réduit le temps de détection

Partage du contexte
Réduit le temps d'investigation

Automatisation des stratégies
Réduit le temps de correction




CISCO