Le télétravail en toute sécurité

Roger Courchesne – ESI
Malaurie Morin Proulx, Cisco

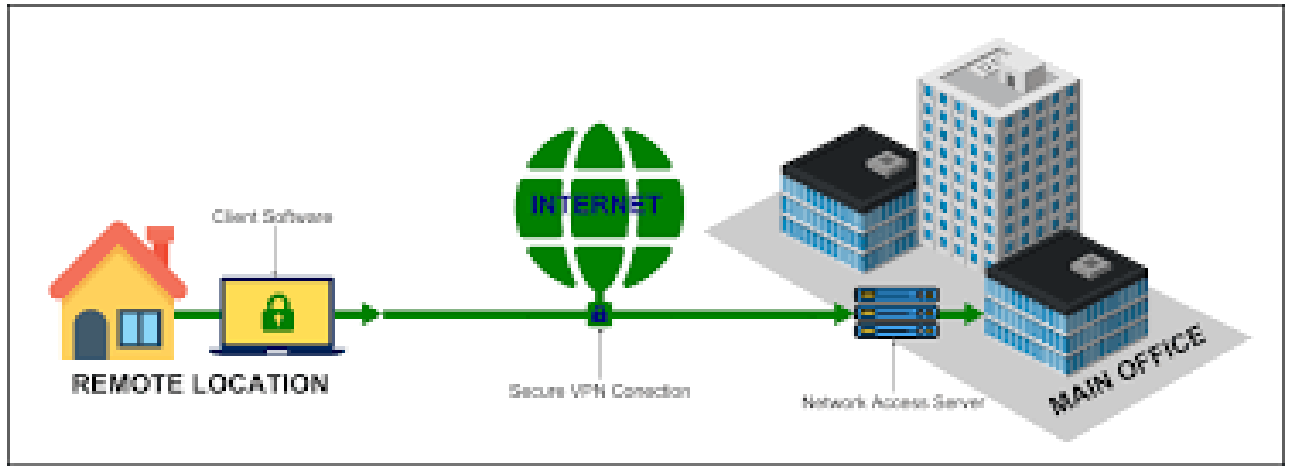
28 octobre 2020

ORDRE DU JOUR

- Définir le télétravail - retour à la base!
- Quels sont les ingrédients d'une bonne solution d'accès à distance sécurisé?
- Quelles sont les applications les plus utilisées?
- Les connectivités de base
- Comment sécuriser les télétravailleurs avec les solutions Cisco

TÉLÉTRAVAIL : UNE DÉFINITION

- Exercer ses fonctions professionnelles à distance du lieu de travail (ex. de la maison, du chalet…)
- Accéder à des outils, des données, des applications et à ses collègues, comme si nous étions au bureau
- Tout ceci rendu possible grâce aux TI, à l'accès Internet haute vitesse et aux mécanismes de sécurité
- Le télétravail exige une discipline. Il est souvent permis puisque l'employé peut exercer ses fonctions sans compromettre sa productivité



TÉLÉTRAVAIL : UNE DÉFINITION

ATTENTION AUX DISTRACTIONS…

ET À LA DISTINCTION ENTRE LE TRAVAIL ET LA MAISON!

LES INGRÉDIENTS D'UNE BONNE SOLUTION D'ACCÈS À DISTANCE

Des employés disciplinés

Une infrastructure TI capable de recevoir le trafic des télétravailleurs

Un appareil conforme au normes de la compagnie (ordinateur et appareils mobiles)

Un accès Internet haute vitesse

Un accès sécurisé

QUELLES SONT LES APPLICATIONS OU RESSOURCES LES PLUS UTILISÉES?

- Les serveurs réseau contenant des fichiers d'entreprise partagés
- L'intranet de l'entreprise
- Les applications « on et off-premises » :
  - Le serveur de messagerie et les répertoires des employés
  - Feuille de temps, CRM, ERP (SAP, JD Edwards)
  - Gestion de projet, logiciel comptable, compte de dépenses, facturation…
- Les outils de collaboration :
  - Webex Meeting, Webex Team, Microsoft Teams
  - Téléphonie IP, la vidéoconférence
  - Applications de centre d'appels…

Connectivité de base

Tunnel Initiator and Terminator

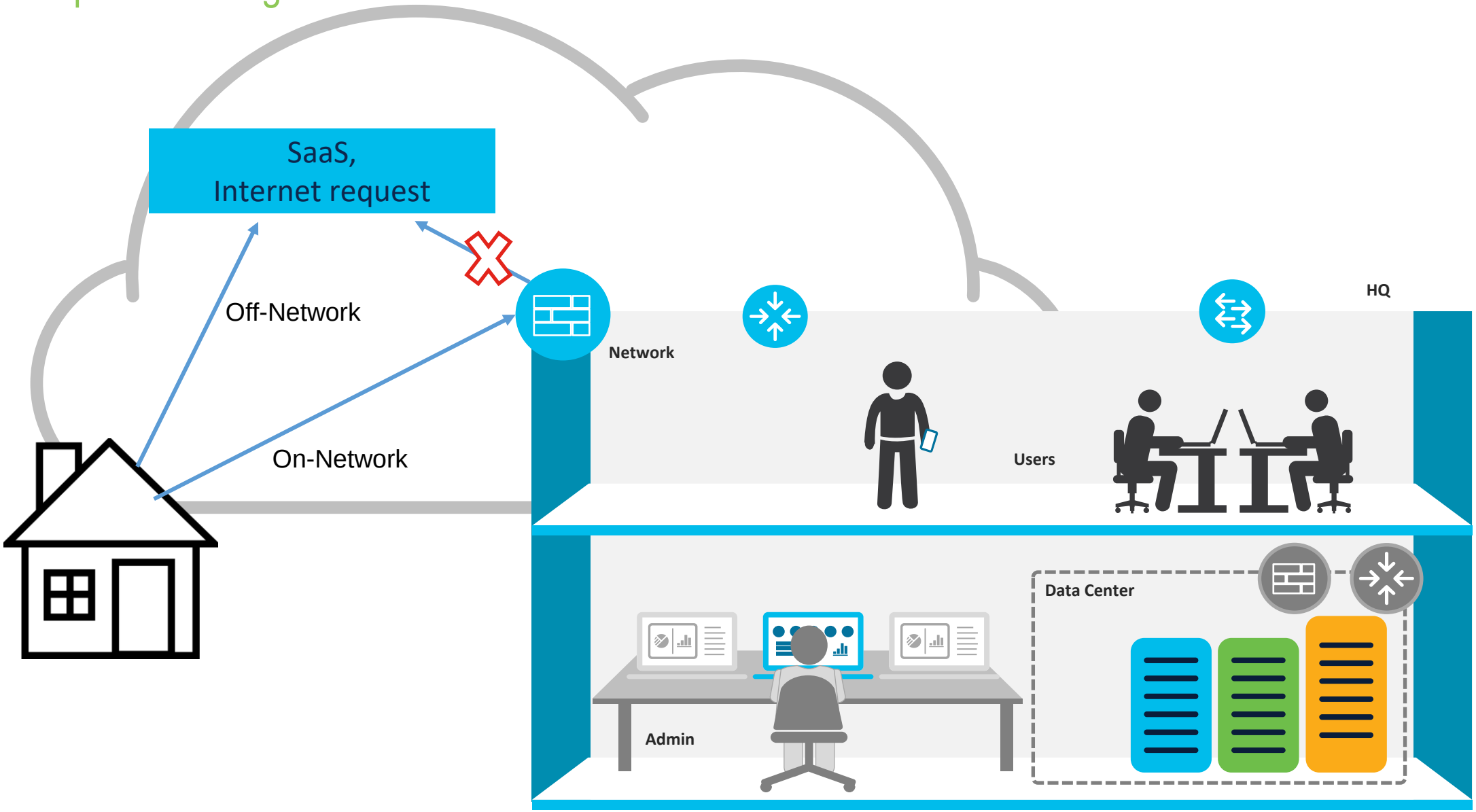
1- Client VPN : AnyConnect

2- Endpoint :

- **Meraki MX**
- **Firepower NGFW**
- **Routeur**

Connectivité de base

Split tunnelling



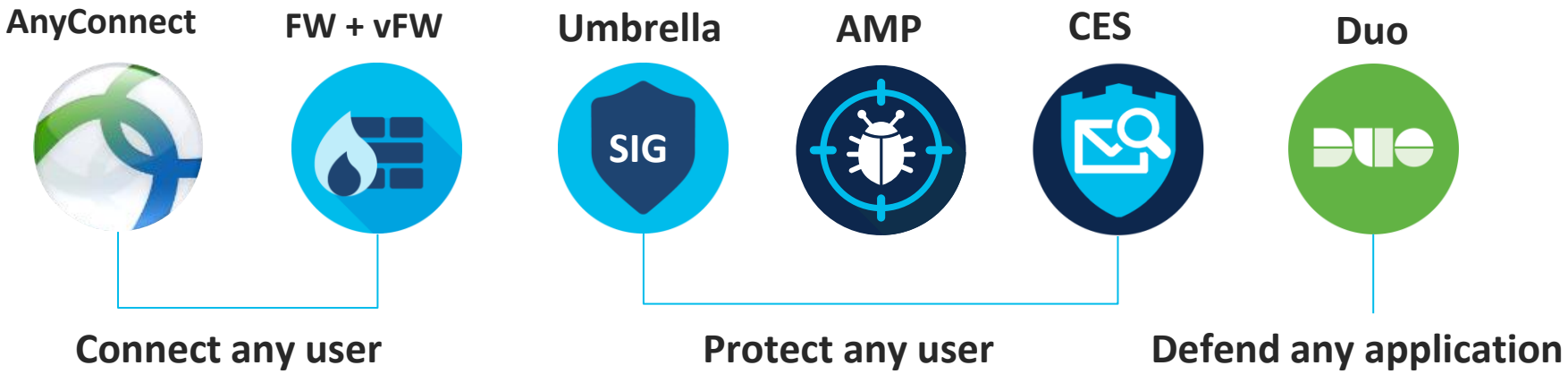
Principales préoccupations des TI avec l'accès à distance

→Lacunes en visibilité et en couverture de sécurité

→Volume et complexité des outils de sécurité

→Budgets et ressources de sécurité limités

Comment sécuriser les télétravailleurs avec les solutions Cisco?



PARE-FEU CISCO

- Appliance
  - Cisco ASA
  - Cisco FirePower (FTD)
  - Meraki MX Series
- Virtuel
  - ASAv et FTDv
  - ESXi et KVM, Azure et AWS
- ESI vous aide à faire le choix, le dimensionnement, l'architecture, l'installation et le soutien

CLIENT VPN CISCO ANYCONNECT

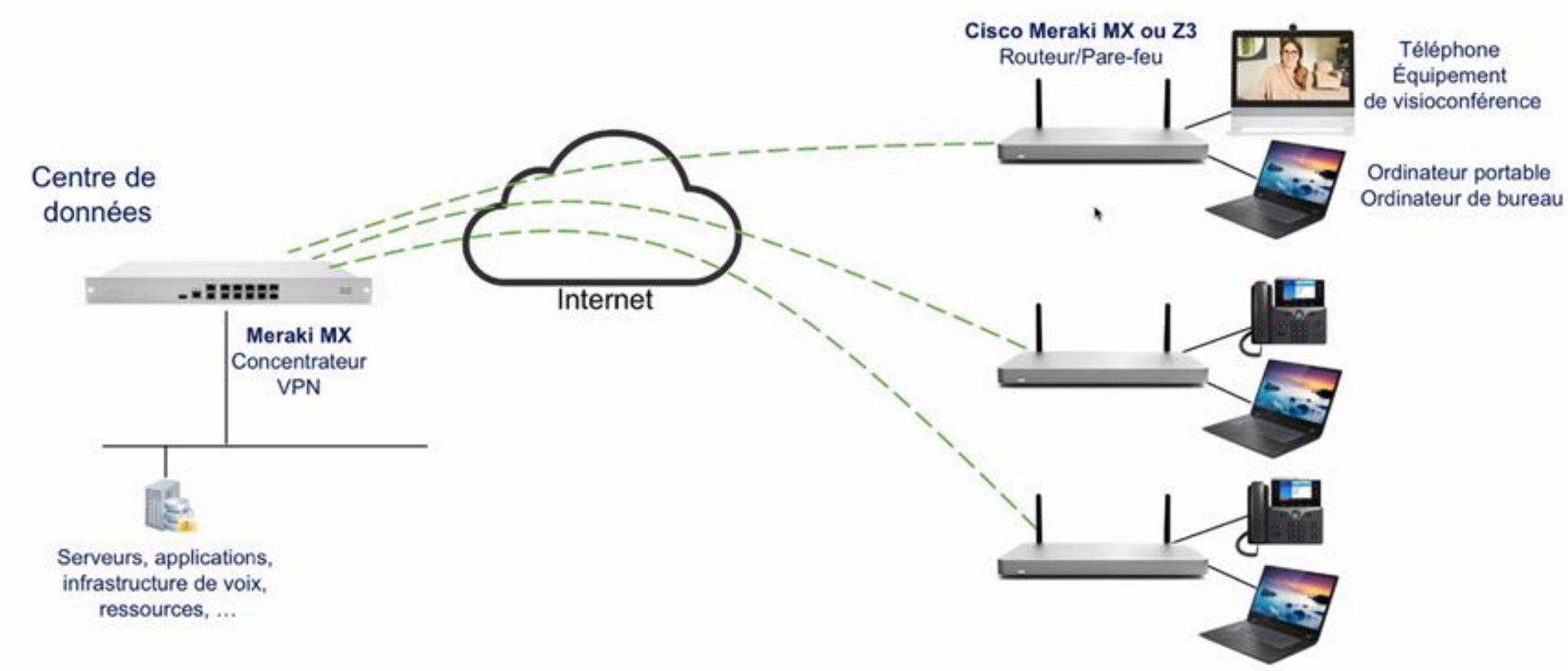
Cisco AnyConnect Secure Mobility

- Abonnement de 1, 3, 5 ans
- 2 saveurs : AnyConnect Plus ou Apex
- PC : Windows, MAC, Linux
- Mobile : IOS, Android

Client VPN Cisco AnyConnect - Fonctionnalités

- Accès à distance VPN IPSec (IPSec Client)
  - Intégration « WSA ou Cloud Web Security »
  - Sécurité web intégrée, défense contre les menaces de logiciels malveillants, protection contre l'hameçonnage, CCcb
- Itinérance avec Cisco Umbrella (sur et hors réseau)
  - Sécurité des dispositifs en itinérance renforcée lorsque le VPN est désactivé
- Assistance avec AMP for Endpoints (AMP Enabler)
  - Protection plus proactive pour garantir qu'une attaque est rapidement atténuée au niveau du endpoint distant
- Module de visibilité du réseau (Apex)
  - Découverte des anomalies de comportement potentielles en surveillant l'utilisation des applications
- Module de conformité et de remédiation (Apex)
  - Validation de la posture : antivirus, pare-feu personnel et antispyware

Gamme de produits Meraki



Cisco Umbrella

- Acquisition de OpenDNS en 2015
- Sécurité flexible
  - « Cloud-Delivered Security » considéré comme un « Cloud Access Security Broker » (CASB with SIG)
- Protection utilisateurs sur et hors réseau
- Licences :
  - Essential
  - Advantage
  - Secure Internet Gateway

DNS Security Essentials	DNS Security Advantage	Secure Internet Gateway (SIG) Essentials
Good for small companies or as first line of defense for any size company	Good for mid-sized companies or as first line of defense for any size company	Ideal for companies with Cisco SD-WAN, and large companies with advanced security and web policy needs

Cisco Umbrelle Package Comparison

Cisco Umbrella – Licence « Essential »

Cisco Umbrella

Protection de la couche DNS

- Bloque les domaines associés à l'hameçonnage, aux logiciels malveillants, aux botnets et à d'autres catégories à haut risque (cryptomining, domaines nouvellement vus, etc.)
- Bloque les requêtes vers des destinations malveillantes et indésirables avant même qu'une connexion ne soit établie
- Arrête les menaces sur n'importe quel port ou protocole avant qu'elles n'atteignent votre réseau ou vos points de terminaison
- Découvre et bloque le « shadow IT » (par domaine) avec le rapport de découverte d'applications

ESI TECHNOLOGIES

Cisco Umbrella – Licence « Advantage »

Cisco Umbrella

- Protection de la couche DNS (et IP)
  - Comprend les fonctionnalités de la licence Essential
  - Bloque le trafic direct vers IP pour CC&CB qui contournent DNS
- Passerelle web sécurisée
  - Proxy sélectif : inspection de l'URL pour le domaine suspect
  - Bloque les URL basées sur Cisco Talos et les fichiers avec AMP
- Umbrella Investigate
  - Permet d'accéder à la console Web d'Investigate, Threat Intelligence interactive
  - Et d'utiliser l'API « Investigate On-Demand »

ESI TECHNOLOGIES

Cisco Umbrella – Licence « Secure Internet Gateway » (SIG)

Cisco Umbrella

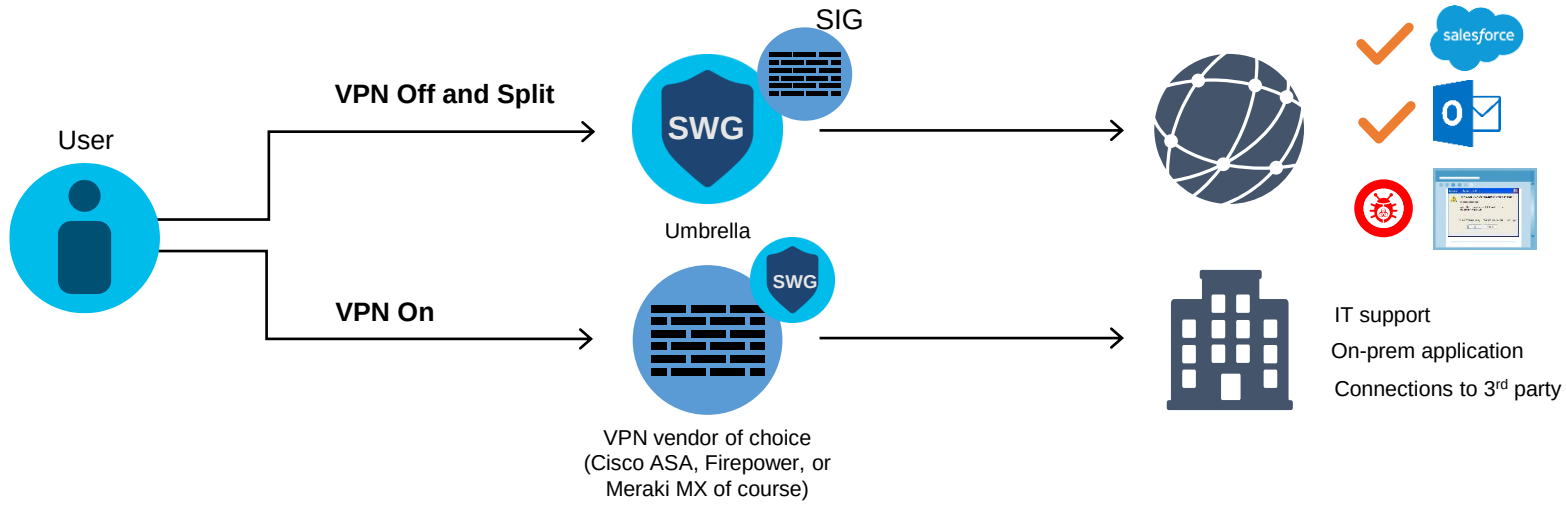
- Visibilité et contrôle de tout le trafic Internet sur tous les ports et protocoles… c'est un proxy complet!
- Sandboxing dans le cloud Cisco Threat Grid pour identifier les comportements malveillants
- Stratégies d'IP, de port, de protocole et d'application personnalisables dans le tableau de bord Umbrella
- Prise en charge du tunnel IPsec pour acheminer en toute sécurité le trafic vers l'infrastructure cloud
- Journaux de rapports automatisés
  - Tout cela soutenu par Cisco Talos, les équipes de renseignement sur les menaces
  - Avec une disponibilité de 100%

Cisco Umbrella

Protection de sécurité flexible sur et hors réseau

Politiques cohérentes sur les sites distants

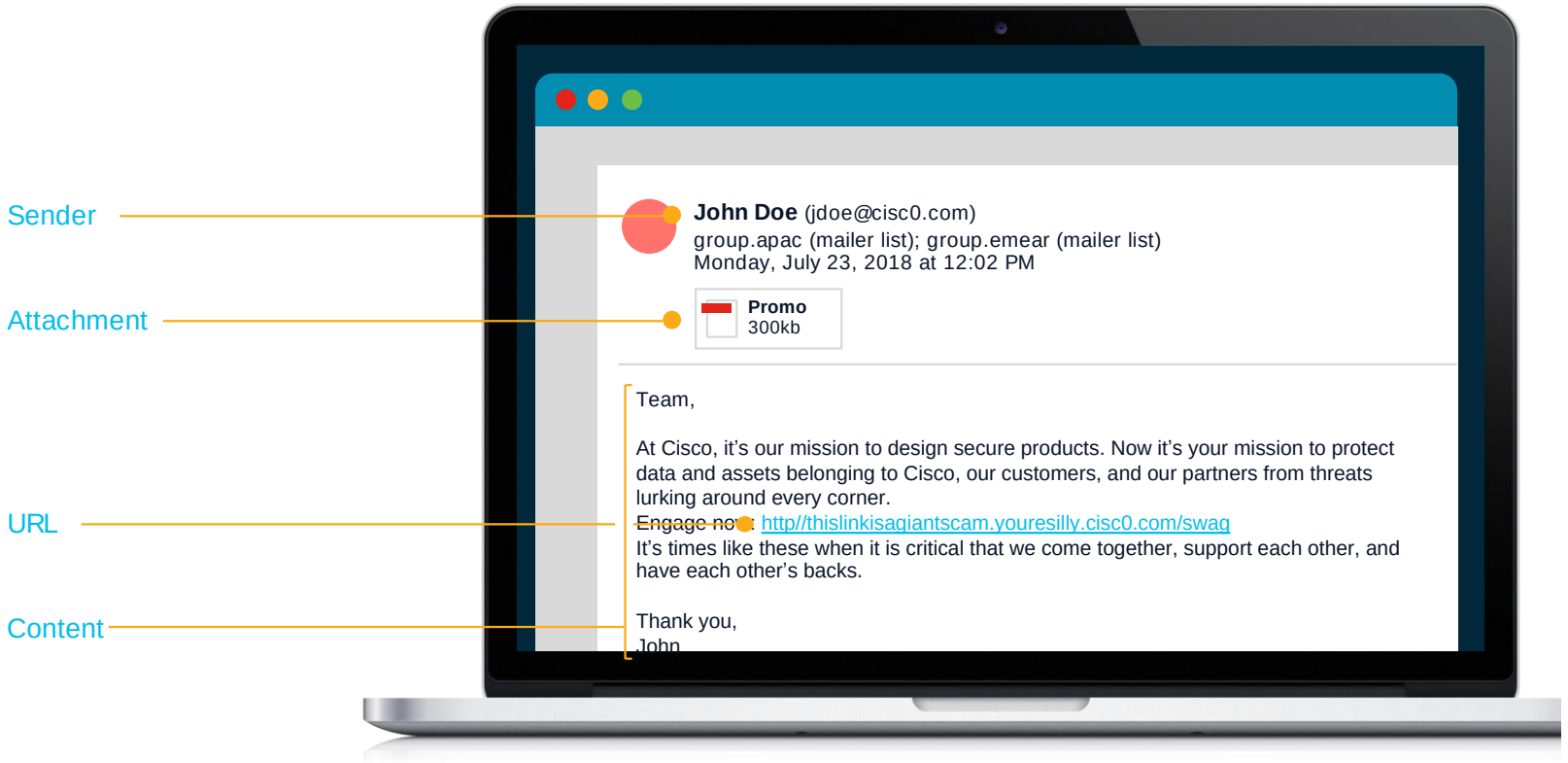
Meilleures performances et satisfaction des utilisateurs partout où il vont



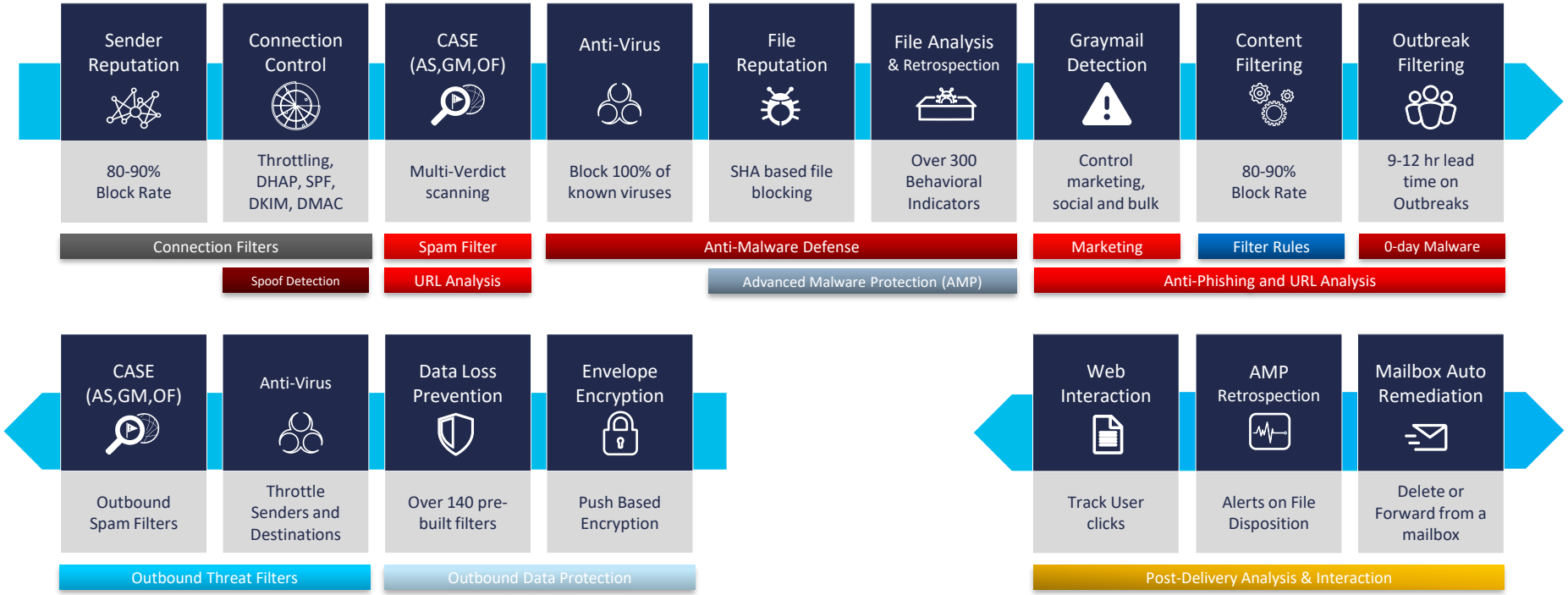
Cisco Cloud Email Security

Courriel : La première et dernière frontière

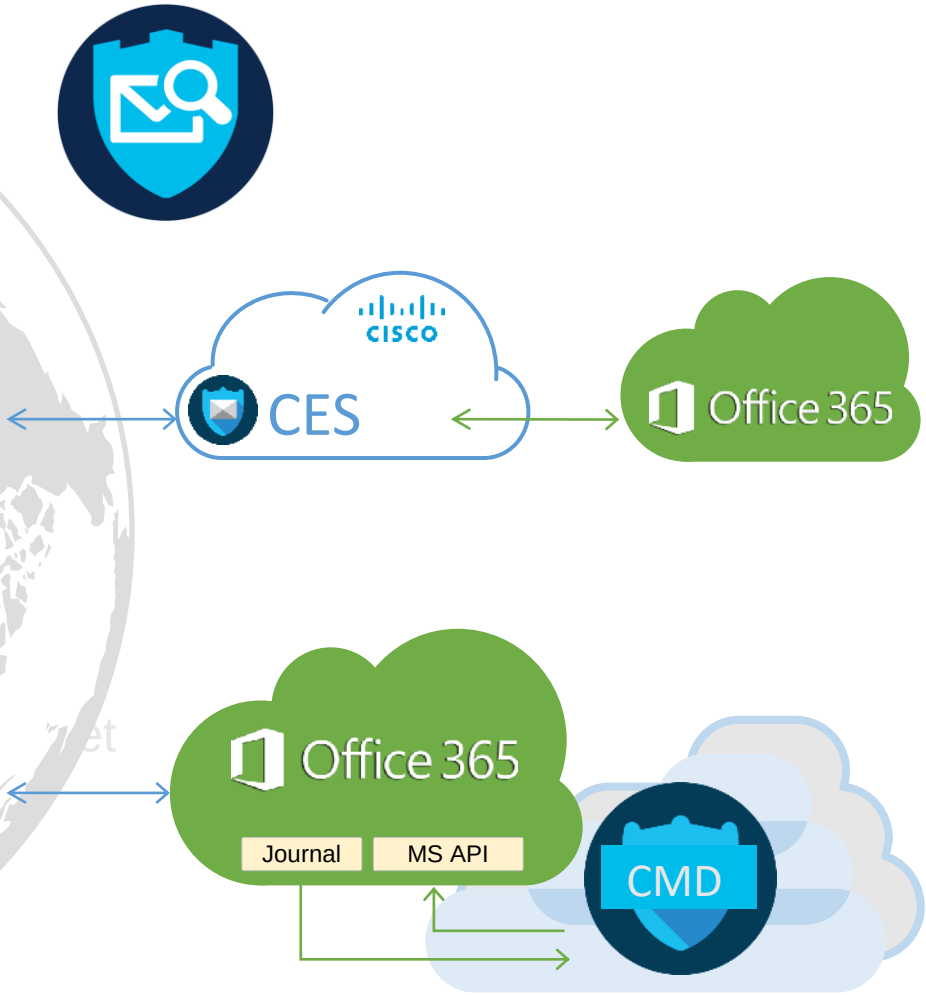
Toujours le vecteur de menace numéro 1



Sécurité des courriels entrants et sortants



Passerelle vs. CESS



Cloud Email Security (passerelle)

1. Le « MX record » a été remplacé par l'adresse CES
2. CES analyse les messages et prend une action
3. Le message est livré

Cloud Mailbox Defense (CESS)

1. L'enregistrement MX est inchangé
2. Une copie de chaque message est envoyée à CMD
3. CMD scanne et corrige à l'aide d'une API

CMD: Cisco Mailbox Defense

Cisco Cloud Email Security

O365	Cisco Email Security w/ O365
Anti-spam filters	Anti-spam filters
Anti-virus protection	Anti-virus protection
Policy enforcement	Policy enforcement
Disaster recovery	Disaster recovery
Directory services	Directory services
Advanced threat protection	Graymail detection
Message tracking	Message tracking
	Outbreak Filters
	Email encryption
	Advanced Malware Protection
	Detailed reporting
	STIX and TAXI feeds
	Data loss prevention (DLP)

ESi TECHNOLOGIES

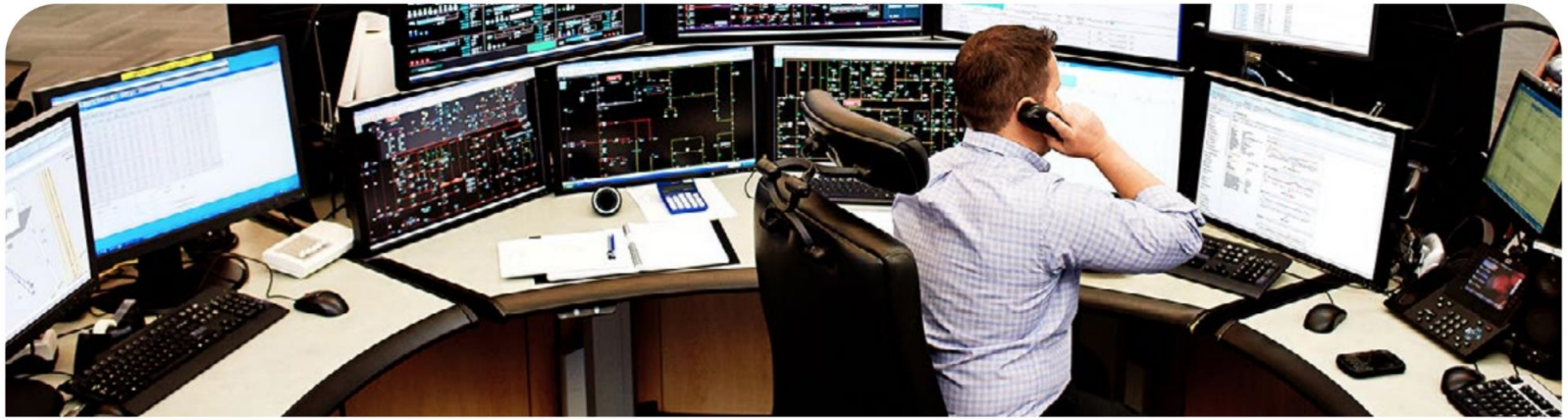
Cisco AMP: Advanced Malware Protection – Licence Essential

AMP for Endpoints

- AMP for Endpoint : le dernier moyen de défense qui remplace les anciens antivirus
  - NGAV : La base des données des signatures réside sur le poste
  - Continuous Monitoring : surveille toutes les activités des terminaux - fournit une détection au moment de l'exécution - bloque les comportements anormaux
  - Dynamic File Analysis : l'environnement sandboxing, optimisé Cisco Threat Grid, analyse le comportement des fichiers suspects
  - Behavioral Monitoring : Surveille en permanence toutes les activités des utilisateurs et des terminaux pour se protéger contre les comportements malveillants en temps réel
  - Vulnerability Identification : Identifie les logiciels vulnérables dans votre environnement pour aider à réduire la surface d'attaque
  - Endpoint Isolation : Capacité à isoler les terminaux qui ont été compromis pour empêcher la propagation des menaces

Cisco AMP: Advanced Malware Protection – Licence Advantage

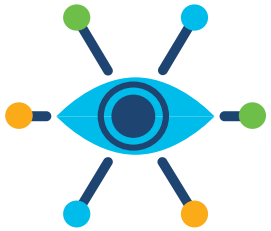
AMP for Endpoints



- Le plus haut niveau d'AMP pour les terminaux, incluant les fonctionnalités de la licence Essential
  - + Advanced Search : offre la possibilité de simplifier les enquêtes de sécurité, une visibilité approfondie sur ce qui s'est passé sur n'importe quel terminal à un moment donné
  - + Threat Grid Cloud : fournit un accès facile à l'analyse avancée des logiciels malveillants de Cisco et au portail de renseignements sur les menaces

Cisco EDR/AV

Que faut-il pour détecter et répondre à toutes les menaces qui peuvent entrer?

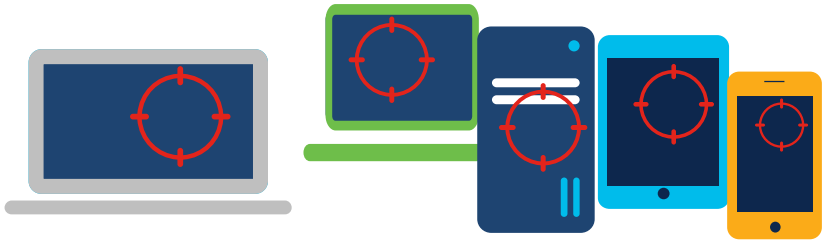


Visibilité complète

Compréhension du contexte

Meilleur contrôle

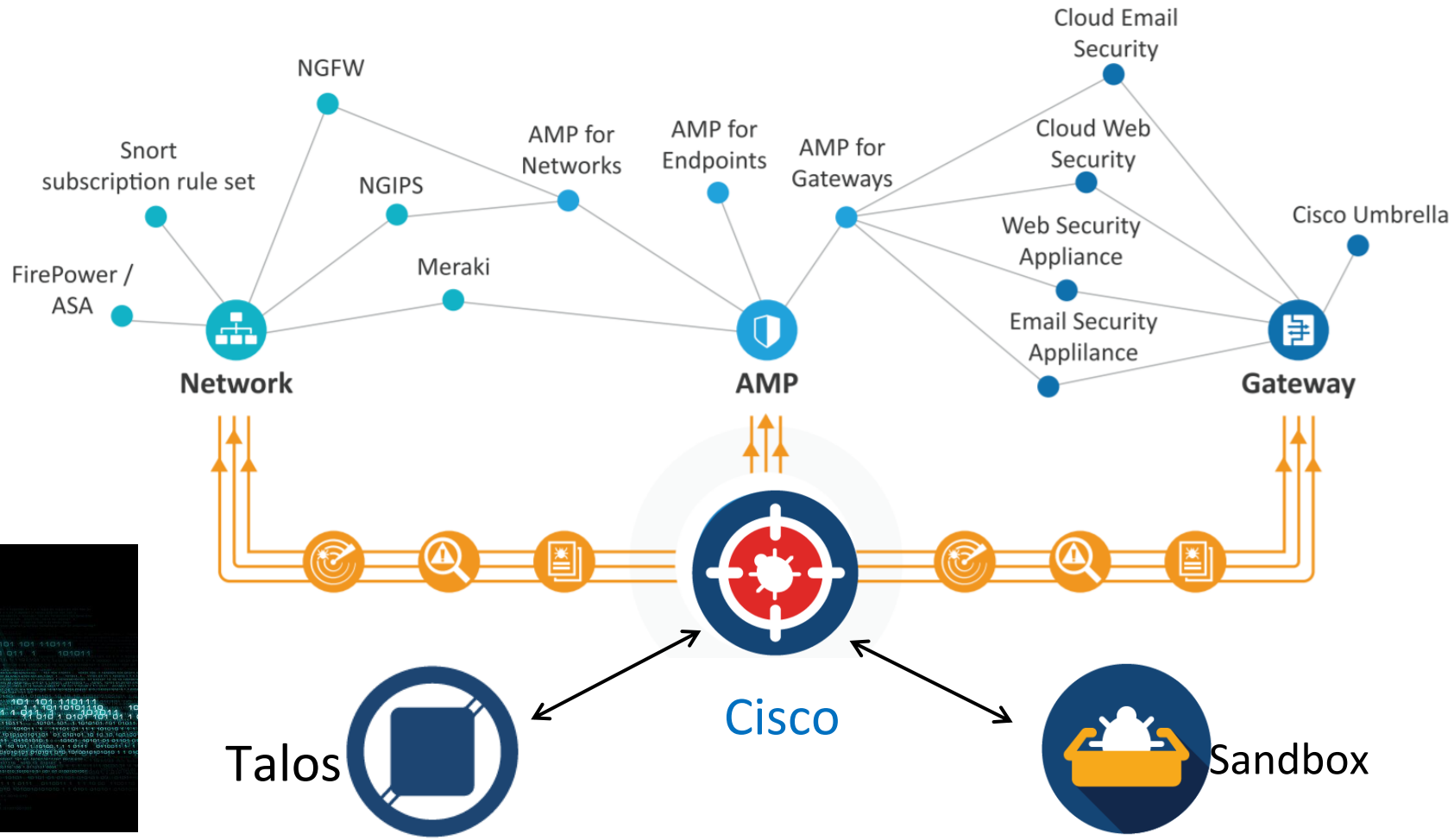
Sur les ordinateurs et appareils mobiles



PC, Mac, Linux, Mobile

Voir une fois, bloquer partout

Partagez vos renseignements sur le réseau, le web, le courrier électronique et les terminaux

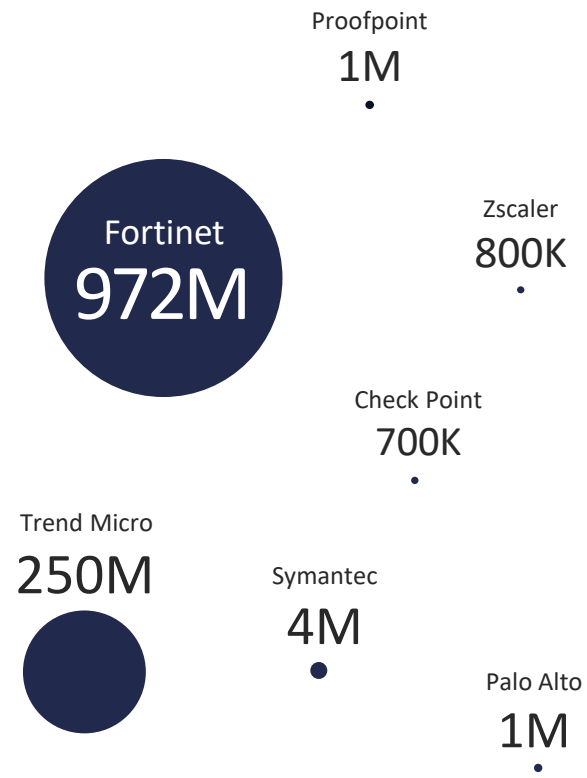


Plus de menaces bloquées à quotidiennement que n'importe qui d'autre

TALOS

Cisco Security Research

20B



- Plus de 250 chercheurs sur les menaces à plein temps
- Plus de 11 000 systèmes de leurres et pièges à menaces
- Des millions d'agents de télémétrie intégrés à leurs produits déployés dans le monde entier

ESi TECHNOLOGIES

Cisco DUO

- Selon le rapport d'enquête sur les violations de données 2019 de Verizon[1], 80% des failles de sécurité impliquent des mots de passe compromis
- Authentification multifacteur moderne et efficace
- Toutes les applications, à tout moment, n'importe où
- Duo protège vos applications en utilisant une deuxième source de validation pour vérifier l'identité de l'utilisateur avant d'accorder l'accès

Verify identity in seconds.

Protect any application on any device.

Easily deploy Duo in any environment.

[1] Via DBIR Interactive

Cisco DUO

Méthode d'authentification à deux facteurs

→ Prend en charge tous les utilisateurs : identifiant/mot de passe + 2FA

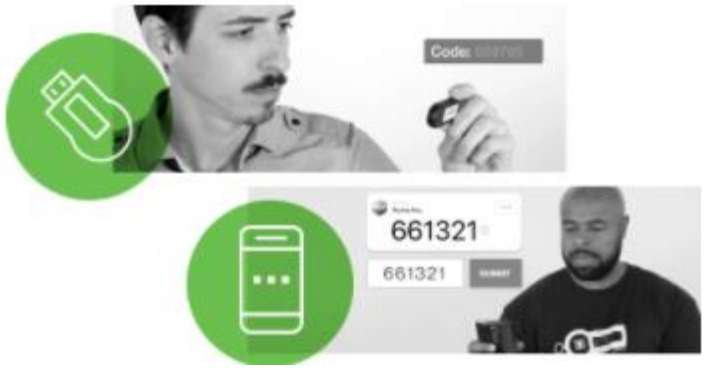
Duo Push

iOS, Android

U2F et biométrique

macOS, Windows

Jetons et codes d'accès



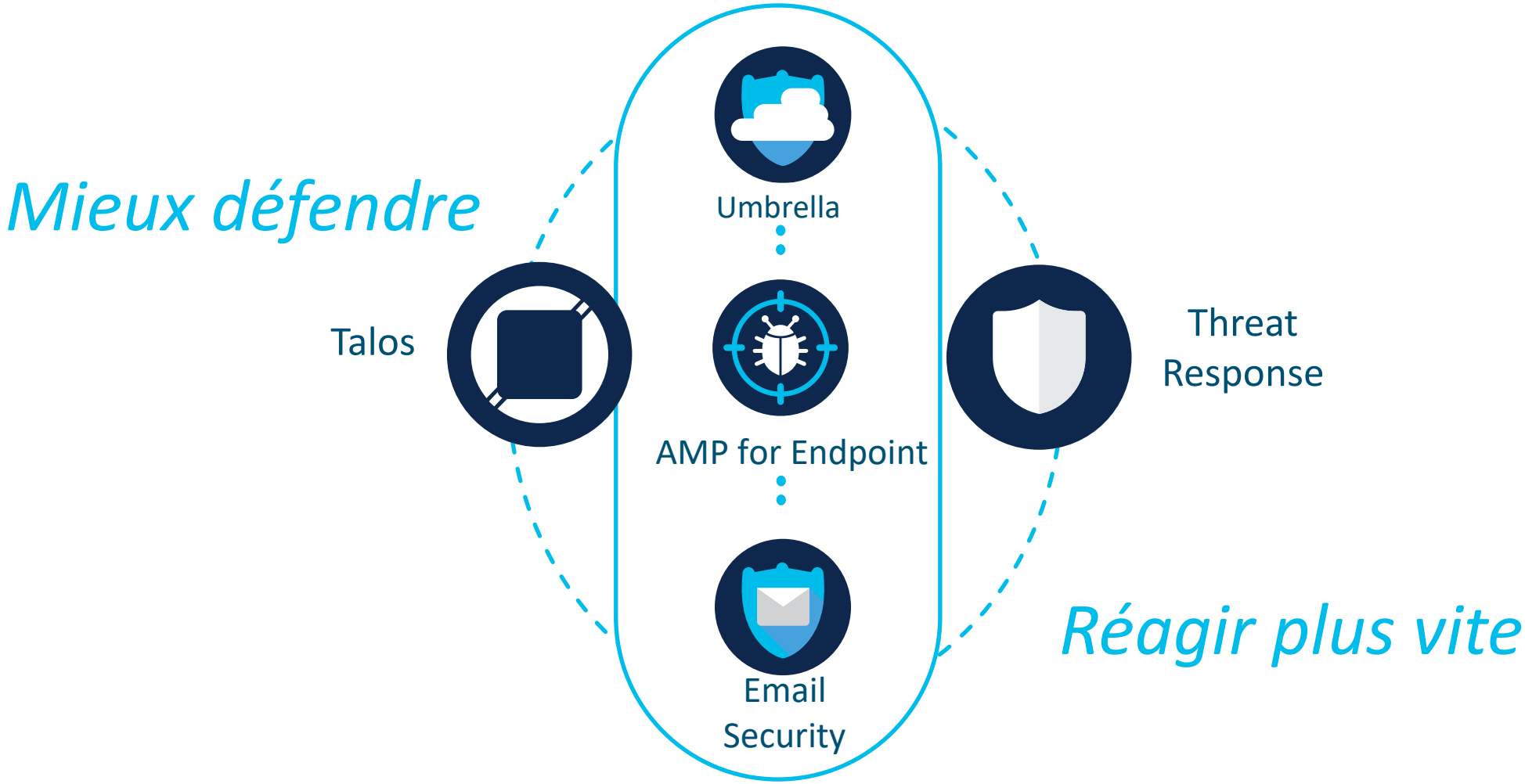
DÉMO DUO!

https://demo.duo.com/

Besoin d’aide?... L’approche d’accompagement d’ESI

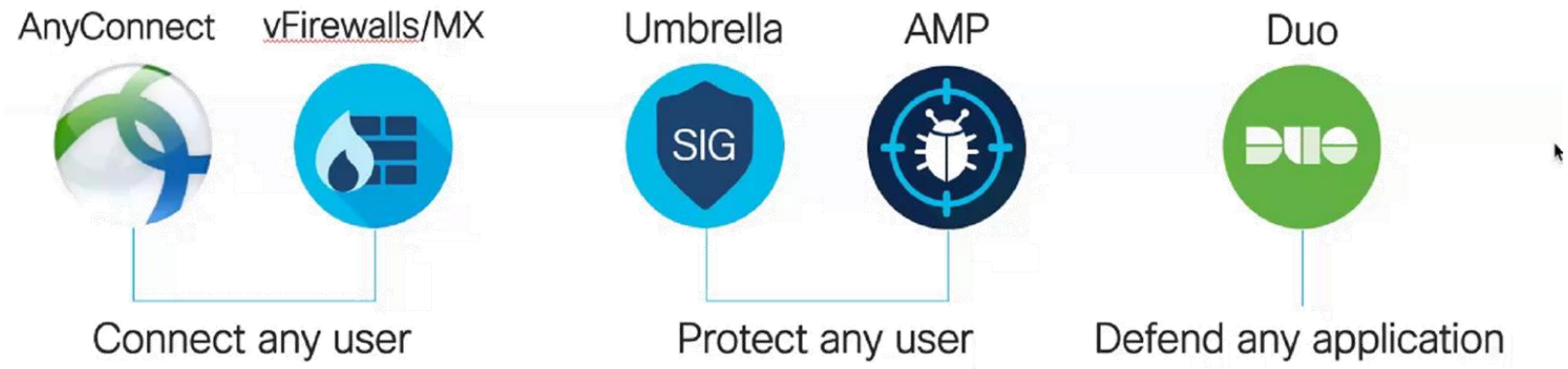
Analyse et découverte	Architecture	Gestion du risque	Stratégie d’exploitation
			
Solution existante Expansion Fonctionnalités	Solutions partenaires Services pros, PoC	Solutions de sécurité adjacentes Alternatives	Document d’installation Facilité de gestion Formation

Architecture de sécurité intégrée de Cisco



Ce qu'il faut retenir…

- Demandez de l'assistance pour une solution de télétravail sécuritaire
- Pensez à protéger vos employés, qu'ils soient branchés à votre réseau ou non (Umbrella)
- Ayez une solution pour les courriels (CES)
- Considérez un NGAV ou un EDR (AMP)
- Pensez à une authentification forte (DUO)



Période de questions

Merci de votre attention!