La Cyber-Resilience est davantage que la sécurité de l'IT. Comprendre l'approche du CISO vis-à-vis des métiers.

Bechtle-IT Forum | 13.06.2023| SwissTech Convention Center Lausanne

Raphaël Marichez, CSO-Cybersecurity and Digital transformation advisor, Palo Alto Networks
Philippe Glohr, Solution Architect, Bechtle Suisse

1

Niveau de menace actuel

2

Cyber Résilience, qu'est-ce ?

3

Cas d'usage de la cyber-résilience : Prisma Access

4

Une approche de plateformes intégrées pour la résilience

1

Niveau de menace actuel

2

Cyber Résilience, qu'est-ce ?

3

Cas d'usage de la cyber-résilience : Prisma Access

4

Une approche de plateformes intégrées pour la résilience

Les attaques continuent d'augmenter et de défier les organisations

Les attaques sont communes

63%

des organisations ont été victimes au cours de la dernière année.

Elles sont difficiles à résoudre

37 jours

ont été nécessaire en moyenne pour se remettre d'une attaque.

Elles coûtent

$2.4M

était le coût moyen associé à la récupération de l'attaque.

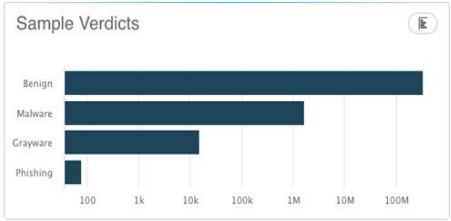
Les organisations qui manquaient de préparation à la réponse aux incidents et aux crises mettaient plus de temps à se remettre des attaques et les trouvaient plus coûteuses.

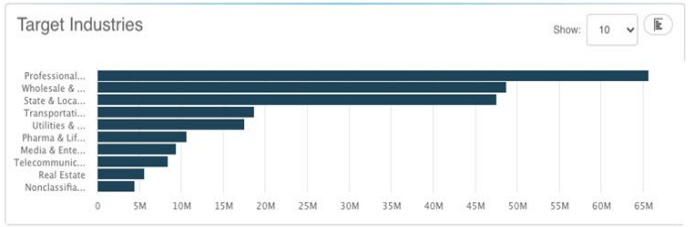
Source: The 2021 State Of Enterprise Breaches, Forrester Research, Inc., April 8, 2022

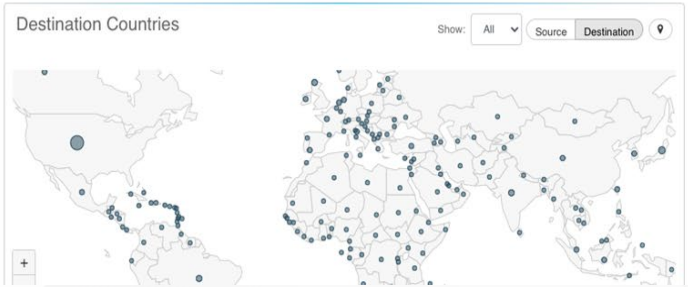
Niveau de menace actuel

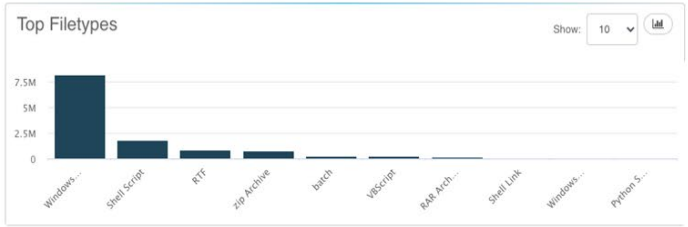
Les Cyber menaces

- Déni de service
- Rancongiciel
- Hameçonnage
- Cheval de Troie
- Usurpation d'identités







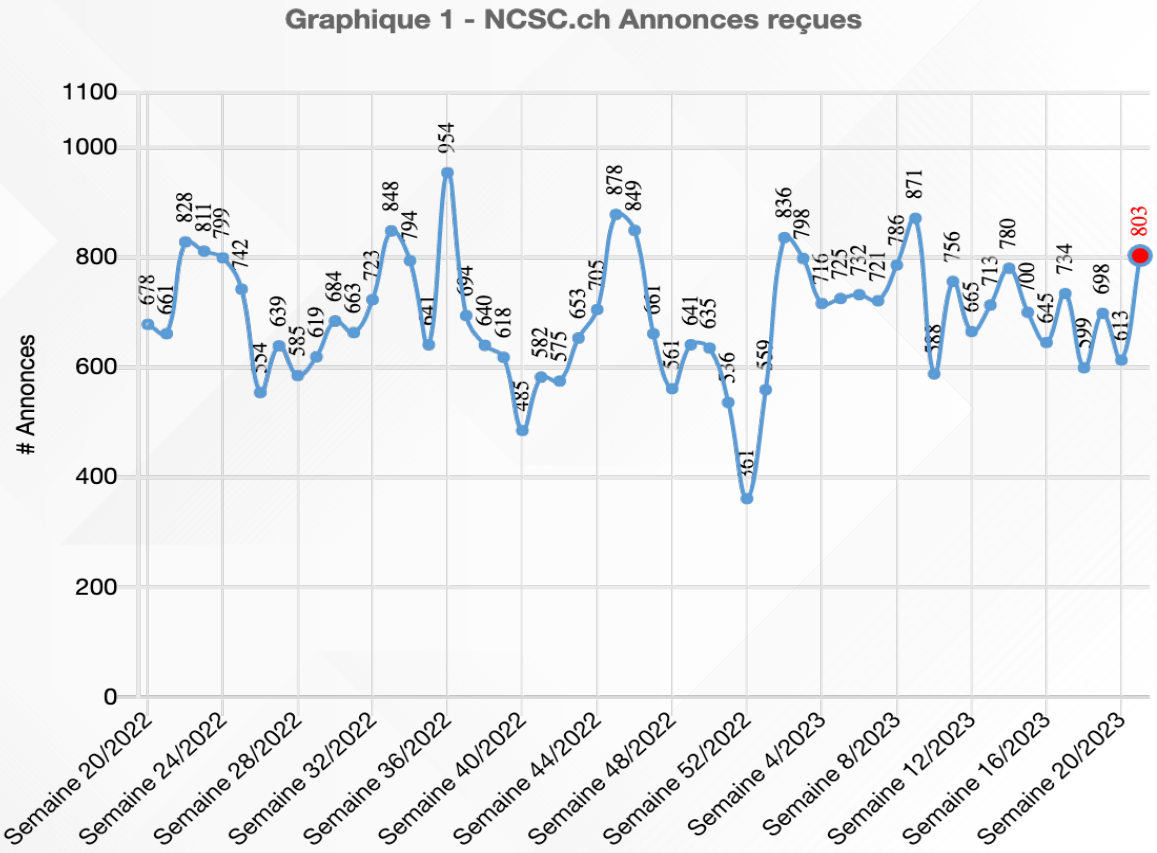


Les cyber risques en Suisse

Centre National pour la Cybersécurité (Melani)

- Arnaques
- Hameconnage
- Spoofing
- Logiciel malveillant

Loi sur la sécurité de l'information (LSI)



Cyber attaques, Quelques exemples

Cyberattaque

Des cybercriminels menacent de publier des données sensibles de la NZZ (update)

Des cyberpirates se sont introduits dans le réseau des CFF

Tessiner Privatklinik Opfer eines Cyberangriffs

Neuchâtel a amélioré sa cybersécurité

Le Canton a accéléré la mise en place de nouvelles mesures de sécurité déjà planifiées à la suite de la cyberattaque de l'Université de Neuchâtel

Une firme informatique et ses clients victimes de hackers

Des hackers diffusent les données médicales de milliers de Neuchâtelois

Des pirates ont mis à exécution leur menace et ont diffusé les informations très sensibles sur les patients de cabinets neuchâtelois.

Cyberkriminelle veröffentlichen Daten von Schweizer Medienhaus

1

Niveau de menace actuel

2

Cyber Résilience, qu'est-ce ?

3

Cas d'usage de la cyber-résilience : Prisma Access

4

Une approche de plateformes intégrées pour la résilience

Résilience opérationnelle

“La capacité à exécuter des opérations critiques en cas de perturbation.”

Ex: DORA,
risque systémique financier

Résilience des systèmes de communication (“fonctionnelle”)

La “performance de la fonction” : au niveau du système et de sa décomposition fonctionnelle, pas de l’usage.

“La capacité à résister aux impacts négatifs dus à des menaces connues ou non, y compris incertaines et inattendues.”

“Résilience sociétale”

“Secured by design”

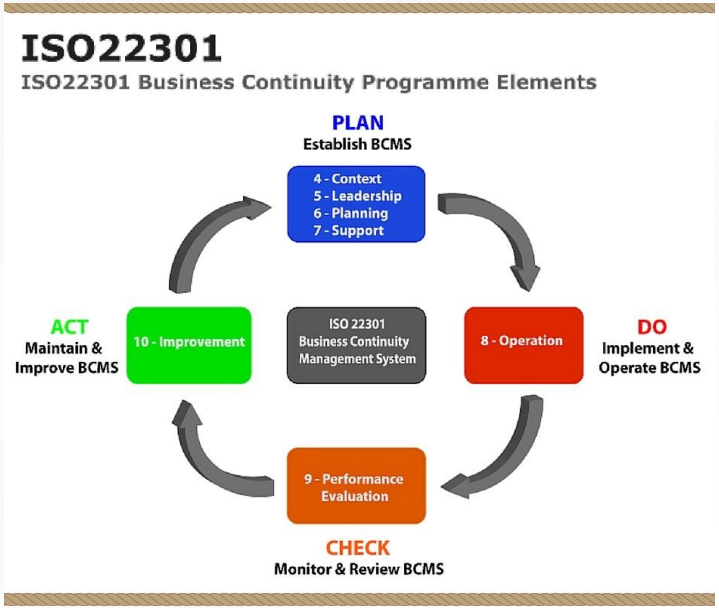
Ex: CRA, NIS2

"Le cyber est un bien social. Il s'agit de résilience sociétale. Nous devons changer fondamentalement la relation entre le gouvernement et l'industrie.” (Jen Easterly, DG CISA, 2023)

Résilience opérationnelle *(Operational Resilience)*

L'ISO 22301, Sécurité et résilience – Systèmes de management de la continuité d'activité, publié en 2012, décrit les exigences d'un système de management pour :

- **se protéger** contre les incidents perturbateurs,
- **en réduire** la probabilité d'occurrence,
- **y répondre et s'en remettre** lorsqu'ils surviennent. ⇐ "**Résilience**"



Résilience opérationnelle *(Operational Resilience)*

Le Comité de Bâle sur le contrôle bancaire adopte Bâle III **en 2010** pour “renforcer la **résilience** des établissements et systèmes bancaires“

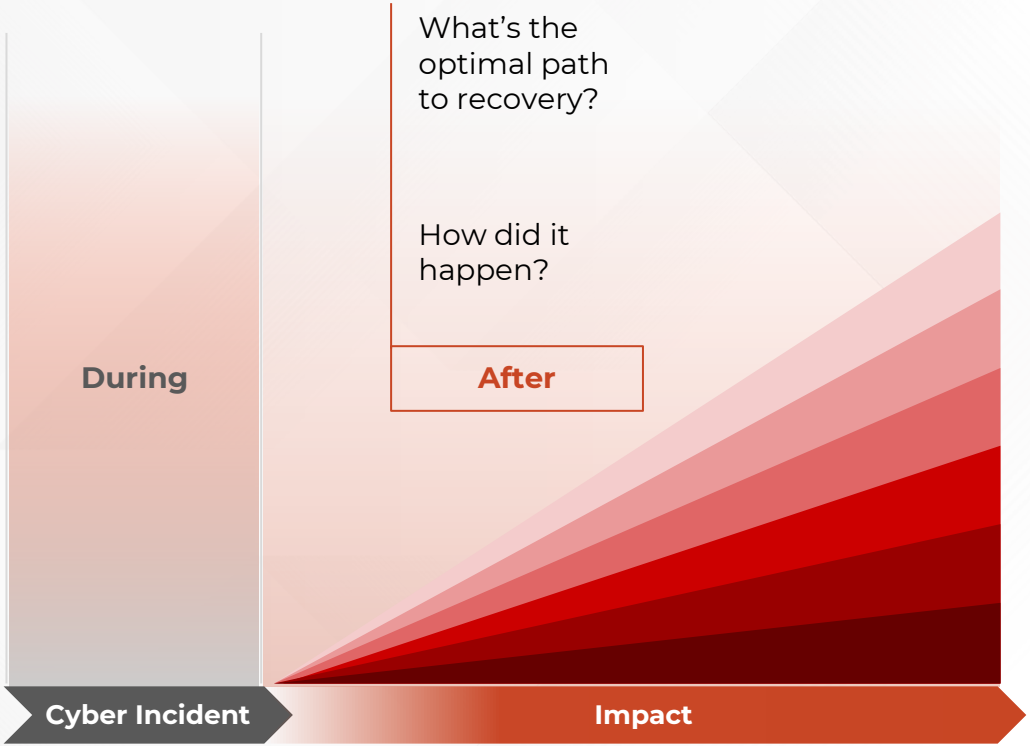
Aujourd’hui (2021), il définit la “Résilience opérationnelle” ainsi :

- la capacité d'une banque **à exécuter des opérations critiques en cas de perturbation** (“disruption”) plus précisément :
- identifier et se protéger contre les menaces et les défaillances potentielles,réagir et s'adapter,ainsi que récupérer et apprendre des perturbations,en vue de minimiser leur impact sur la réalisation des opérations critiques

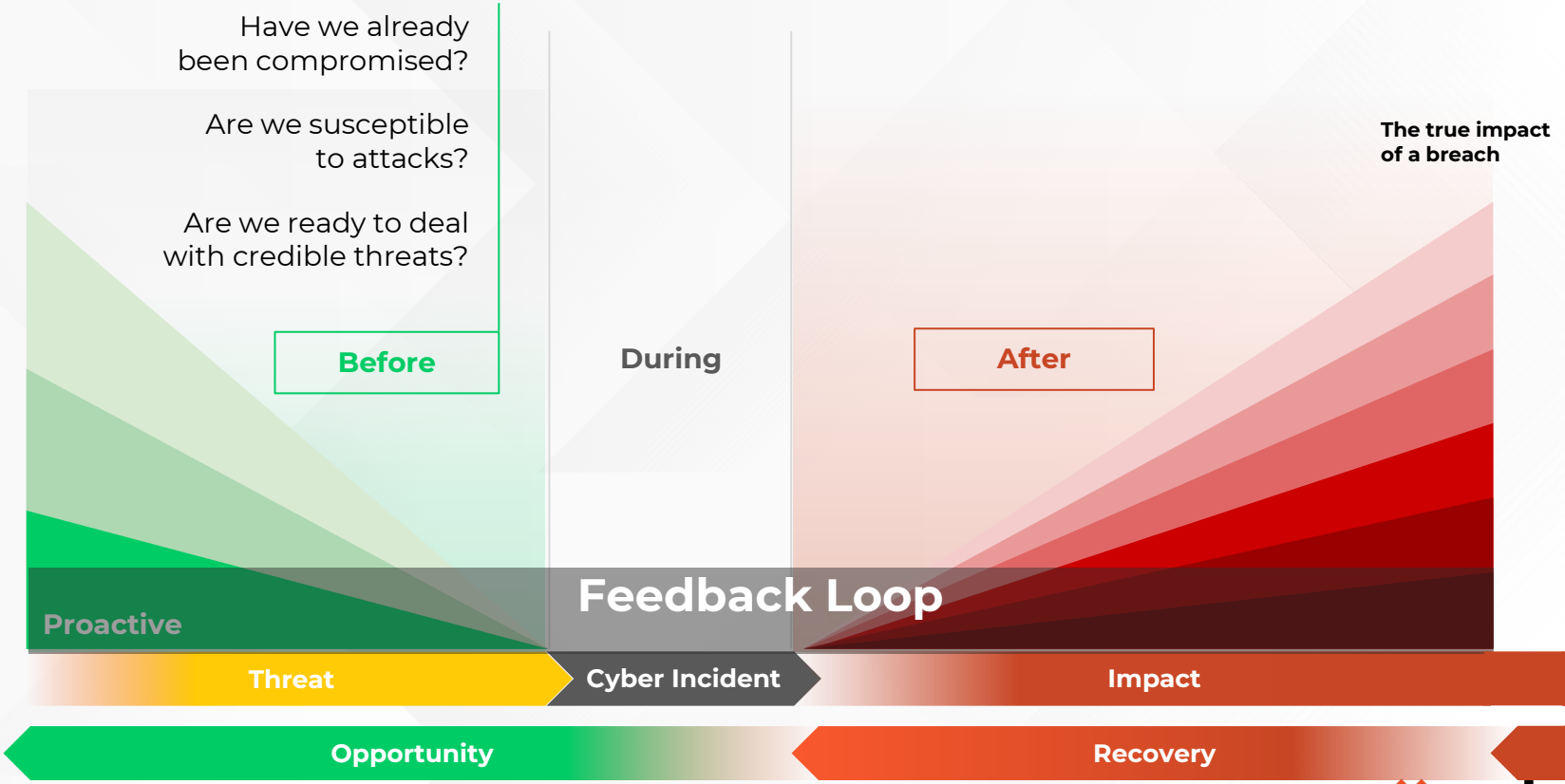
De *Business Continuity* à *Operational Resilience*

Business continuity

(business impact analysis, return time objective)



De *Business Continuity* à *Operational Resilience:* Une posture permanente et évolutive



De *Operational Resilience* à *Cyber Resilience*

2017

Wannacry

Equifax

Risque sur les systèmes par “l’interdépendance financière, les dépendances opérationnelles et l’impact sur la confiance”.

Le FMI considère les cybermenaces comme un “risque pour la stabilité financière” dans son Rapport sur la stabilité financière dans le monde d’octobre 2017.

De *Operational Resilience* à *Cyber Resilience*

Pile, capacités opérationnelles :

Perturbation d'une capacité numérique

- Perte d'un datacenter (sinistre)
- Cryptolocker
- Perte d'un service (DoS)…
- Perte de compétence rare (RH)
- …

Face, activités :

Dysfonctionnement d'une opération critique "cyber" :

- Gestion de la réputation en ligne (communication)
- *risk rating* "cyber" (assurabilité "cyber")
- Dommage causés à ses clients (ESN, fintech…)
- Confiance des clients dans ses services en ligne…

Résilience opérationnelle

2ème nuance: le fonctionnement des infrastructures

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Norme minimale TIC (27.08.2018)
Et
Stratégie nationale pour protéger la Suisse des cyber-risques (SNPC 2018-2022)
*"Le but est d'améliorer la **résilience** (capacité de résistance et de réactivation) **des infrastructures** critiques en Suisse."*

Résilience fonctionnelle

*"La **résilience fonctionnelle** représente la capacité d'un système technique à se préserver de dommages importants tout en assurant au minimum le service nécessaire aux infrastructures critiques" (2012, "Le concept de résilience à l'épreuve du génie urbain" - France)*

3ème nuance: la “ *Résilience Sociétale* ” (nouveau)

- Jen Easterly, CISA director (CES 2023 in Las Vegas)

“We live in a world of massive connections where that critical infrastructure that we rely upon is all underpinned by a technology ecosystem that unfortunately has become really unsafe,”

“We've essentially accepted as normal that **technology is released to market** with dozens or hundreds or thousands of vulnerabilities and defects and flaws,”

“Cyber is a social good”
“**It’s about societal resilience**. And my last message is that we need to fundamentally change the relationship between government and industry”

Expérience

Director
Cybersecurity and Infrastructure Security Agency
juil. 2021 - aujourd’hui · 1 an 9 mois
Arlington, Virginia, United States

Morgan Stanley
4 ans 6 mois

Head of Firm Resilience and the Fusion Resilience Center
janv. 2021 - juil. 2021 · 7 mois

Global Head of the Fusion Resilience Center
janv. 2020 - déc. 2020 · 1 an

The Fusion Resilience Center expands the remit of the Cybersecurity Fusion Center full range of business-disrupting threats from cyber attacks and fraud to technolog

Global Head of the Cybersecurity Fusion Center
févr. 2017 - janv. 2020 · 3 ans
New York City

Morgan Stanley’s Global Cybersecurity Fusion Center is charged with assessing, de

Résilience sociétale

Le bingo résilience !

#1 Résilience opérationnelle

#2 Résilience fonctionnelle

#3 Résilience sociétale

Résilience	L'aptitude d'un système, d'une organisation ou d'une société à faire face à des perturbations internes ou externes et à maintenir son bon fonctionnement ou à le rétablir aussi rapidement et complètement que possible.

Cyberstratégie nationale (CSN) (2023)
https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/medienmitteilungen/newslist.msg-id-94237.html

Un exemple : s'agit-il de cyber-résilience?

L'attractivité des talents cyber en entreprise

La gestion prévisionnelle des compétences (emplois, attractivité) dans le domaine cyber.

⇒ Il s'agit d'un processus proactif, qui peut "apprendre" des perturbations
⇒ Il s'agit de s'assurer d'une capacité opérationnelle (RH)

Il s'agit donc bien de **résilience opérationnelle**, produisant des effets dans le **domaine cyber.**

L’anticipation et la flexibilité

- Mykhaïlo Fedorov, Ministre en charge du numérique, Ukraine

“Les missiles russes ne peuvent pas détruire le cloud."

La confiance et les interdépendances

OECD
BETTER POLICIES FOR BETTER LIVES

GLOBAL FORUM ON
DIGITAL SECURITY
FOR PROSPERITY

HOME ABOUT PAST EVENTS

7-9 June 2021 Virtual, hosted by Israel Watch the replays

3rd event

Local challenges, global solutions: Building cyber resilience together in a post-COVID-19 world

Résilience sociétale

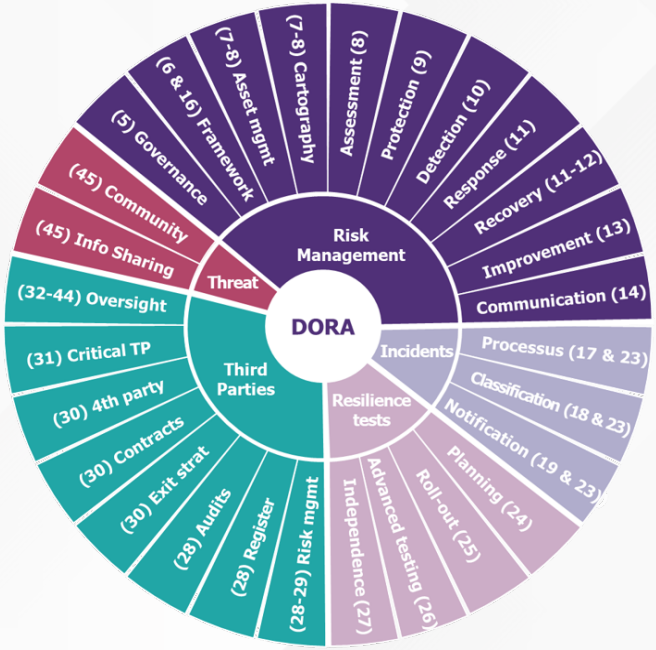
The Act will

- Ensure that **products with digital elements** placed on the EU market have **fewer vulnerabilities** and that manufacturers remain **responsible for cybersecurity** throughout a product's life cycle;
- **Improve transparency** on security of hardware and software products;
- Business users and consumers benefit from **better protection.**

DARA : l'harmonisation de règles "cyber" sectorielles

- DORA renforce le **versant numérique de la résilience opérationnelle** du secteur financier par des mesures portant sur la **sécurité des réseaux et des systèmes d'information**

(ACPR, 5/12/2022)



De la sécurité des systèmes à la cyber-résilience

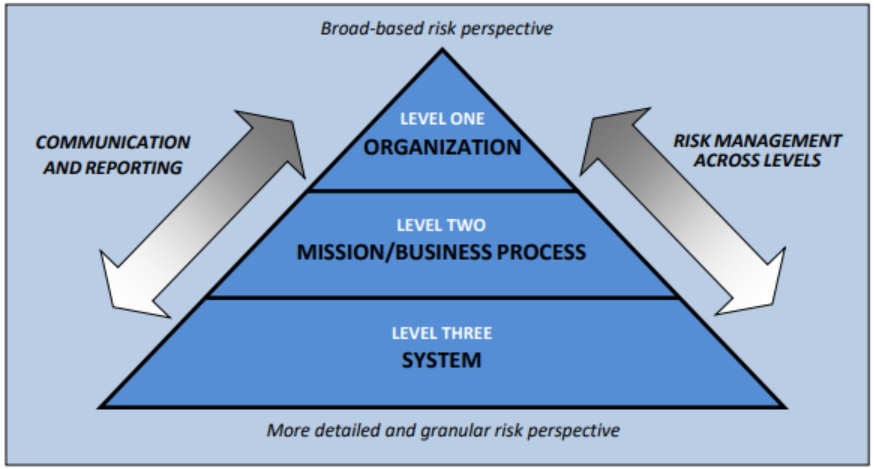


FIGURE D-1: ORGANIZATION-WIDE RISK MANAGEMENT APPROACH

Vu du NIST (2018, 2021)

Les objectifs de cyber-résilience (anticiper, résister, récupérer et s'adapter) soutiennent le **lien** entre :

- la gestion des risques au niveau de **la mission** ou **des activités opérationnelles**,
- et la gestion des risques au niveau de **l'organisation** et **du système**

Vu du Information Security Forum (ISF), 2019

La cyber-résilience complète la cyber-protection pour aider à garantir que l'organisation peut résister à un cyber-événement majeur et continuer à fonctionner avec un minimum de perturbations. Ceci est réalisé grâce à une gamme de capacités, y compris les pratiques de continuité des activités, la gestion des incidents, le soutien juridique, la gestion des relations publiques et la cyberassurance.

1

Niveau de menace actuel

2

Cyber Résilience, qu'est-ce ?

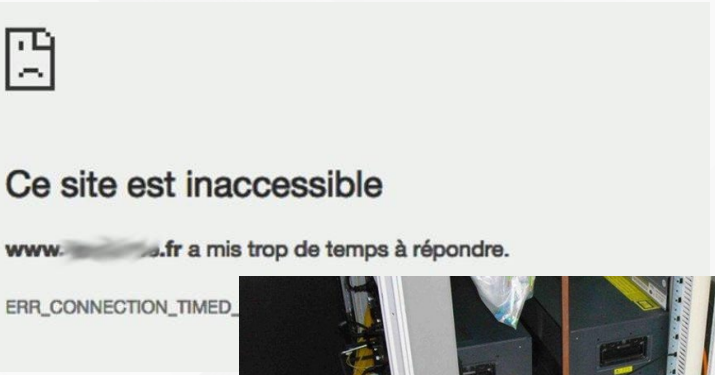
3

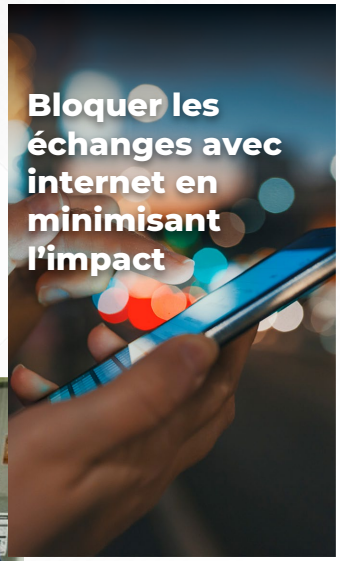
Cas d'usage de la cyber-résilience : Prisma Access

4

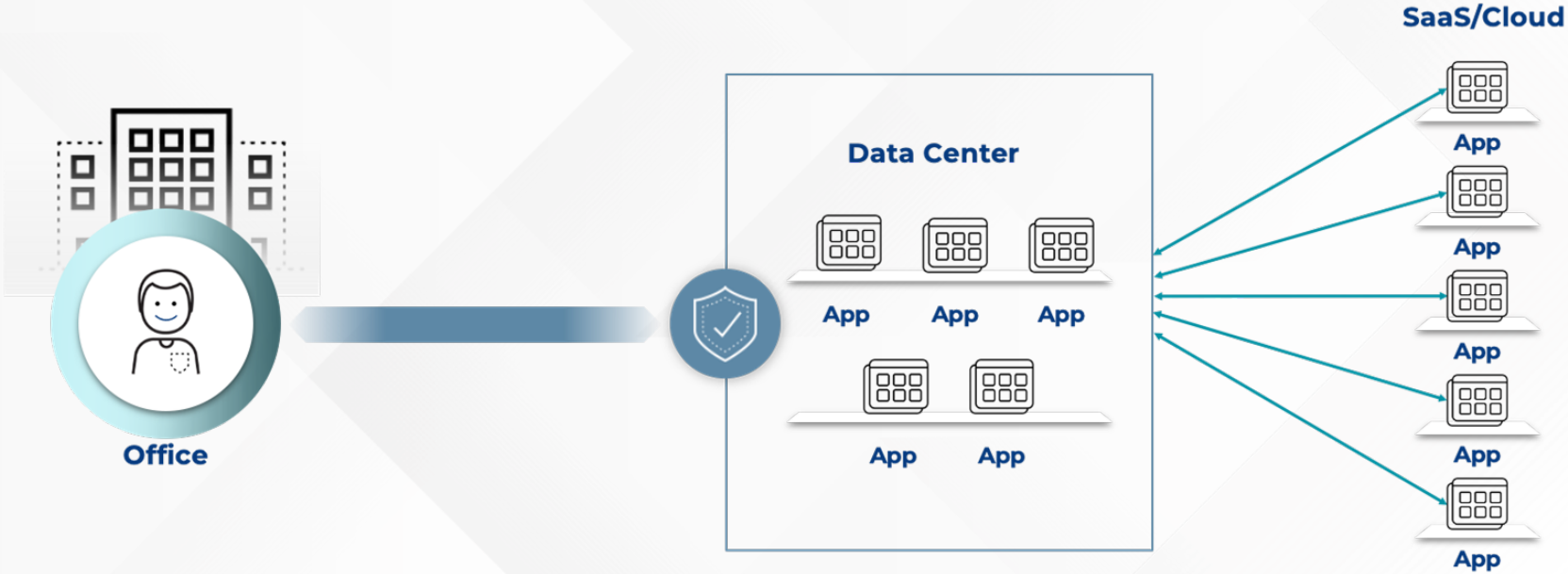
Une approche de plateformes intégrées pour la résilience

Du “Réseau interne” à l’ “*Internet d’Entreprise*”

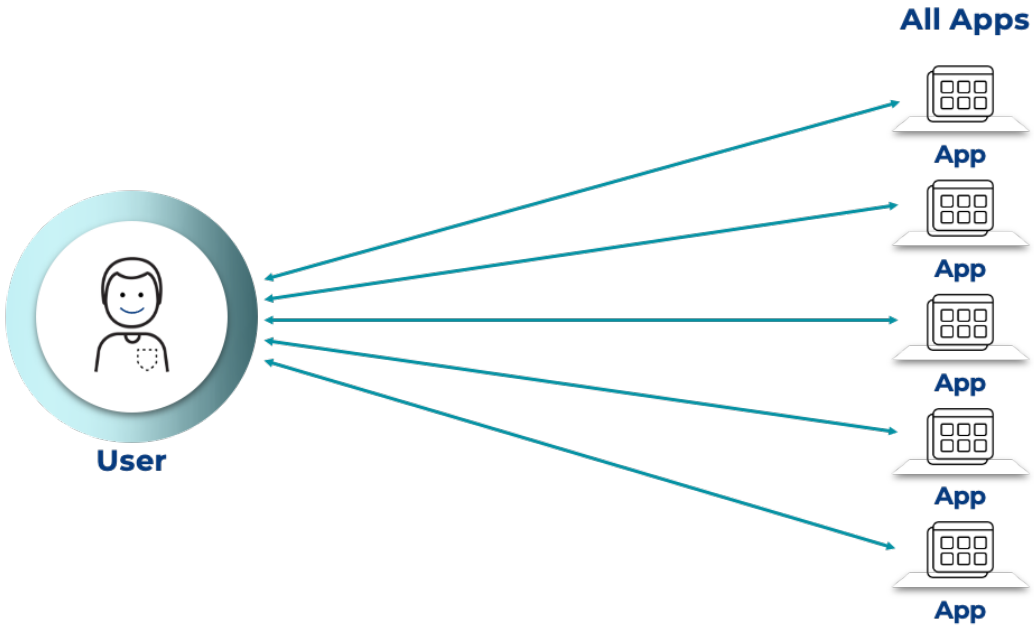




LA SÉCURITÉ ÉTAIT SIMPLE QUAND:
LE TRAVAIL ÉTAIT À UN ENDROIT PRÉCIS

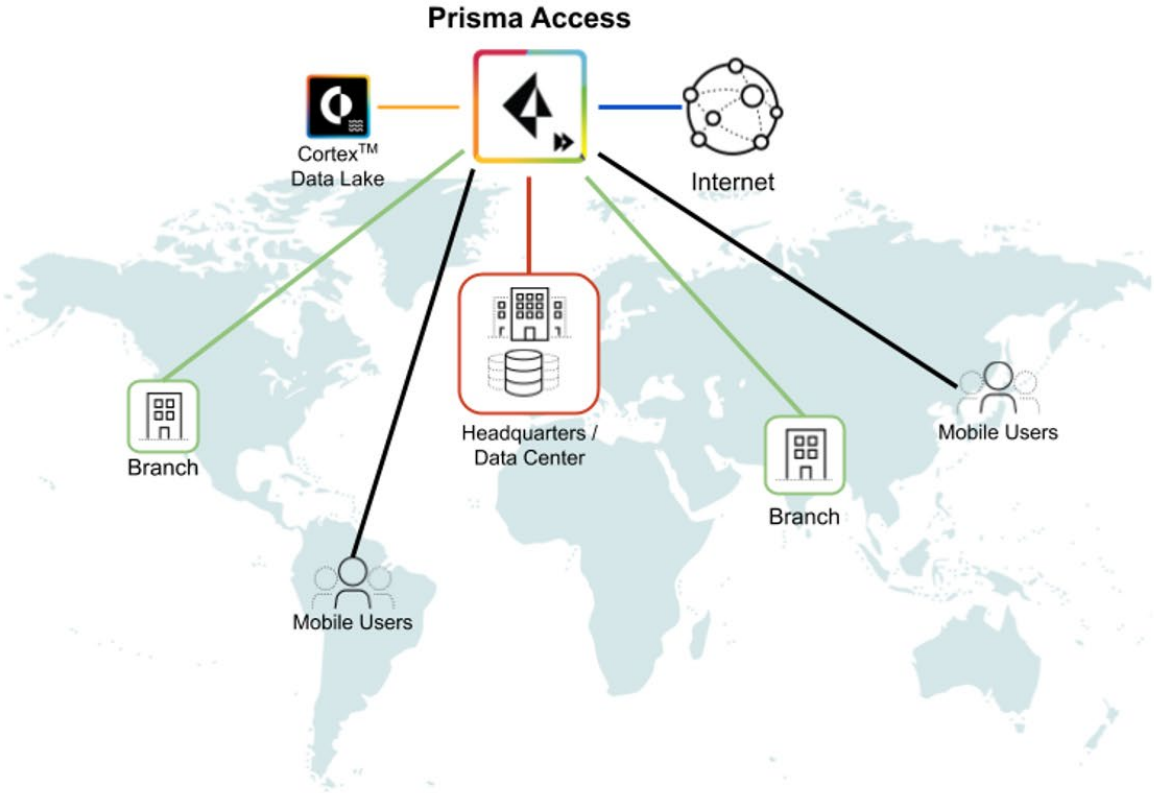


LES IMPLICATIONS DE SÉCURITÉ DU TRAVAIL HYBRIDE: LES UTILISATEURS VONT MAINTENANT DIRECTEMENT VERS LES APPLICATIONS

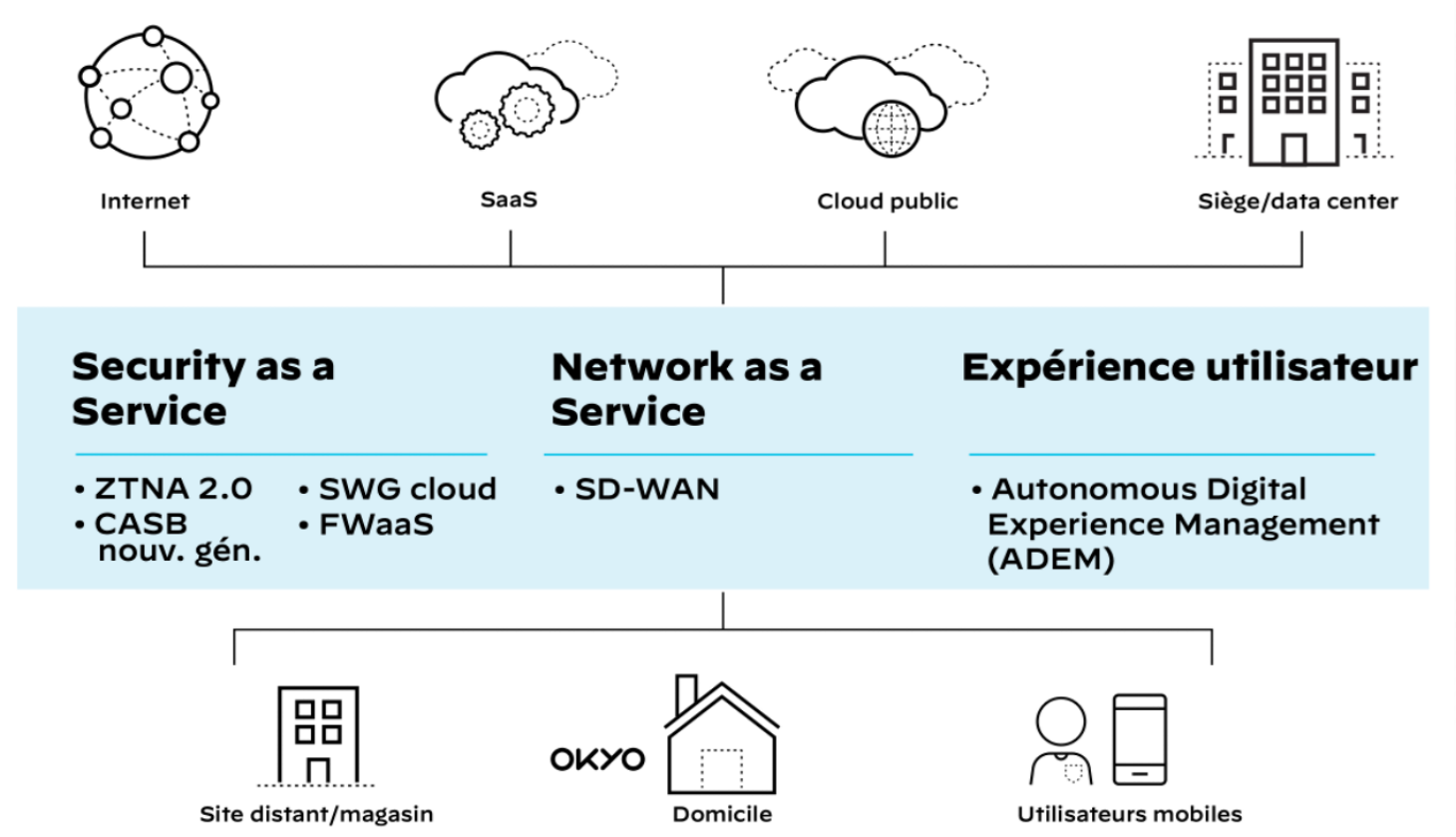


- La plupart des applications vivent désormais en dehors du DC
- Les utilisateurs travaillent à domicile et au bureau
- Architecture directe vers l'application requise

Qu’est-ce que Prisma Access ?



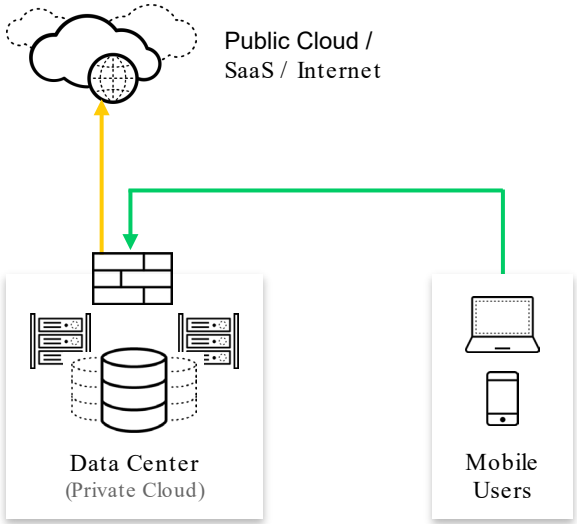
Service Cloud



Exemple: reprise d’activité VPN sans compromis sur la sécurité

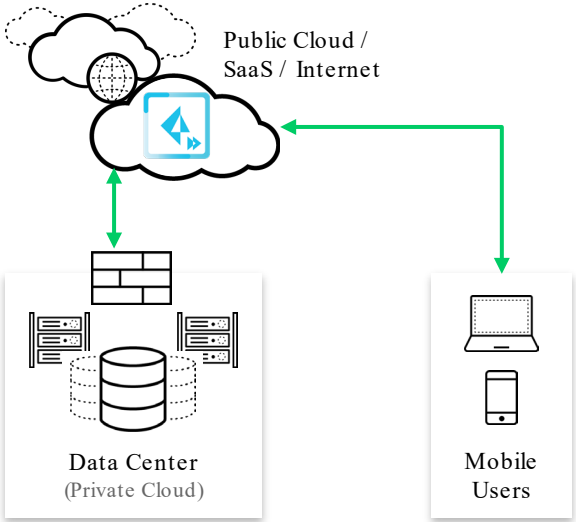
Solution VPN en place

Tout le trafic est redirigé vers le centre de données via le réseau d’entreprise

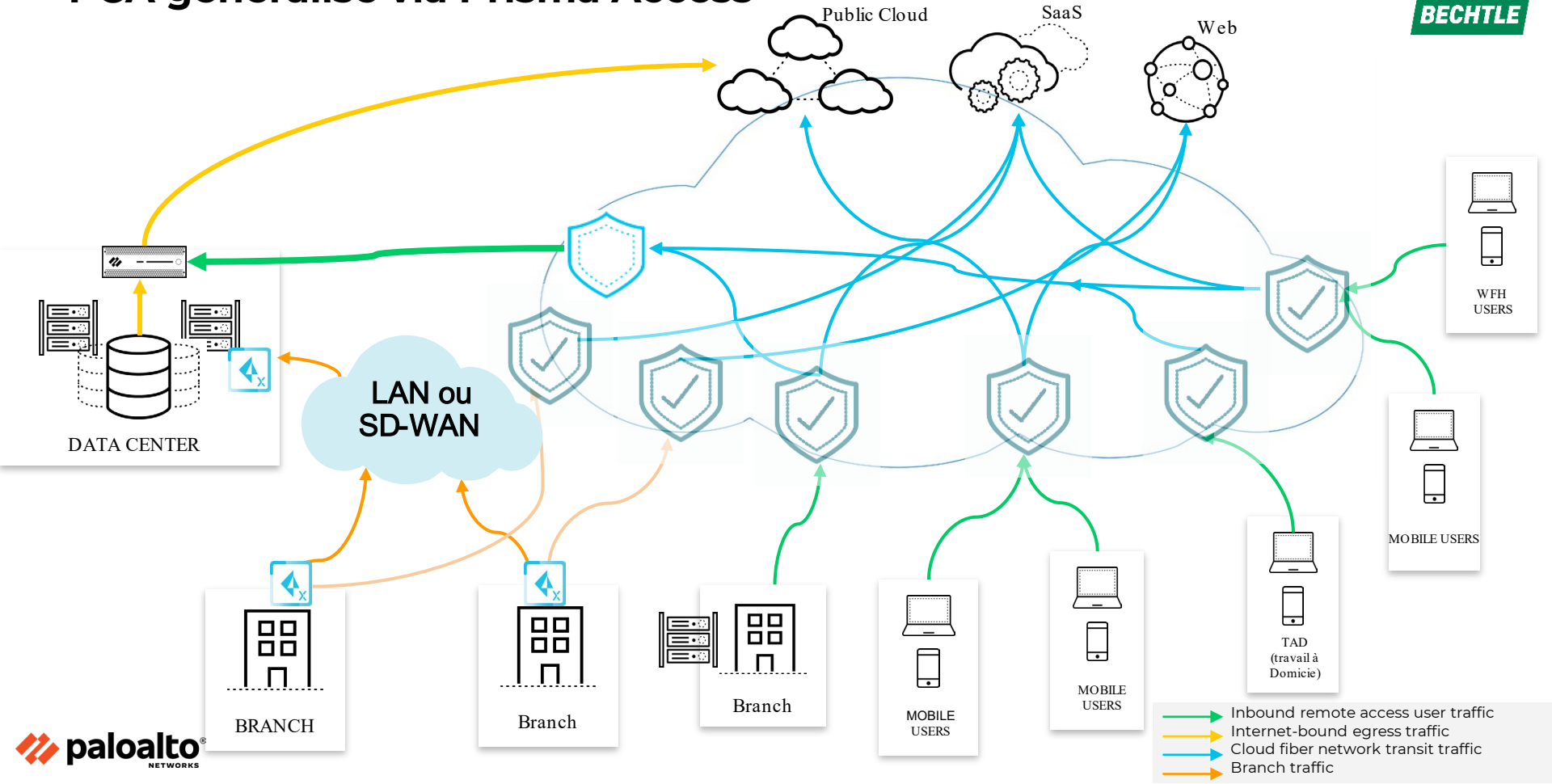


PCA via Prisma Access

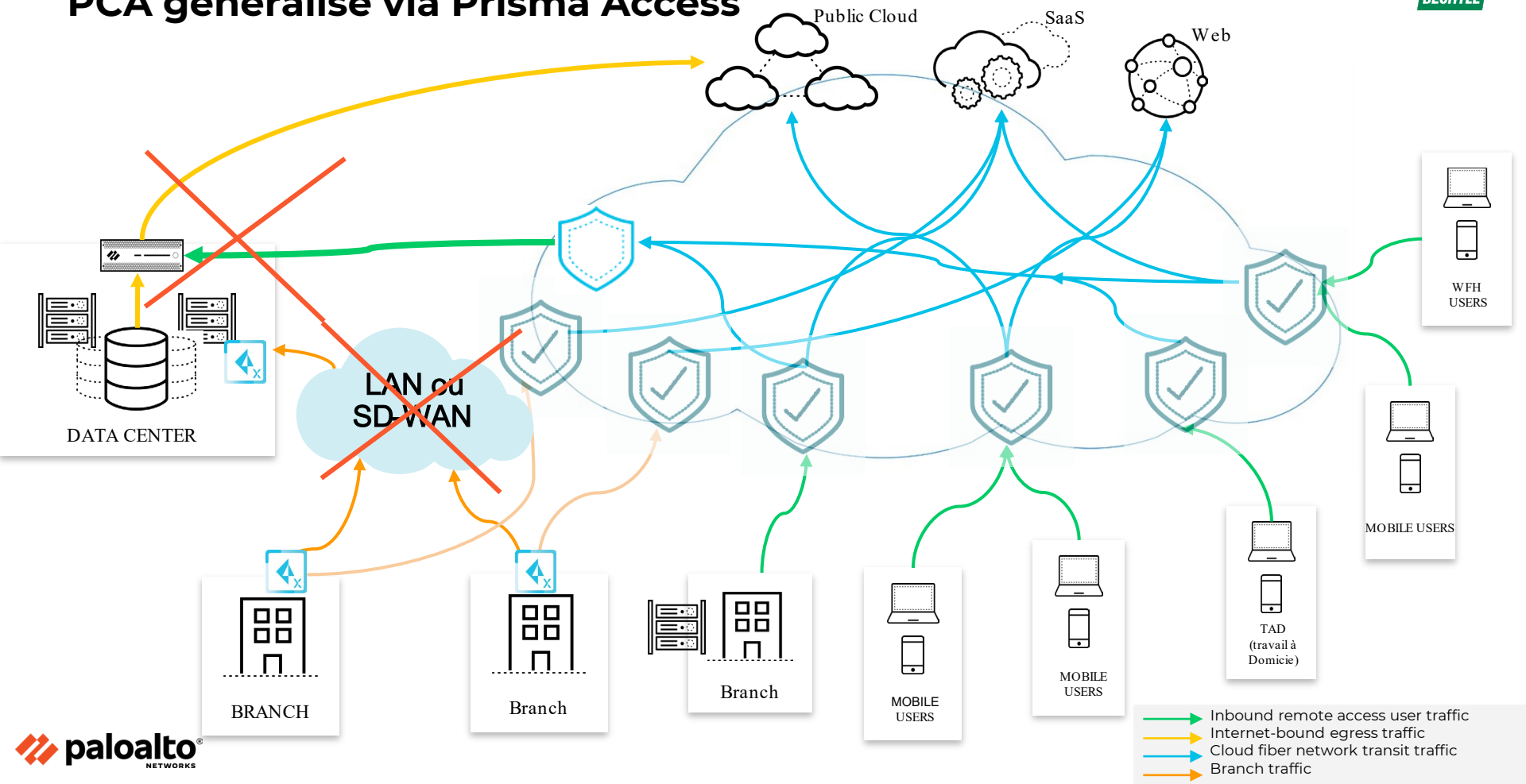
Accès sécurisé évolutif de n'importe où vers n’importe quelle application



PCA généralisé via Prisma Access



PCA généralisé via Prisma Access



1

Niveau de menace actuel

2

Cyber Résilience, qu'est-ce ?

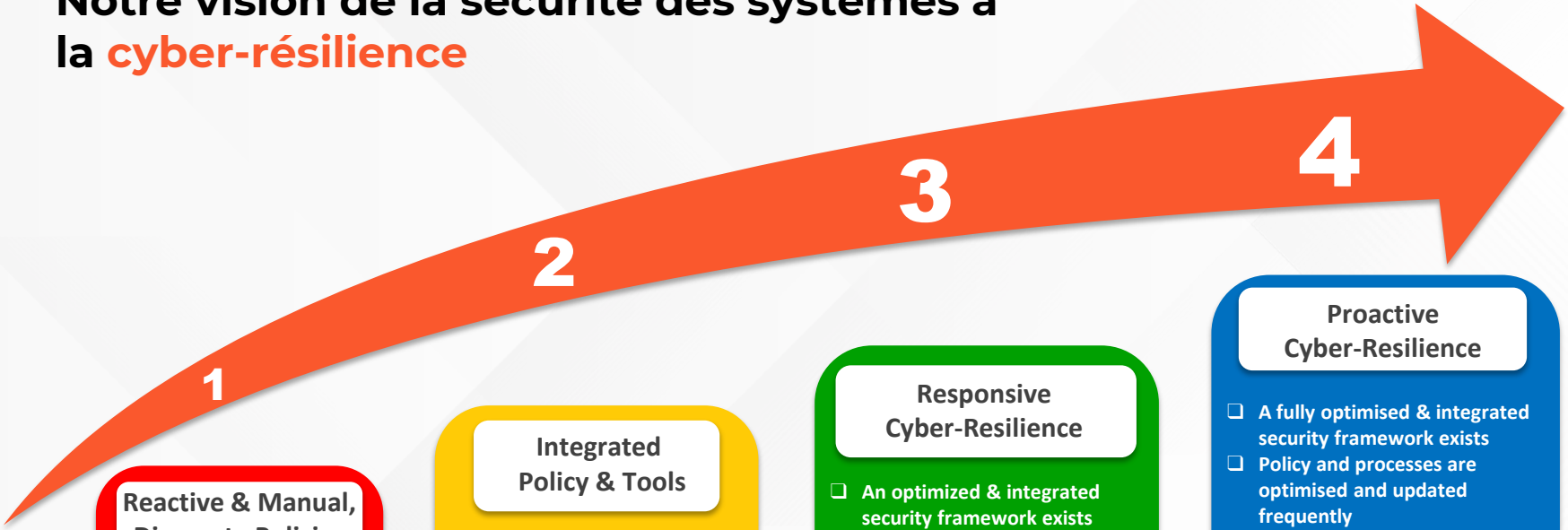
3

Cas d'usage de la cyber-résilience : Prisma Access

4

Une approche de plateformes intégrées pour la résilience

Notre vision de la sécurité des systèmes à la cyber-résilience



1 — Reactive & Manual, Disparate Policies

- ❑ Ad-hoc Responses
- ❑ Fire Fighting
- ❑ Disparate policy
- ❑ Disparate tools
- ❑ Limited processes
- ❑ Minimal security visibility

2 — Integrated Policy & Tools

- ❑ Partially integrated security framework exists
- ❑ Policies encapsulate some security requirements
- ❑ Security Framework is internally focused
- ❑ Deficiencies still exist, limited security visibility is common

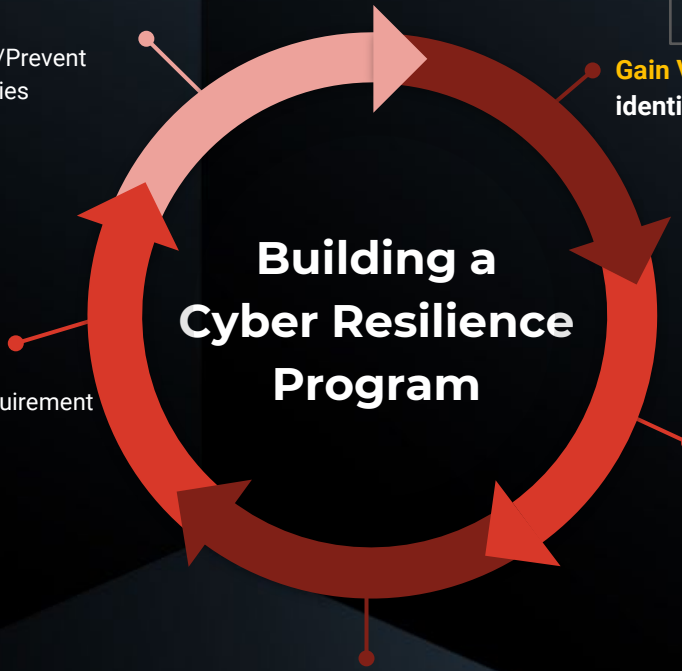
3 — Responsive Cyber-Resilience

- ❑ An optimized & integrated security framework exists
- ❑ Processes and policies include most security requirements
- ❑ Improved security visibility
- ❑ Basic cyber governance is in operation
- ❑ Capability to respond to cyber incidents exists

4 — Proactive Cyber-Resilience

- ❑ A fully optimised & integrated security framework exists
- ❑ Policy and processes are optimised and updated frequently
- ❑ Established cyber governance structure
- ❑ External & internal threat intelligence is gathered, correlated and acted upon
- ❑ Partnering in cyber ecosystems is common
- ❑ Organisation can demonstrate proactive cyber agility

Building a Cyber Resilience Program



Gain Visibility across an agile and diverse ecosystem and identify the organization's **Digital Crown Jewels**

- Expanse Attack surface MGMT
- NGFW Security Lifecycle Reviews

Leveraging Threat Intelligence assess possible business impact scenarios to crown jewels

- MDR Partners with Cortex Threat Intel Management
- Unit 42 services

From the current state, define a Cyber Transformation Roadmap

- Consolidate towards a Cybersecurity platform
- Segmentation and security controls aligned to risk - Zero Trust model
- Verify fundamental hygiene capabilities (especially the Cloud)

- Cyber Transformation Blueprint
- BVC Cyber Security Platform Assessment

Improve Response and Resilience capabilities

- SoC: Align MTTD/MTTR to the business requirement
- Ability to identify segmentation failures
- Recovery processes & Capabilities testing

- Unit 42 services
- Platform services

Continuous Improvement

- SoC telemetry of ZT & Detect/Prevent
- Testing of resilience capabilities
- Business/Exec level reporting

Merci!

Des questions? Contactez-nous: it-forum.ch@bechtle.com

Plus d‘informations :
bechtle.com