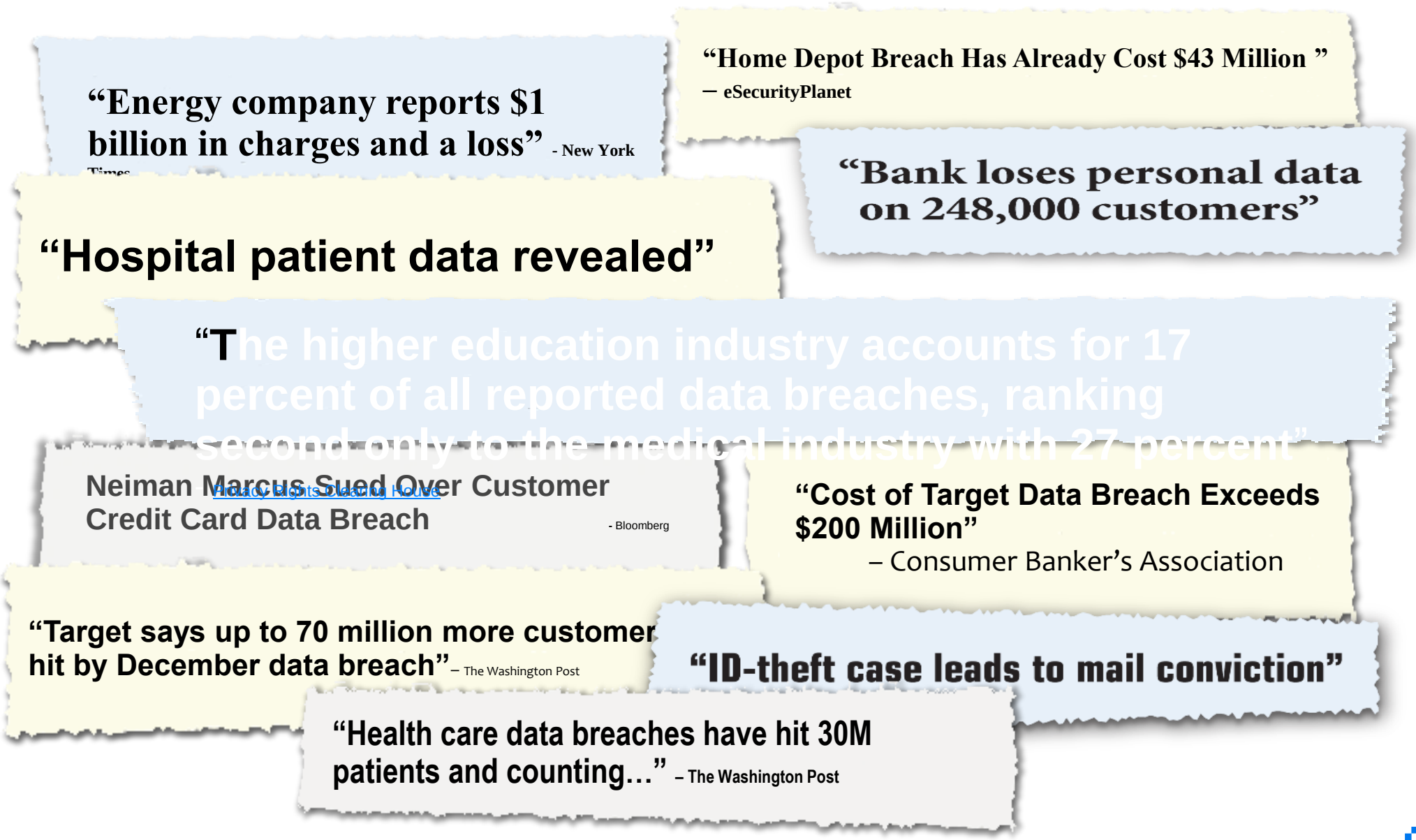
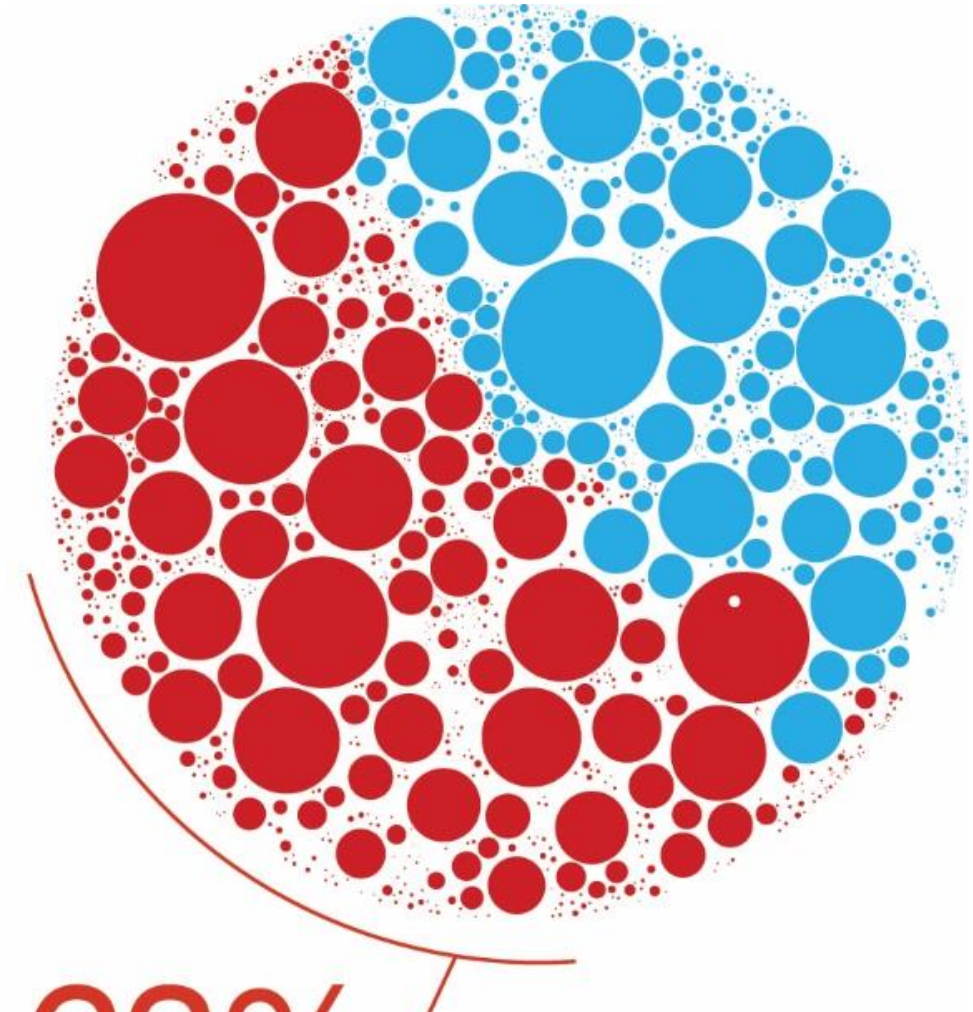
10 Actions à risque exposant votre organisation

MICRO FOCUS®


"Energy company reports $1 billion in charges and a loss" - New York Times
"Home Depot Breach Has Already Cost $43 Million "
– eSecurityPlanet
"Bank loses personal data on 248,000 customers"
"Hospital patient data revealed"
"The higher education industry accounts for 17 percent of all reported data breaches, ranking second only to the medical industry with 27 percent"
Neiman Marcus Sued Over Customer Credit Card Data Breach
- Bloomberg
Privacy Rights Clearing House
"Cost of Target Data Breach Exceeds $200 Million"
– Consumer Banker's Association
"Target says up to 70 million more customer hit by December data breach" – The Washington Post
"ID-theft case leads to mail conviction"
"Health care data breaches have hit 30M patients and counting…" – The Washington Post

Les utilisateurs sont le maillon faible de la sécurité



Source: Verizon Data Breach Investigations Report 2016

“Only **42** per cent said they were confident they could prevent fraud from their own employees.*”

*Sondage MNP LLP, février 2017

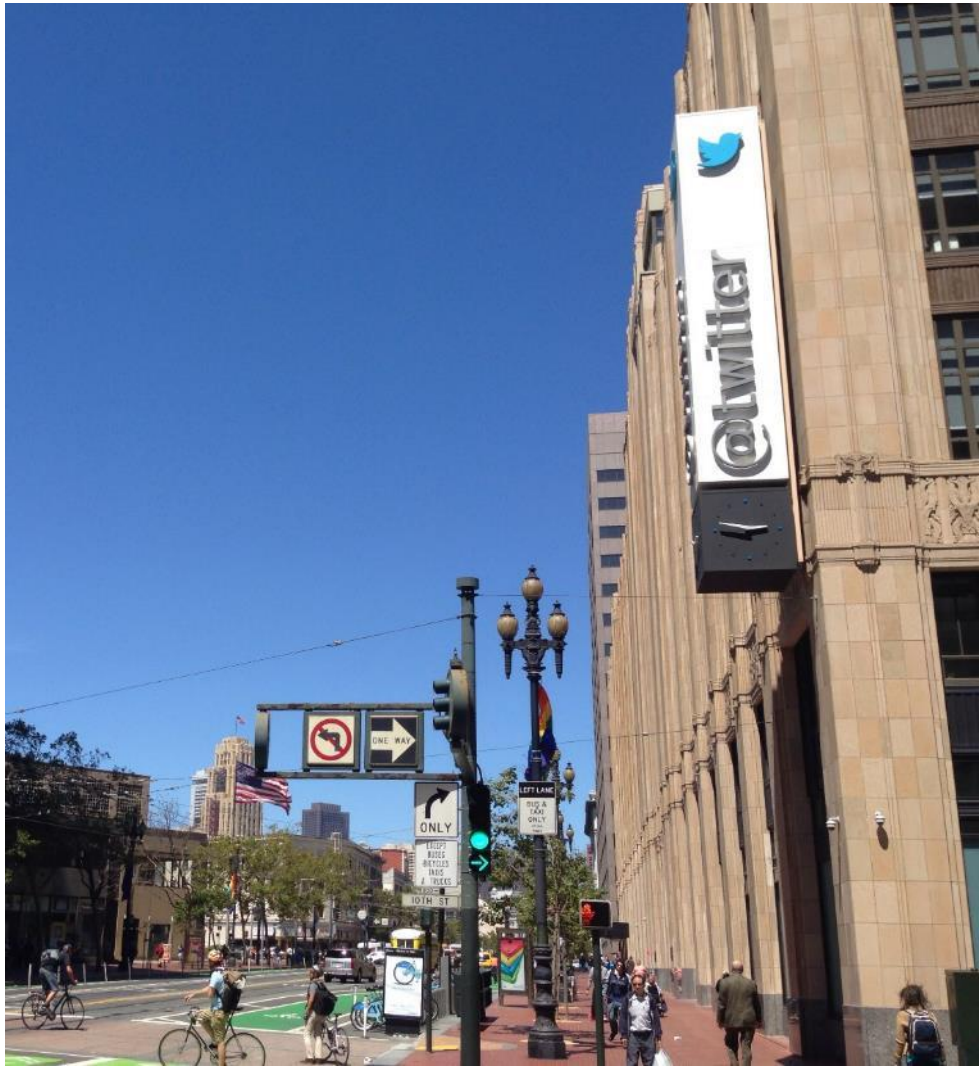
http://www.theglobeandmail.com/technology/alarming-number-of-businesses-hit-by-hackers-in-past-year-poll/article34144277/

Quels activités vos utilisateurs font-ils qui expose votre organisation?

Les actions les plus probables

1. Les Medias Sociaux

« Un quiz Facebook me demande de l’information personnelle détaillée, bien sûr que je partage avec tous mes “ami(e)s” »



Source: csoonline.com

2. Les Crédules

“Bien sûr, je vais cliquer sur ce lien. Je suis à la recherche d'un nouvel emploi.”

Source: Verizon Data Breach Digest 2016

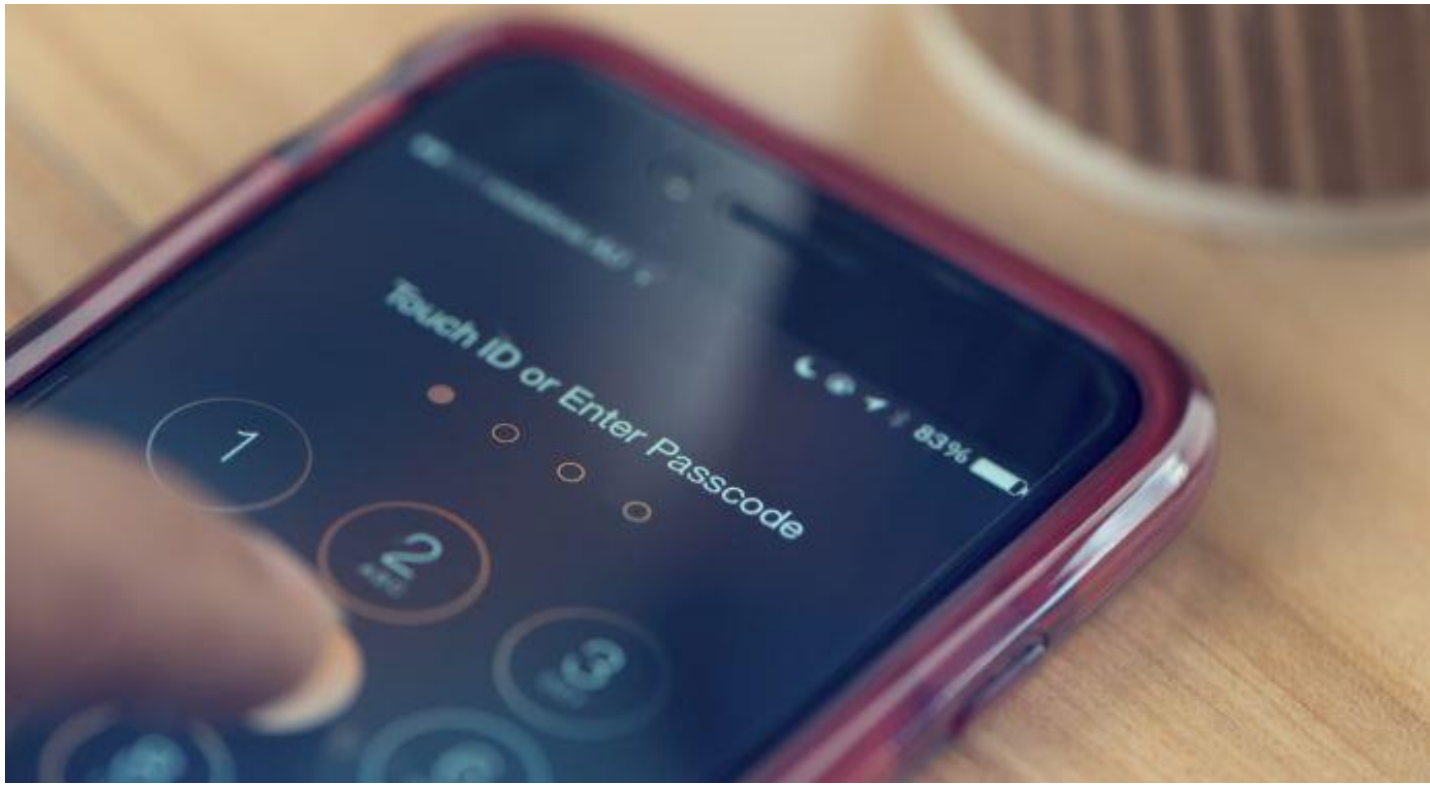
3. Les Poissons

“Le président me dit d’exécuter le transfert, donc je le fais.”

Source: cbsnews.com

4. Les Diligents

“J'ai reçu un message texte de mon fournisseur mobile me demandant un code. Le voici!”



Source: NYU

5. Les bons Samaritains

“Elle a dit avoir oublié sa carte à la maison.”

6. Les Post-It

“Nous avons utilisé 'azerty12345' comme mot de passe. Puis, après avoir été piratés, nous sommes allés à la télévision et avons montré d'autres mots de passe sur des Post-it.”

Source: arstechnica.com

7. Les Clés USB

“J'ai reçu une clé USB dans le courrier. Elle était étiquetée avec le logo d’un fournisseur, alors je l’ai insérée dans mon ordinateur.”

Source: Verizon Data Breach Digest 2016

Les actions les plus dangereuses

8. Les “Outsourcing”

“Pourquoi travailler, quand je peux jouer?”

Source: Verizon Data Breach Digest 2016

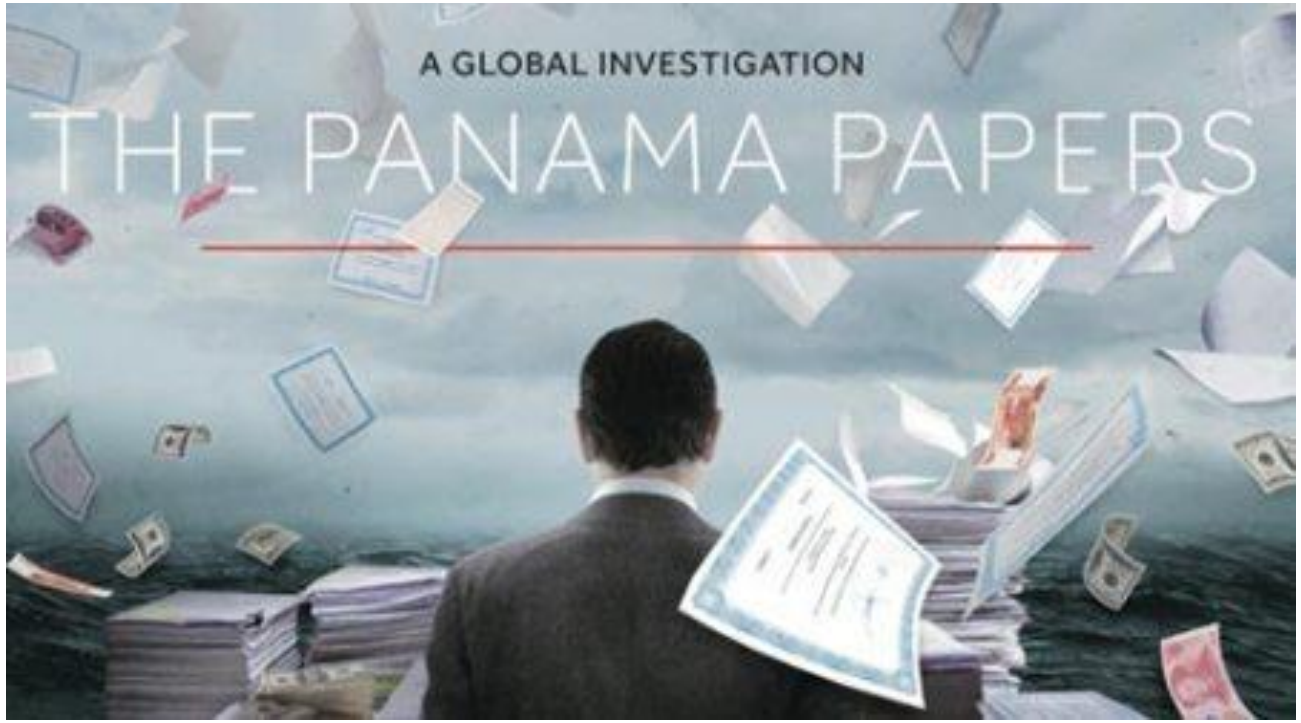
9. Les “Insiders” (initiés)

“Trois employés ont secrètement installé un logiciel sur le réseau du fournisseur de services cellulaires de sorte qu’un service de déverrouillage pouvait recevoir des centaines de milliers de demandes pour supprimer les verrous sur les téléphones.”

Source: PCWorld.com

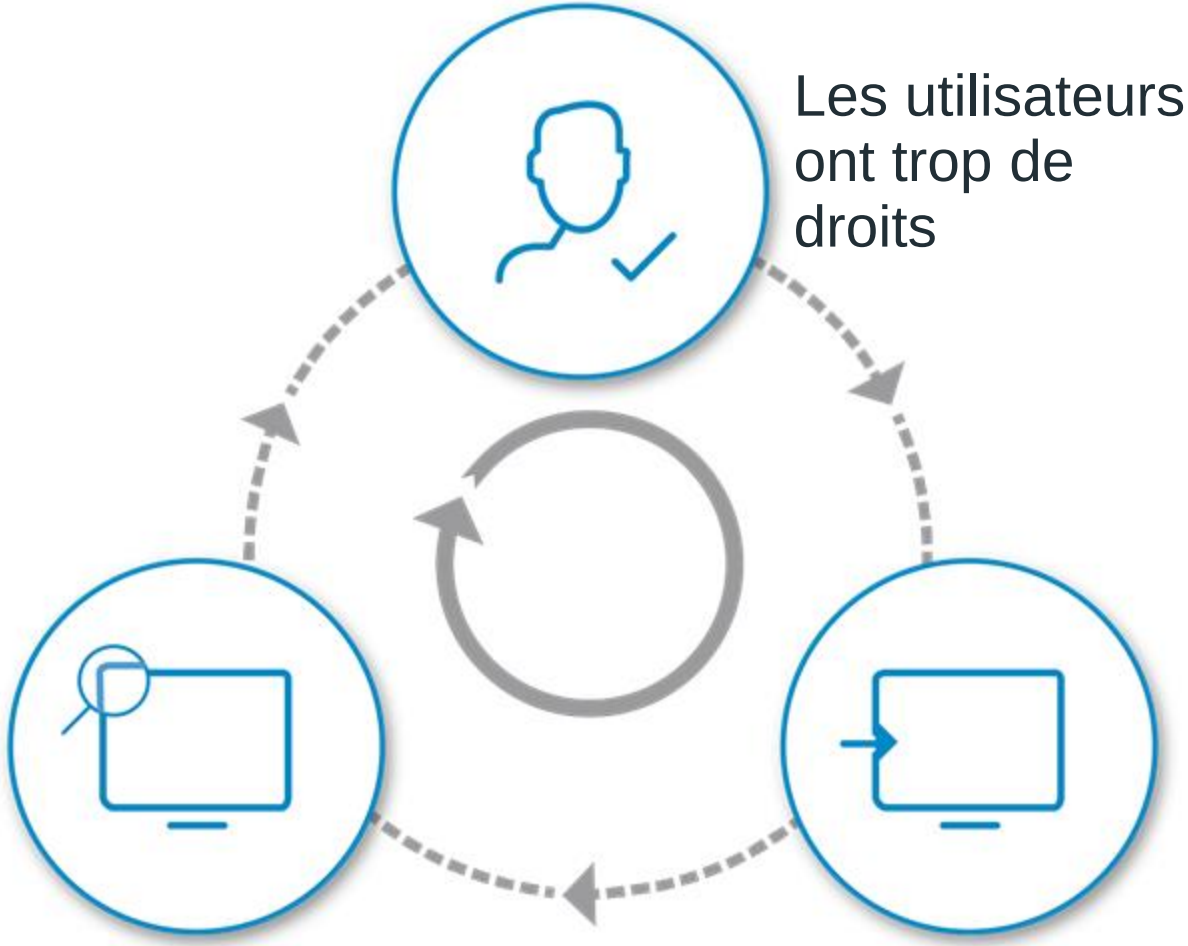
10. Les Hacktivistes

«Un spécialiste de TI au bureau de Mossack Fonseca à Genève a été arrêté par les autorités, a rapporté le journal Suisse Le Temps."



Source: USAToday.com

Quels sont les éléments communs?

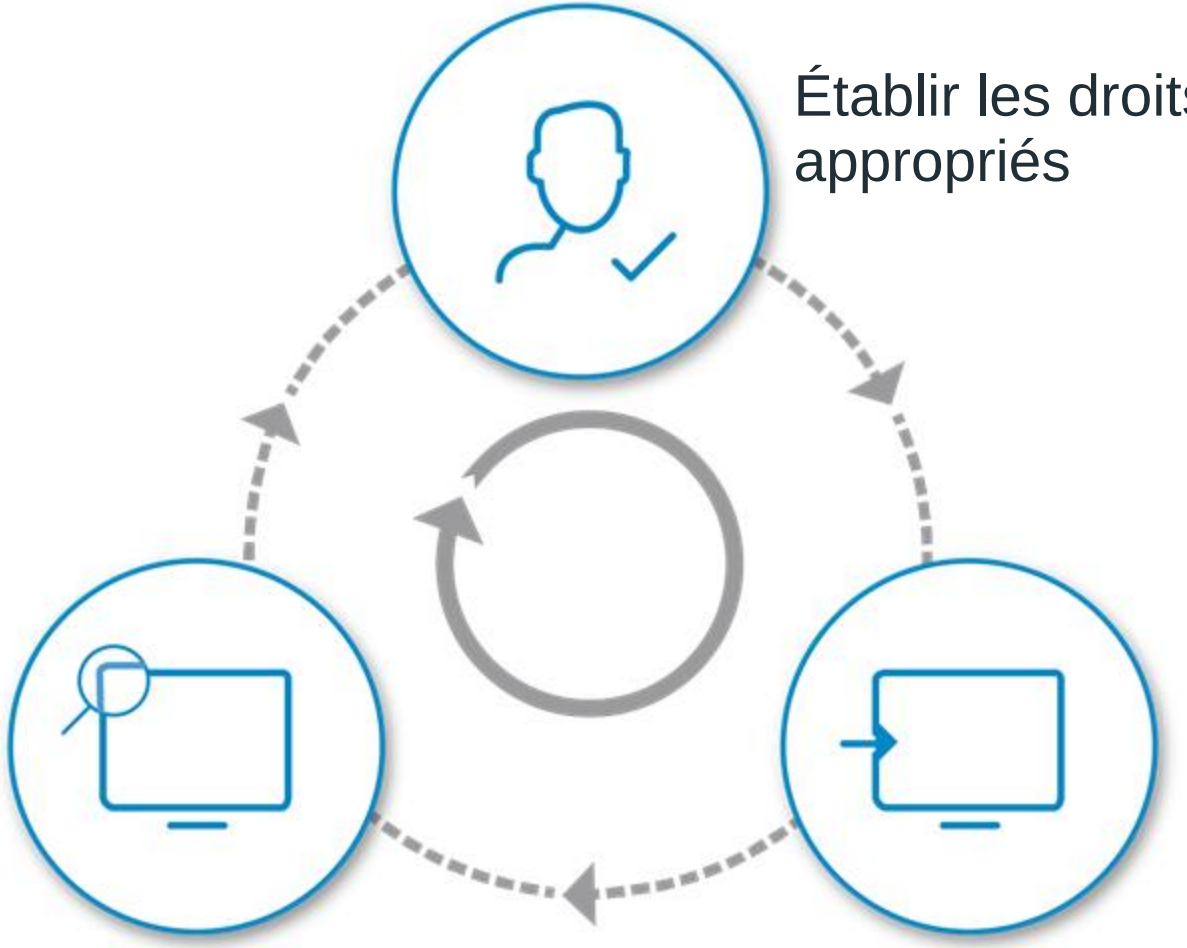


Les utilisateurs ont trop de droits

Les accès sont non gérés ou non contrôlés

Les activités des utilisateurs sont peu, ou pas supervisées

L'approche Micro Focus

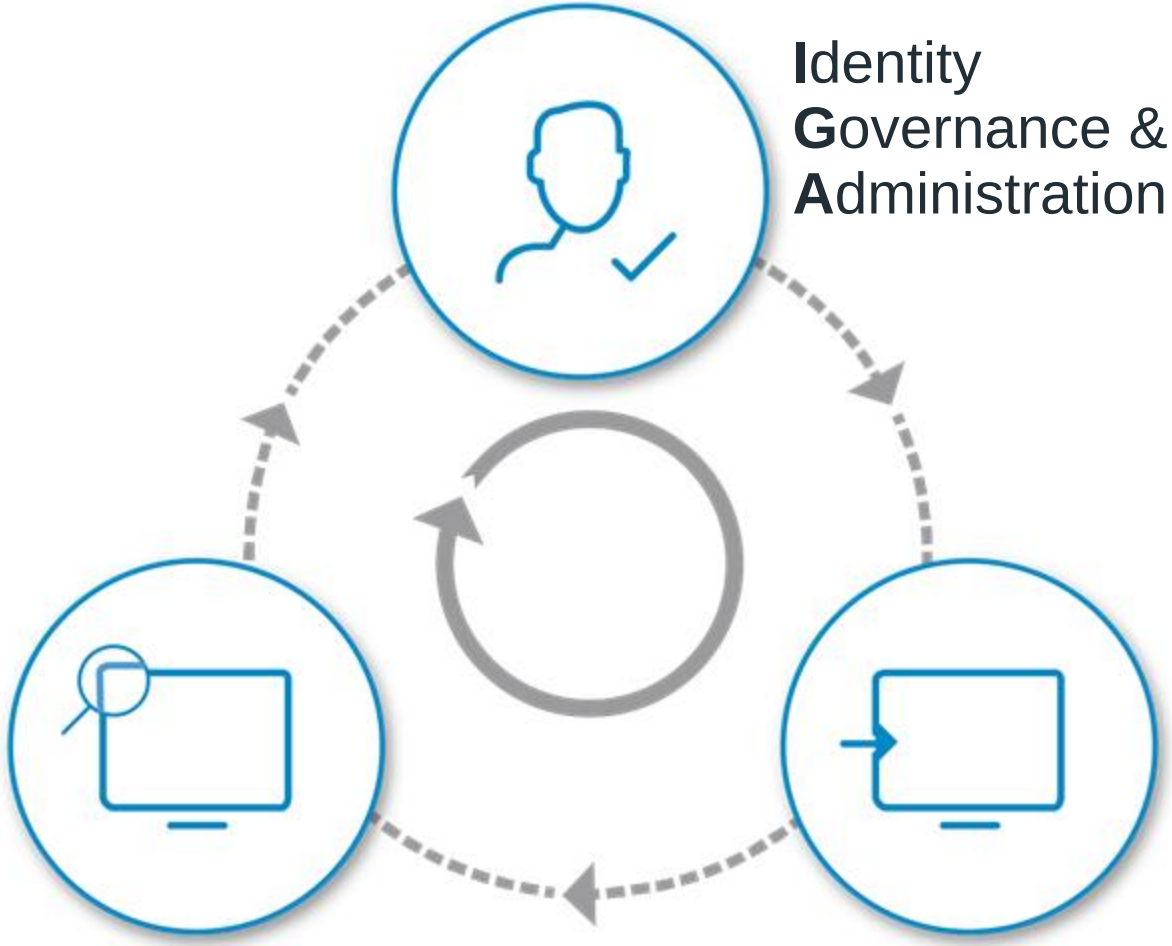


Établir les droits appropriés

Appliquer les contrôles d'accès

Superviser les activités des utilisateurs

L'approche Micro Focus



Identity
Governance &
Administration

Access
Management &
Authentication

Secure
User
Monitoring

Qui est Micro Focus?

90+

Bureaux Mondial

4,500+

Employés

$1.3bn+

Revenu Annuel

20,000+

Clients

5,000+

Partenaires

Micro Focus

Bannière Combinée

Attachmate	NetIQ	Novell	SUSE	Borland	MICRO FOCUS
Host Connectivity	Systems Management	Collaboration	Enterprise Linux Servers	Test Automation & Management	Enterprise Application Management
Enterprise Security & File Transfer	Identity, Security, & Compliance	File and Networking Services	Software Appliances	Requirements Management	COBOL Development & Deployment
Legacy Modernization	Resource Management	Endpoint Management	Linux Desktops	Change & Configuration Management	Interoperability Solutions (CORBA)
Seattle, WA	Houston, TX	Provo, UT	Nuremberg, Germany	Rockville, MD	Newbury, Berkshire UK

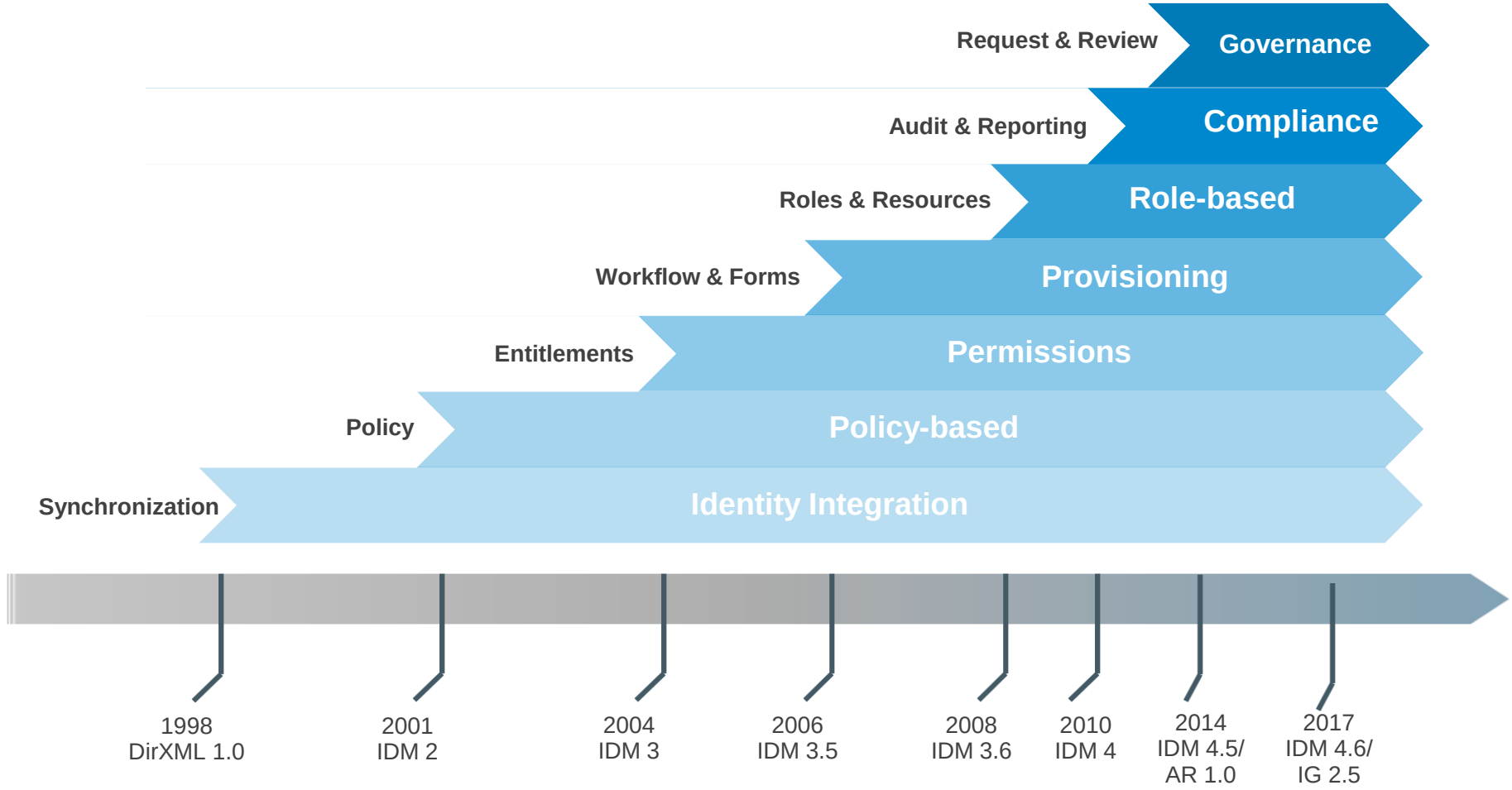
MICRO FOCUS

GESTION IDENTITÉ ET GOUVERNANCE (IGA)

Gestion de l’Identité et Gouvernance

Appliquer le principe du moindre privilège

L’évolution de IDM



Capacités Critiques d’une Solution GIA

- Access certification
- Reporting and analytics
- Identity life cycle
- Fulfillment
- Access requests
- Role and policy management
- Workflow orchestration
- Password Management
- Auditing
- Risk Management

Extended IGA

- Privileged Account Management
- Advanced Multifactor Authentication
- Access Management / SSO
- User Self-Service
- Security and Event Monitoring

Solution GIA Micro Focus

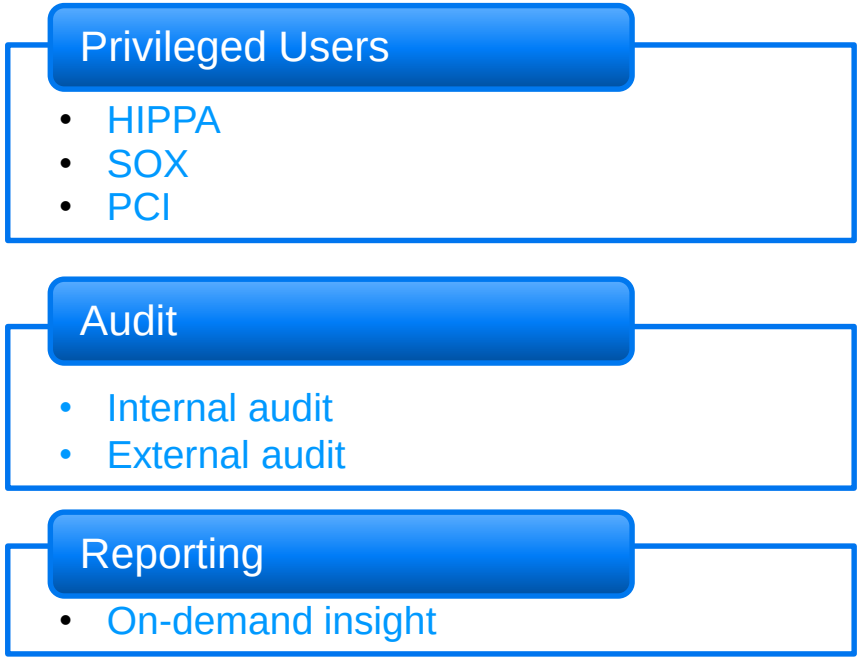
Résoudre les défis d’entreprise

- Gérer et atténuer les risques

Solution GIA Micro Focus

Résoudre les défis d’entreprise

- Gérer et atténuer les risques
- Maintenir la conformité



Solution GIA Micro Focus

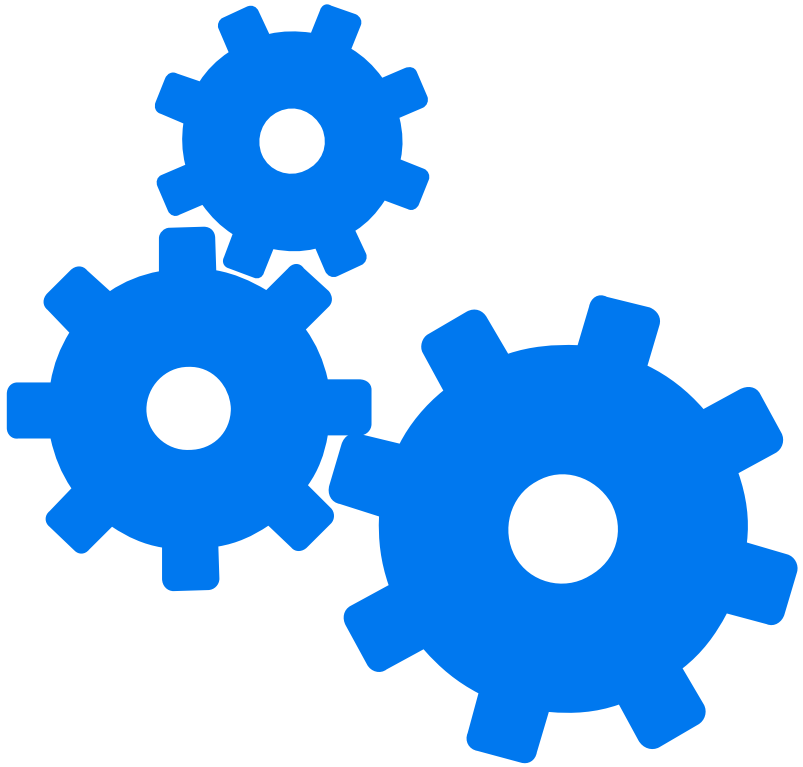
Résoudre les défis d’entreprise

- Gérer et atténuer les risques
- Maintenir la conformité
- Aider la productivité

Solution GIA Micro Focus

Résoudre les défis d’entreprise

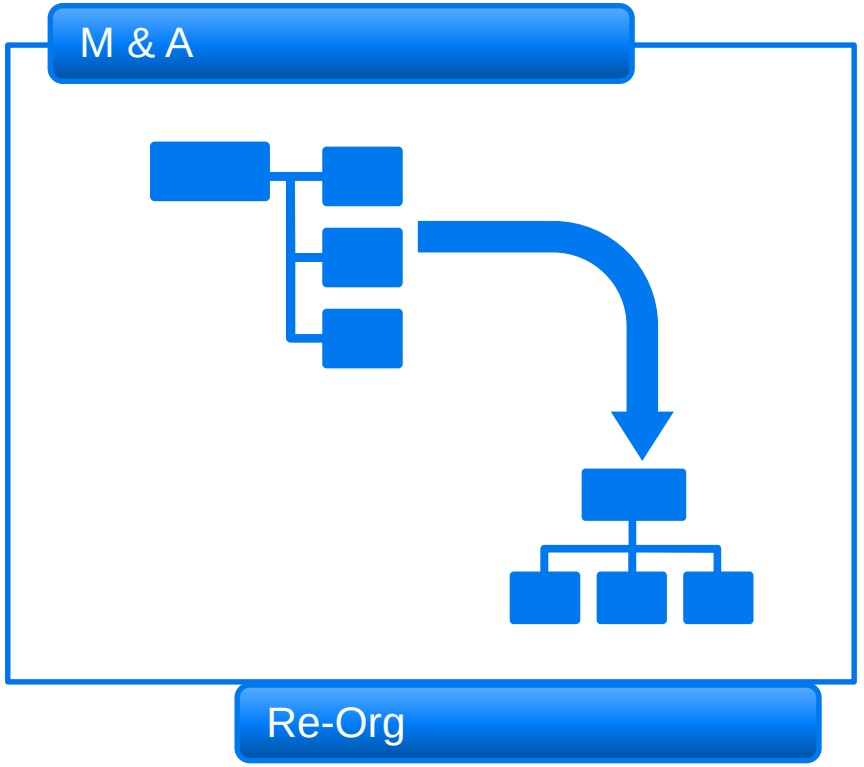
- Gérer et atténuer les risques
- Maintenir la conformité
- Aider la productivité
- Atteindre une efficacité opérationnelle



Solution GIA Micro Focus

Résoudre les défis d’entreprise

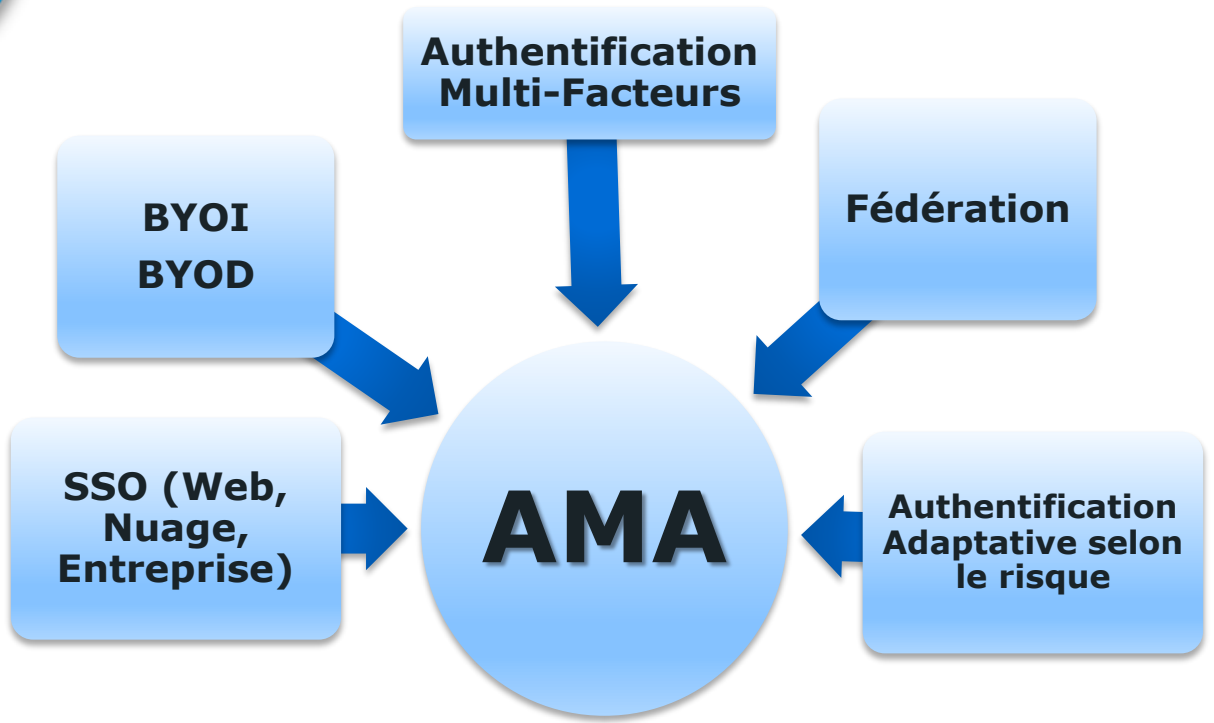
- Gérer et atténuer les risques
- Maintenir la conformité
- Aider la productivité
- Atteindre une efficacité opérationnelle
- Adapter au changement



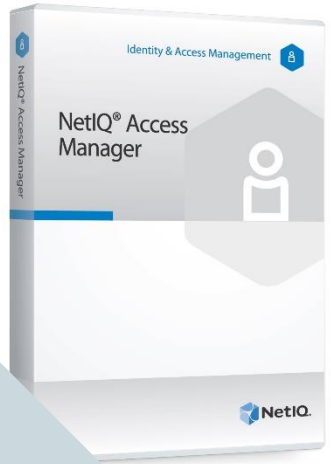
GESTION ACCÈS ET AUTHENTIFICATION (AMA)

Gestion Accès et Authentification

Sécurisée les accès



L’évolution de Access Manager



1999-2000
- **iChain**
- 32 bit architecture
- Web SSO

2008
- **Access Manager 3.0**
- 32 bit architecture
- Web SSO
- SAML and Federation

2010
- **Access Manager 3.1**
- 32 bit architecture
- SAML and Federation
- Flexible deployment

2012
- **Access Manager 3.2**
- 64 bit architecture
- Scaling and performance
- New appliance model

2013
- **Access Manager 4.0**
- Code Promotion
- Social Login
- Secure Token Service
- Federation Wizards

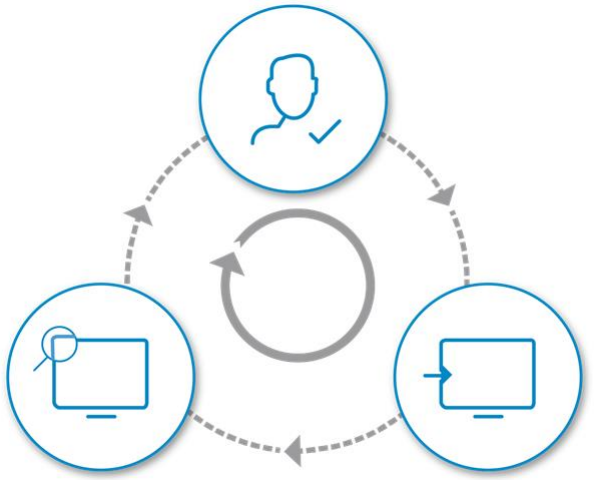
2015
- **Access Manager 4.1**
- Risk based authentication
- OAuth/OpenID Connect
- REST APIs

2015
- **Access Manager 4.2**
- Improved user experience
- Landing page
- Improved administration

2016
- **Access Manager 4.3**
- Mobile Access integration
- SaaS application catalogue
- Access analytics

Ce qui rend Micro Focus unique

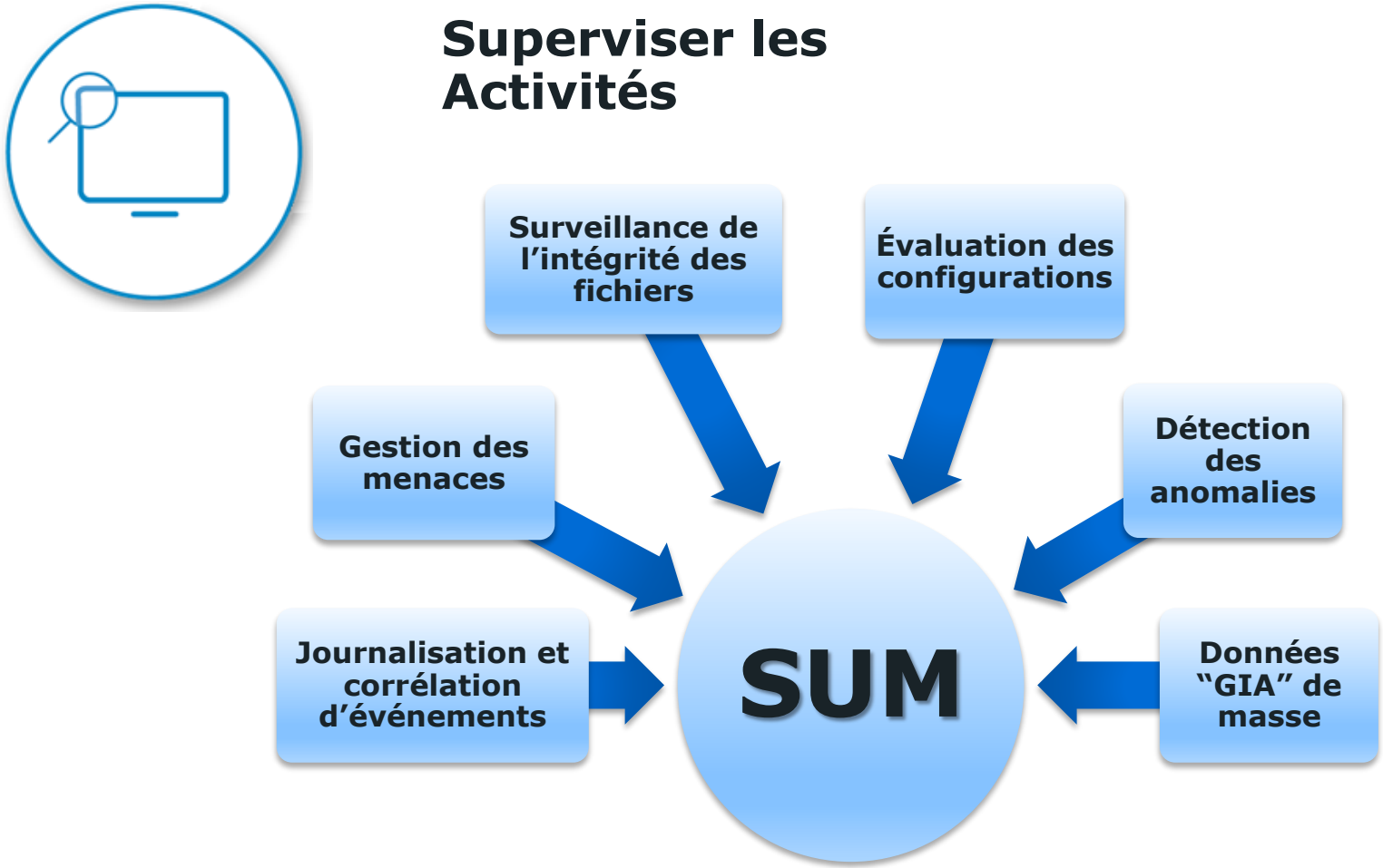
- **Adaptatif,** l'accès basé sur le risque rend l'authentification aussi simple que possible pour les utilisateurs
- **Augmentation** des accès privilégiés lorsque le risque en indique le besoin
- Lier une authentification **multi-facteurs** à une augmentation de privilèges pour réduire davantage les risques d'abus d'identification



SUPERVISION SÉCURISÉE DES UTILISATEURS (SUM)

Supervision sécurisée des utilisateurs

Analytiques - Identifier les comportements anormaux



Surveillance des activités

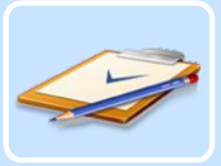
Questions clés

Quelles (quoi) modifications ont été apportées?

Quand les modifications ont été exécutées?

Qui a effectué les modifications?

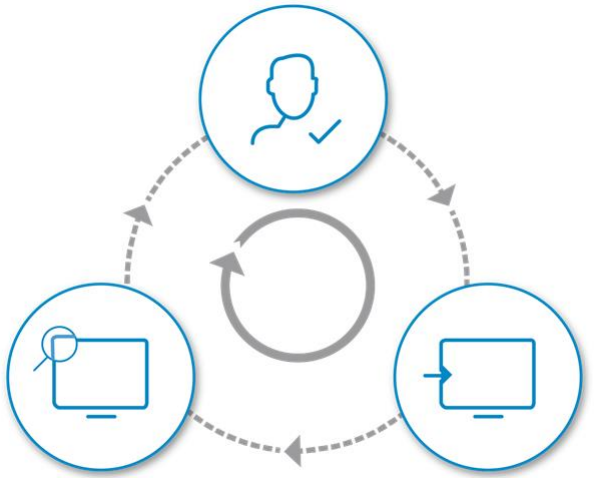
D'Où proviennent les modification?



Est-ce-que les modifications étaient **autorisées**?

Ce qui rend Micro Focus unique

- **Statistiques** des accès– Savoir ce que font les utilisateurs avec leurs accès
- **Supervision** de l'activité des utilisateurs en temps réel et déclenchement automatisé d'activités
- **Identifier** les "choses" sur le réseau pour la sécurité des "IoT"



ANALYTIQUES

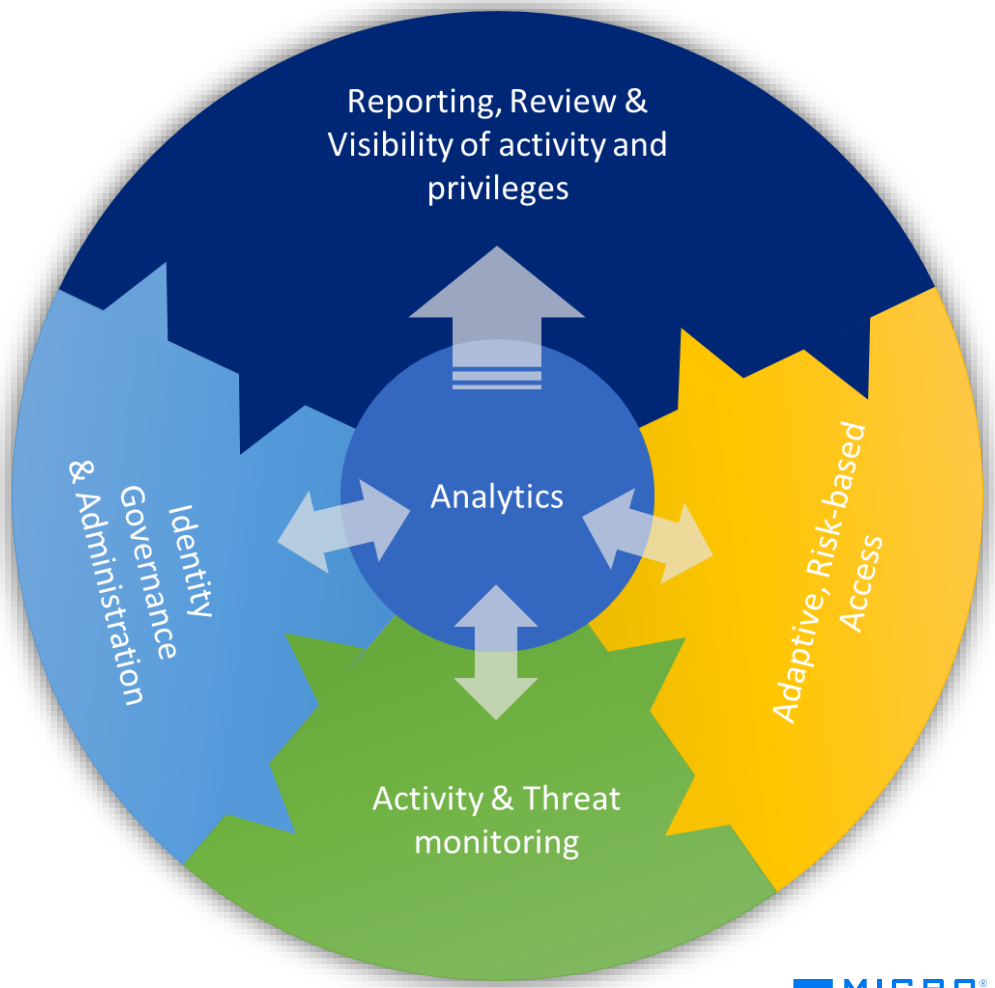
MICRO FOCUS

L’automatisation et l’efficacité
ne suffisent plus:
nous devons intégrer
l’**Intelligence** de l’**Identité**

MICRO FOCUS

Analytiques

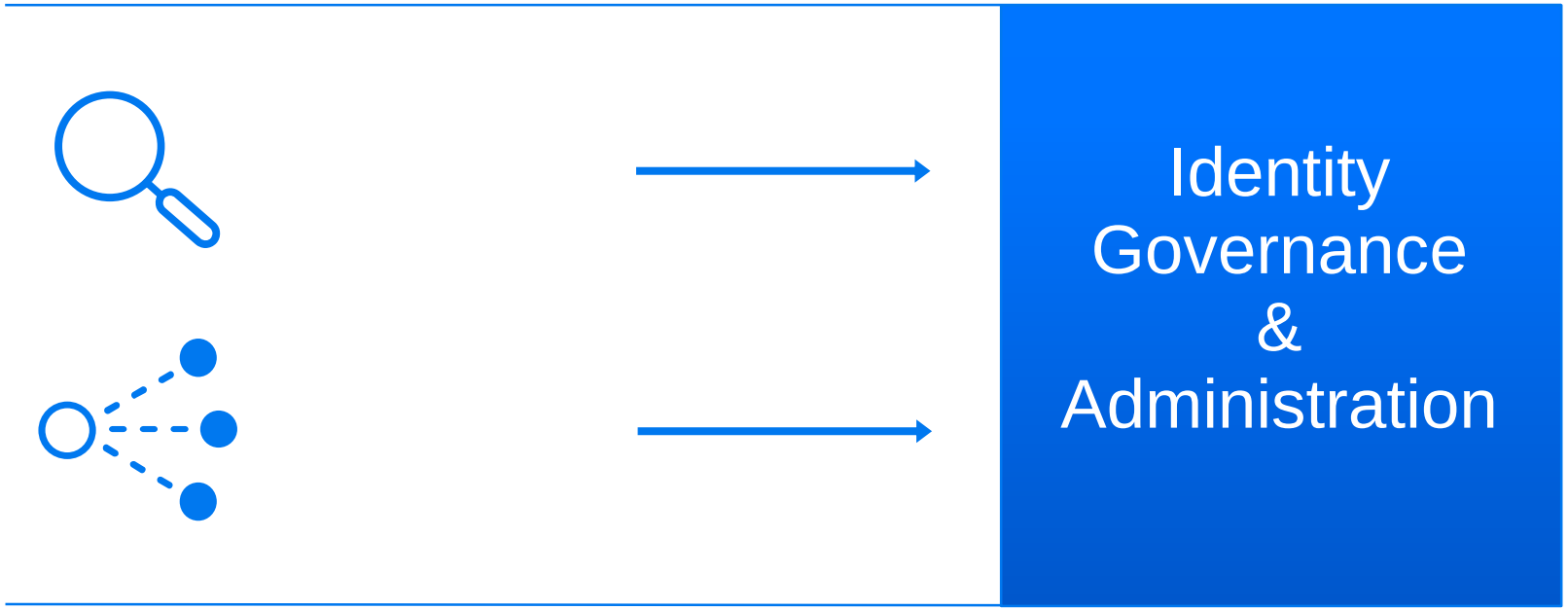
- **Exploiter** les données de tous les produits et applications
- **Produire** un aperçu de l'état de la sécurité basé sur l'intelligence de l'identité
- **Partager** l'analytique avec tous les produits et applications



Si les utilisateurs sont un problème de sécurité, quel rôle prend votre **GIA?**

MICRO FOCUS

Gouvernance de l’Identité



User provisioning allowed identities to be tied to accounts and coordinated coarse-grained account life cycles with global identity life cycles. Access governance pierced the veil of accounts to reveal the entitlements that represent the privileges that users actually possess. – Gartner*

*Iverson, Brian. “Identity Governance and Administration: How We Got Here” Gartner Blog Network, March 5, 2015

Authentification avancée

FIDO U2F	PIN Code	Live Ensure	Voice Bio	Soft Token	Emergency
HSM	Challenge	NFC	Face Biometric	Hard Token	LDAP Password
SMS	Fingerprint	RFID	Email OTP	Smartphone	
Voice Call	LDAP	PKI			

Gestion des Accès Privilégié

Nos solutions permettent de gérer les accès d'utilisateurs privilégiés; pour les accès serveurs, applicatifs, ainsi que les accès aux systèmes de fichiers.

Nous aidons à réduire les risques de:

- Trop d'administrateurs
- Mots de passe partagés des comptes "root"
- Augmentation des privilèges non géré
- Incapacité à déléguer des privilèges granulaires
- Absence de politiques d'accès centralisées
- Manque de visibilité sur les droits d'accès
- Incapacité à démontrer la conformité avec les privilèges nécessaires

Mark Bell
Directrice des Comptes
Mark.Bell@microfocus.com

Patrick Schneider
Ingénieur des ventes
Patrick.Schneider@microfocus.com

Merci

www.microfocus.com