DriveLock

HYPERSECURE IT

www.query-informatique.com

DriveLock

HYPERSECURE IT

Avec la plateforme HYPERSECURE de DriveLock,
les attaques contre les systèmes informatiques
restent là où elles doivent être : à l'extérieur !

DriveLock

- Plus de 20 ans sur le marché
- Solution primée et certifiée
- De la PME à l'entreprise
- Une plateforme, une console, un agent
- Cloud et On-Premise
- Focus : Satisfaction client
- Efficace, rentable, et à jour sur simple pression d'un bouton

ISG Provider Lens 2022 Quadrant – Cybersecurity – Solutions & Services – Data Leakage/Loss Prevention (DLP) and Data Security – Leader, Germany

SecurITy made in EU – Trust Seal www.teletrust.de/itsmie

techconsult PUR 2022 – CHAMPION – ENDPOINT PROTECTION – SECURITY SOLUTIONS

SecurITy made in Germany – Trust Seal www.teletrust.de/itsmig

Les défis de la cybersécurité

01
10

Numérisation

Pénurie de main d'œuvre qualifiée

Lois et règlementations

Cybercriminalité


DriveLock
Bloquez la réaction en chaîne
Prévenir plutôt que de devoir intervenir

DriveLock

Ralentissez les attaques, anticipez-les, et rendez-les aussi coûteuses que possible pour les attaquants !

ISO 27001 | NIST | NIS2 | BSI | CIS | CMMC

Risque et conformité

Contrôle des périphériques

Filtrage des applications

Solutions de chiffrement

Gestion des vulnérabilités

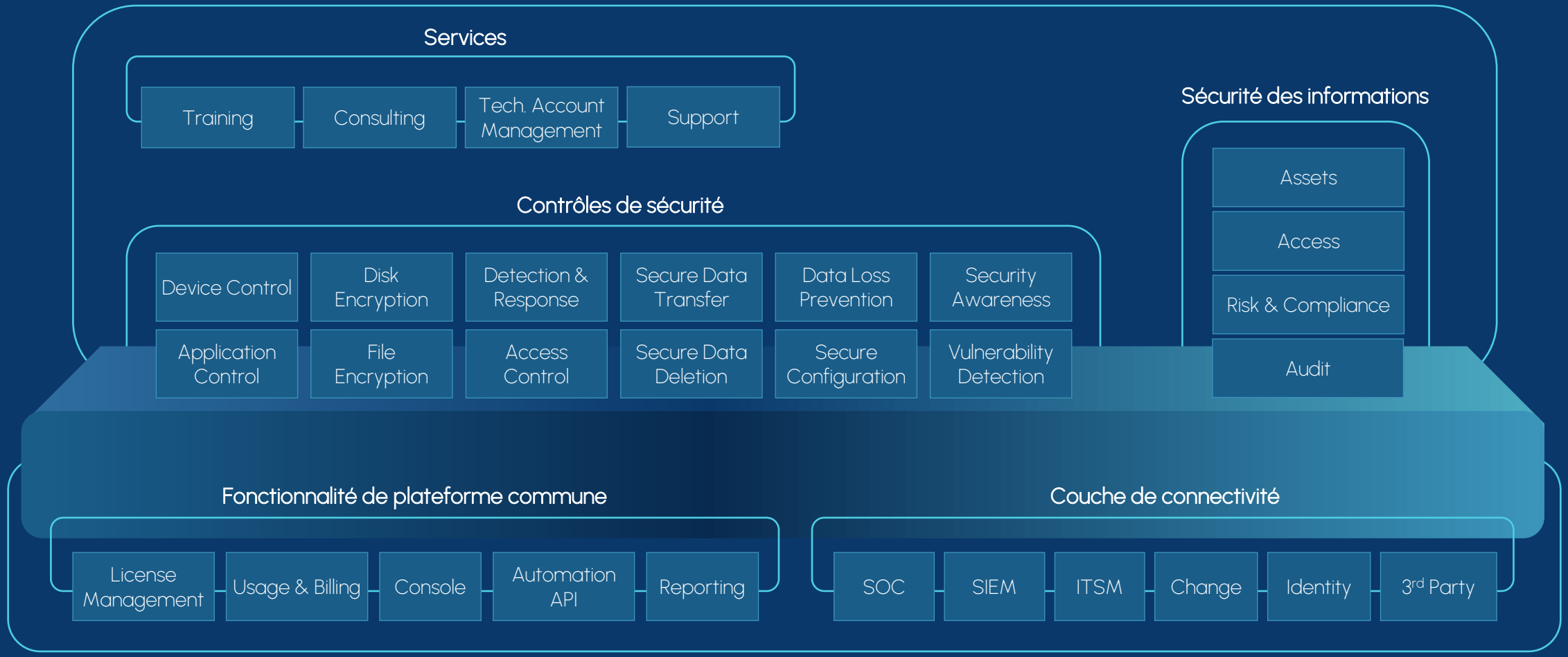
Gestion des configurations de sécurité

Sensibilisation à la sécurité

Anti-Malware

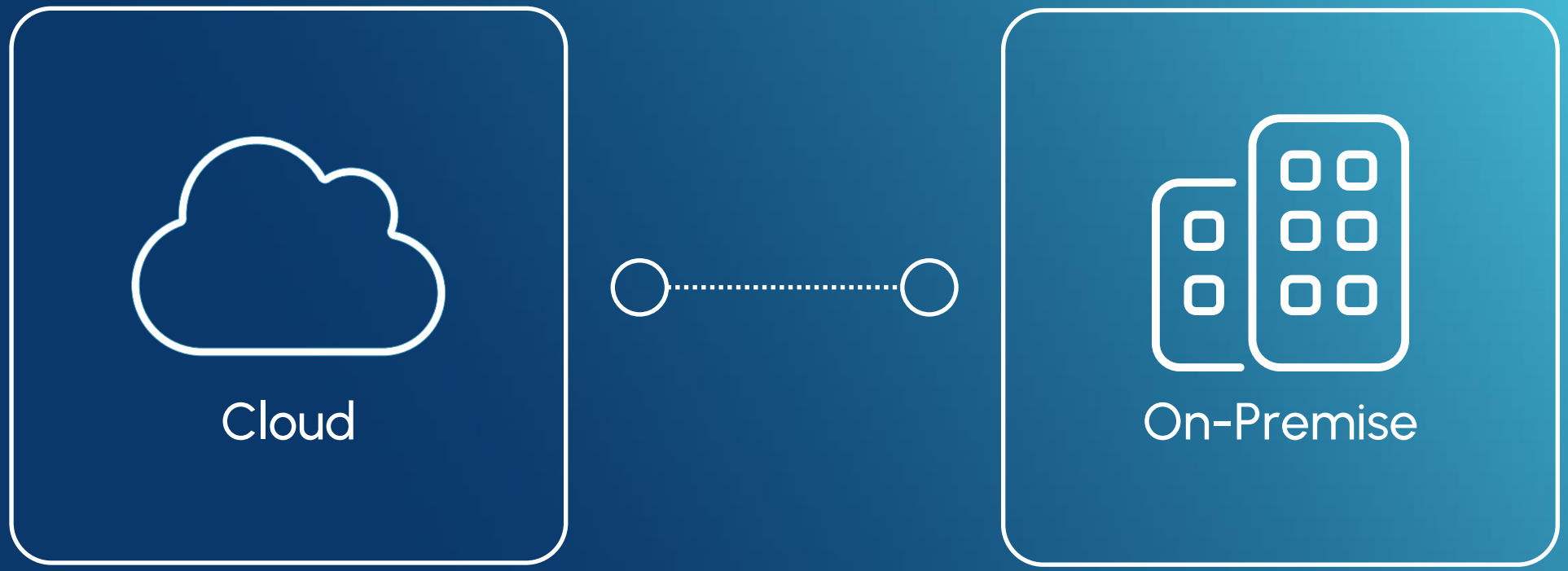
Gouvernance des données

La plateforme HYPERSECURE



Ouvert Intégré Automatisé Extensible Standardisé Stratégique

Modèles de déploiement



Protection basée sur le Cloud

La confiance est basée sur la sécurité, la protection des données et la conformité.

- Focus sur la sécurité
- Déploiement rapide
- Toujours à jour
- Aucun frais de migration ou de mise à jour
- Basculement et évolutivité
- Aucune dépendance

Données stockées dans le cloud

- Profils de sécurité
- Données de télémétrie

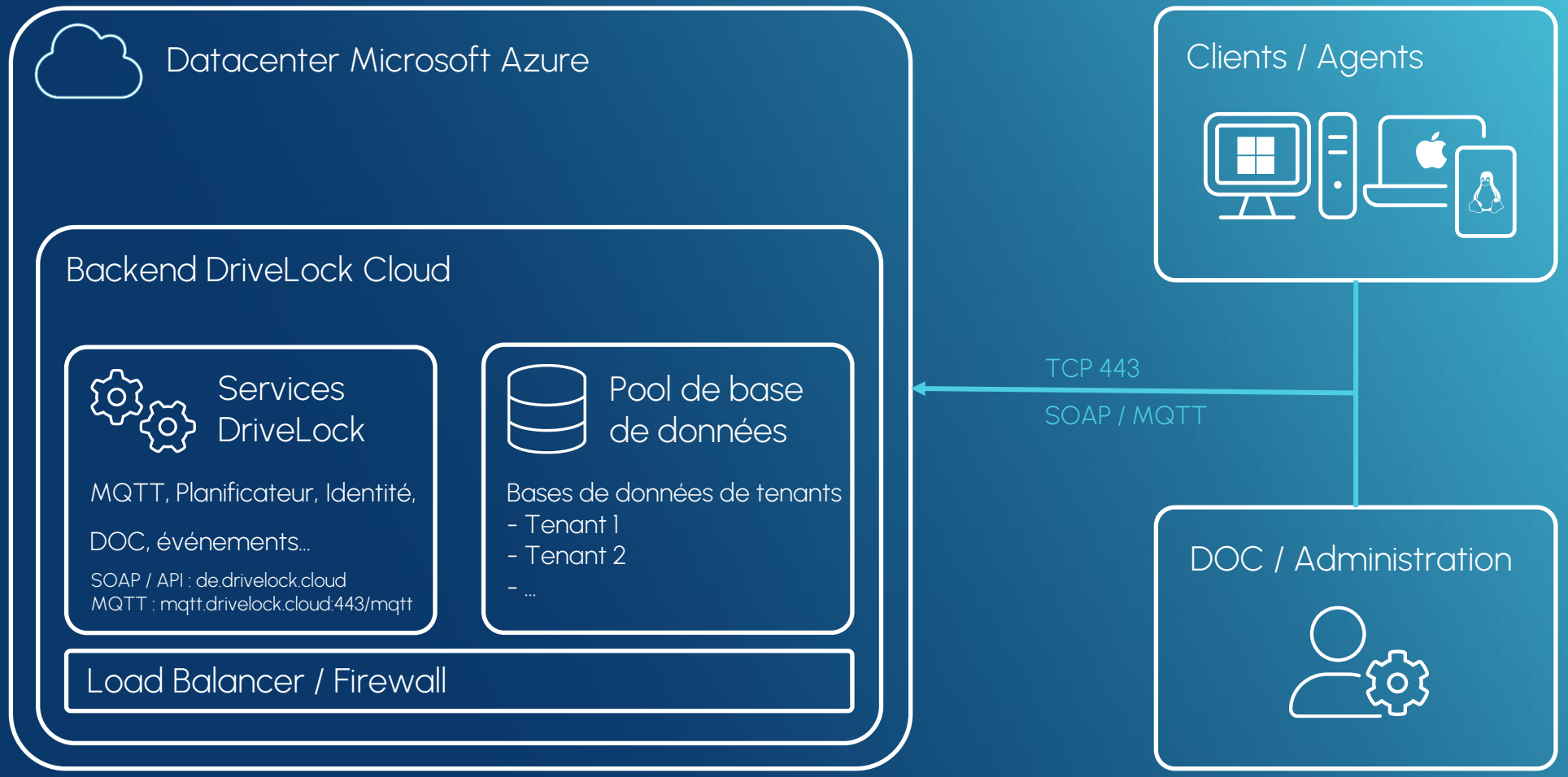
DriveLock et fournisseur Cloud

- Des partenaires solides
- Réglementations RGPD et BSI

Emplacements des datacenters

- DACH (France)
- Europe, USA, APAC

Architecture Cloud



DriveLock

Christophe MULLER@QI-Demo

en

- Dashboard
- Security Controls
  - Drives
  - Devices
  - Applications
  - Encryption
  - Antivirus
  - Awareness
  - Vulnerabilities
- Inventory
- Analytics
- Administration

Standard | Applications | Devices | Alerts | Awareness | Antivirus | Vulnerabilities | Rollout

Current state of the agents

Current	Unknown (>3w)	Need attention	Critical
5,496	1	1,905	0
74.25% of 7,402	0.01% of 7,402	25.74% of 7,402	0% of 7,402

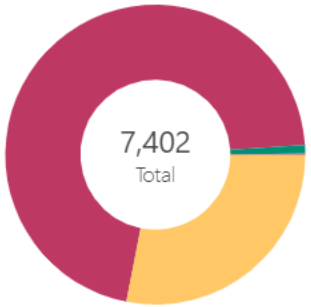
Unlock status and heartbeat

Temporarily unlocked	Heartbeat (<1h)
8	0
0.11% of 7,402	0% of 7,402

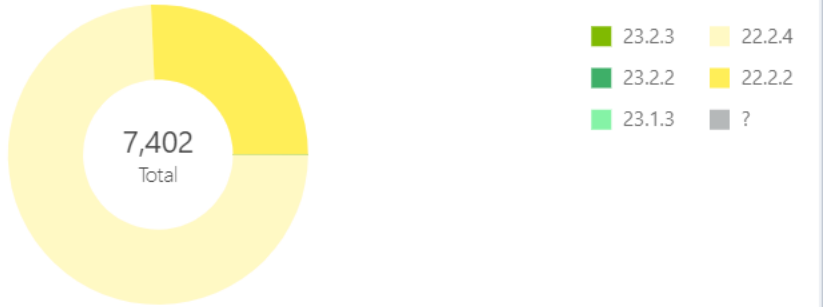
Latest significant events

Pre-boot authentication issues (<1w)	Agent registration issues (<1w)	Latest significant drive events (<1w)	Latest significant device events (<1w)	Latest significant AC events
0	0	7	6	7

Agents by OS

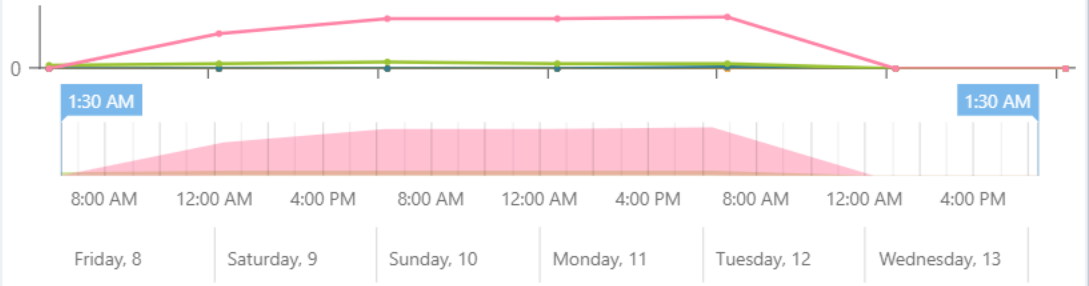


Agent versions



Events by type (within 48h)

Events history



Contrôle des lecteurs et des appareils

Surveiller, limiter, réguler, protéger

- Qu'est-ce qui peut être connecté ?
- Que peut-on copier ?
- Quelles données doivent être chiffrées ?
- Y a-t-il des malwares sur les clés USB ?
- Les données peuvent-elles être transférées via Bluetooth ?

Contrôle des lecteurs internes et externes, des appareils et des smartphones

Protection contre le vol de données et les logiciels malveillants via des supports de stockage amovibles

Visibilité sur l'utilisation des lecteurs et des appareils, ainsi que sur les transferts de fichiers

DriveLock

Christophe MULLER@QI-Demo

en

- Dashboard
- Security Controls
  - Drives
  - Devices
  - Applications
  - Encryption
  - Antivirus
  - Awareness
  - Vulnerabilities
- Inventory
- Analytics
- Administration

Standard | Applications | Devices | Alerts | Awareness | Antivirus | Vulnerabilities | Rollout

Agents with Device Control

7,399

Temporarily unlocked

8

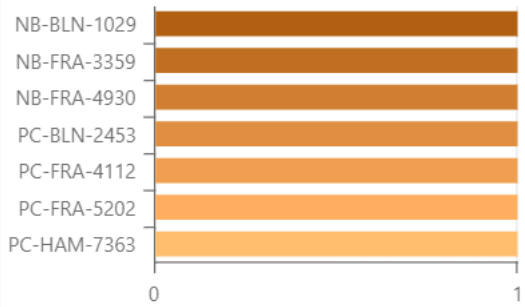
Latest significant drive events (<1w)

-

Latest significant device events (<1w)

-

Blocked drives by computer (<1w)



Files transferred by computer (<1w)

No data available!

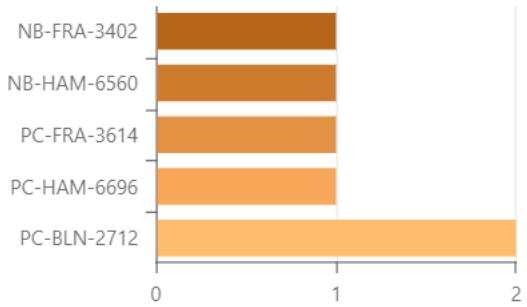
Please modify the filter or check your data repository

Blocked files by computer (<1w)

No data available!

Please modify the filter or check your data repository

Blocked devices by computer (<1w)



New drives (<4w)

Vendor ID	Product ID	Storage ty	Created at
JetFlash	Transcend 16GB	Removable	2/26/2024, 4:25:20 PM
Generic	Flash Disk	Removable	2/25/2024, 6:50:17 PM

25 50 100 200 500 Page 1/1 (2 items) 1

New devices (<4w)

Device typ	Device name	Created at
Media playe	Redmi Note 10S	3/12/2024, 10:09:05 AM
Media playe	Galaxy A52	3/12/2024, 9:31:05 AM

25 50 100 200 500 Page 1/1 (12 items) 1

Contrôle des applications et comportemental

La meilleure protection contre les malwares

- Protégez vos systèmes contre les logiciels malveillants connus et inconnus.
- Empêchez l'exécution de chaînes de processus non autorisées ou indésirables.
- Programmes d'audit des actions et autorisations requises
- Intégration dans votre solution de distribution de logiciels (Trusted Installer)
- Liste blanche/liste noire d'applications, de fichiers MSI, de scripts, etc.

Défendre les systèmes contre les menaces connues et inconnues

Aperçu complet des applications sur les systèmes

Répondre aux exigences de conformité et aux normes réglementaires

DriveLock

Christophe MULLER@QI-Demo | en

- Dashboard
- Security Controls
  - Drives
  - Devices
  - Applications
  - Encryption
  - Antivirus
  - Awareness
  - Vulnerabilities
- Inventory
- Analytics
- Administration

Standard | Applications | Devices | Alerts | Awareness | Antivirus | Vulnerabilities | Rollout

Agents with Application Control

7,398

Latest significant AC events

-

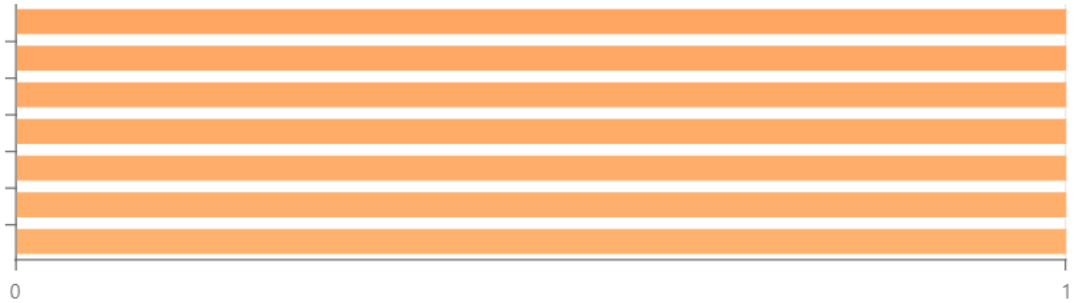
AC temporarily disabled

0

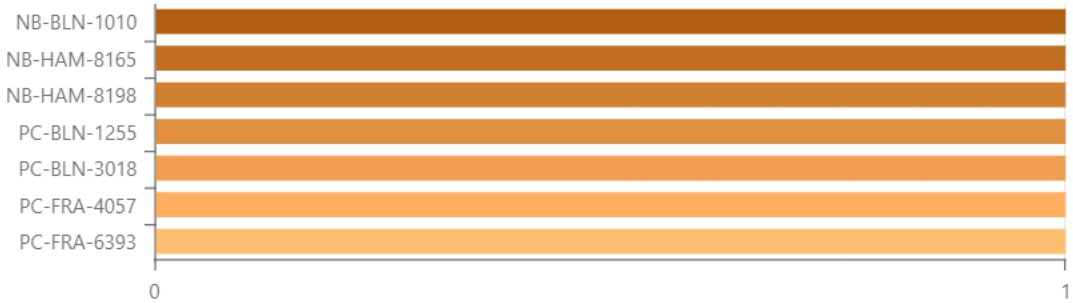
Learned files during unlock (<1w)

0

Blocked applications (<1w)



Blocked applications by computer(<1w)



Blocked applications launched by a user (<1w)

Process name	User name	Computer name	Timestamp	File version	File description
C:\Users\Fatma.Rosenberg\Downloads\	MED\Fatma.Rosenberg	PC-FRA-6393	3/12/2024, 10:10:06 AM	1.0.685.1	Dropbox Update Setup
C:\Users\Kamil.Appelt\AppData\Roamir	MED\Kamil.Appelt	PC-FRA-4057	3/12/2024, 10:05:06 AM	5.15.5.19404	Zoom Meetings

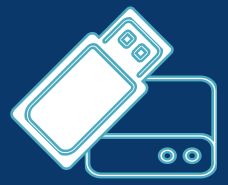
25 50 100 200 500

Page 1/1 (7 items) 1

Chiffrement

Confidentialité, intégrité, protection contre l'utilisation abusive des données

- Prévenir l'utilisation abusive ou le vol de données
- Garantir un accès autorisé aux données sensibles
- Assurer l'intégrité des données pendant la transmission et le stockage
- Garantir le respect des réglementations légales en matière de protection des données



Chiffrement des médias amovibles

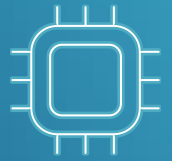
Chiffrement des supports externes avec options de récupération

Chiffrement de fichiers et dossiers

Chiffrement des fichiers sur les serveurs de fichiers et les autres emplacements de stockage

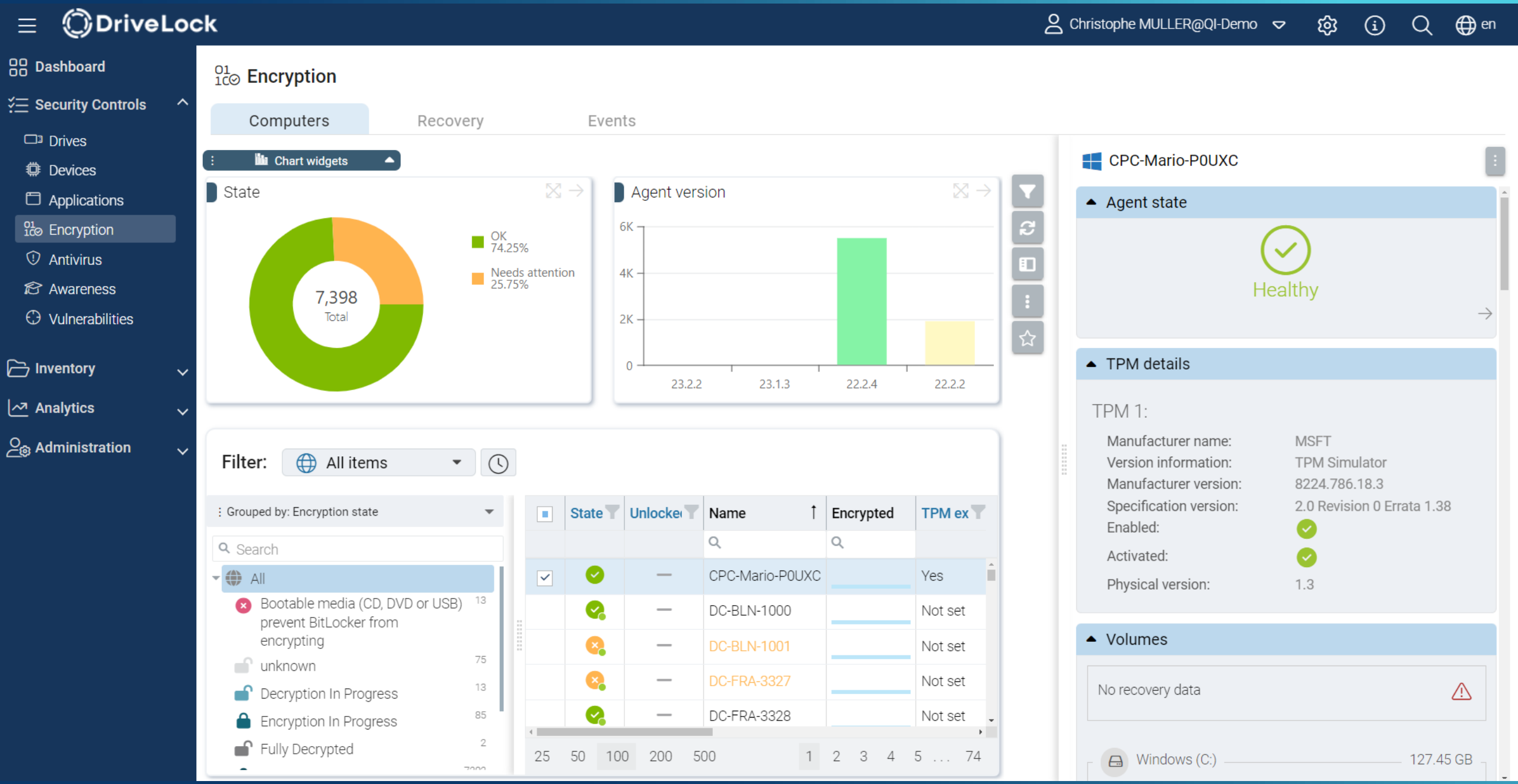
Chiffrement complet du disque

Chiffrement avec BitLocker ou Disk Protection



Authentification avant le démarrage

Authentification pré-démarrage multi-utilisateurs avec options de récupération étendues


DriveLock
Christophe MULLER@QI-Demo
en
Dashboard
Security Controls
Drives
Devices
Applications
Encryption
Antivirus
Awareness
Vulnerabilities
Inventory
Analytics
Administration
Encryption
Computers
Recovery
Events
Chart widgets
State
7,398
Total
OK
74.25%
Needs attention
25.75%
Agent version
6K
4K
2K
0
23.2.2
23.1.3
22.2.4
22.2.2
Filter:
All items
Grouped by: Encryption state
Search
All
Bootable media (CD, DVD or USB) prevent BitLocker from encrypting
13
unknown
75
Decryption In Progress
13
Encryption In Progress
85
Fully Decrypted
2
State
Unlocke
Name
Encrypted
TPM ex
CPC-Mario-P0UXC
Yes
DC-BLN-1000
Not set
DC-BLN-1001
Not set
DC-FRA-3327
Not set
DC-FRA-3328
Not set
25
50
100
200
500
1
2
3
4
5
74
CPC-Mario-P0UXC
Agent state
Healthy
TPM details
TPM 1:
Manufacturer name:
MSFT
Version information:
TPM Simulator
Manufacturer version:
8224.786.18.3
Specification version:
2.0 Revision 0 Errata 1.38
Enabled:
Activated:
Physical version:
1.3
Volumes
No recovery data
Windows (C:)
127.45 GB

Sensibilisation à la sécurité

Le facteur humain dans une stratégie de sécurité globale

- Motiver pour une sensibilisation à la sécurité durable
- Intégrer la main d'œuvre dans la stratégie de sécurité informatique
- Comment la technologie et les utilisateurs peuvent-ils travailler ensemble avec succès ?
- Créer une culture de cybersécurité dans l'entreprise
- Démontrer la conformité aux auditeurs

Conception moderne

Apprentissage expérimental et ludique, ainsi qu'à travers des histoires et des analogies

Solution intégrée

Affichage interactif d'informations relatives à la sécurité, par exemple lors de l'insertion d'une clé USB

Grande bibliothèque de contenu

Différents formats de médias personnalisables peuvent être sélectionnés.

Conforme au RGPD

Documente la mise en œuvre de mesures de protection conformément au RGPD.

Gestion des vulnérabilités

Un aperçu complet de votre surface d'attaque

- Les attaquants exploitent les vulnérabilités des logiciels.
- Maîtriser les risques liés aux vulnérabilités
- Corriger les vulnérabilités de manière proactive et automatique
- Quelles vulnérabilités doivent être prioritaires ?
- Empêcher l'exploitation des failles jusqu'à ce qu'un correctif soit disponible

Gestion centralisée

Identification et évaluation des vulnérabilités découvertes dans un aperçu centralisé

Base de données des menaces

Base de données sur les menaces mise à jour toutes les heures avec des scores CVE et CVSS basés sur les risques

Risque et conformité

Réduire les cyber-risques grâce à une évaluation continue de la position en matière de sécurité et de conformité

Gestion des utilisateurs et groupes locaux

Gestion des utilisateurs et des groupes, et protection des comptes privilégiés

- Empêcher l'exploitation des comptes d'utilisateurs locaux
- Automatiser la gestion locale des utilisateurs et des groupes
- Protéger les comptes privilégiés

Gestion et reporting centralisés des utilisateurs et groupes locaux

Automatisation des mots de passe individuels et aléatoires

Ajustement automatique des réglages lors du changement de secteur

Gestion du pare-feu Windows

Protéger contre les attaques réseau

- Définir des règles de pare-feu en fonction du lieu de travail
- Comment gérer différentes personnalités d'utilisateurs
- Protéger contre les attaques basées sur le réseau

Configuration centralisée basée sur les utilisateurs, les ordinateurs ou les groupes

Options de configuration flexibles et contrôle du réseau situationnel

Règles Microsoft prédéfinies. Options d'importation/exportation

Gestion de Windows Defender

Une synergie efficace pour une architecture de sécurité robuste et holistique

- Gérer Windows Defender plus efficacement
- Avoir un aperçu de la situation des menaces dans son environnement
- Analyser les lecteurs externes à la recherche de menaces avant utilisation
- Réagir automatiquement aux alarmes et aux menaces

Gestion centralisée

Administration simple dans un emplacement central avec un large panel de fonctions d'analyse et de reporting

Configuration simple

Tous les paramètres peuvent être configurés dans une politique DriveLock

Supervision et rapports

Aperçu complet de la situation en matière de sécurité et de classification des logiciels malveillants

Intégration complète

Intégration avec le contrôle des périphériques, la sensibilisation à la sécurité, les risques et la conformité

Détection et réponse aux menaces

Maximisez la sécurité en détectant et en résolvant les incidents

- Obtenir des indications sur les incidents potentiels
- Prédire les failles de sécurité potentielles
- Accompagner dans la résolution des problèmes
- Automatiser les options de réponse flexibles
- Surveiller l'activité en temps réel

Reconnaissance, corrélation et vérification des messages d'événements en temps réel

Journalisation centralisée pour l'évaluation des événements liés à la sécurité

Réponse automatique aux événements liés à la sécurité et aux menaces reconnues

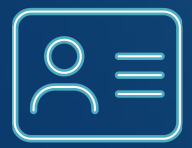
Messages de menaces et d'alarme basés sur le framework Mitre Att&ck®

Contrôle des accès

Visibilité et contrôle sur qui a accès à quoi

- Garantir un travail sécurisé dans l'environnement Microsoft 365
- Ne pas accepter le risque de perte involontaire de données
- Est-ce que je partage des fichiers avec les bonnes personnes ?
- Que partage l'entreprise avec les utilisateurs externes ?
- Éliminer les partages indésirables en un clic

Coopération sécurisée en interne et en externe



Les paramètres de version sont clairs et sous contrôle de façon centralisée

Preuve de conformité aux exigences légales

DriveLock fonctionne en arrière-plan jusqu'à ce qu'il détecte, affiche et résolve un problème.

Microsoft 365 Microsoft Teams OneDrive SharePoint

DriveLock

DRIVELOCK.COM

Contactez-nous pour plus d'informations.

www.query-informatique.com