Datacenters

Magazine Axis, numéro 1

Sécurité et opérations : l'atout Axis en renfort

Renforcement de la sécurité des datacenters par une approche à cinq niveaux

Sécurité en 3D : émergence de nouvelles menaces avec la démocratisation des drones

Levier de réduction de l'empreinte carbone des datacenters

et bien plus encore !

AXIS COMMUNICATIONS

Sommaire

L'évolution des comportements se traduit par un appétit croissant à l'égard des données, et nous sommes toujours plus nombreux à dépendre du datacenter. Les progrès de l'intelligence artificielle (IA), l'avènement de la 5G, la vidéo à la demande et la prolifération des objets connectés sont autant de facteurs qui alimentent cette déferlante de données.

En parallèle, le développement et la dissémination croissante des datacenters compliquent toujours plus le suivi de leurs opérations et leur protection. C'est là qu'Axis capitalise sur son expertise pour assister les grands acteurs européens des datacenters d'une multitude de manières. Dans ce magazine, nous expliquons quelques-uns des enjeux à affronter et le rôle que peuvent jouer les technologies pour y répondre.

Renforcement de la sécurité des sites par l'approche Axis à cinq niveaux
L'approche Axis comporte cinq niveaux de sécurité : périmètre, site, bâtiments, salles de serveurs et baies de serveurs. Avec la vidéosurveillance sur IP associée à des fonctions d'analyse en périphérie de réseau, Axis peut déployer une solution de sécurité physique intelligente qui renforce la sécurité et aboutit à des opérations plus résilientes et plus efficaces.

Détection de l'activité des drones pour atténuer les risques
La présence de drones au voisinage du datacenter est un risque croissant qui doit inciter les responsables de datacenters à compléter leur vision bidimensionnelle de la sécurité par un dispositif de surveillance aérienne plus efficace. Des logiciels spécialisés détectent les drones d'après les signaux radiofréquence (RF) qu'ils émettent, épaulés par les caméras réseau Axis qui transmettent aux opérateurs des alertes précoces d'approche de drone et des indications sur ses intentions.

Réduction de l'empreinte carbone et contribution aux objectifs écologiques
Les opérateurs de datacenters doivent examiner minutieusement les systèmes, produits et matériaux utilisés pour contribuer pas à pas aux objectifs de développement durable et à la réduction de l'empreinte carbone. Des partenariats de confiance, l'emploi de matériaux renouvelables et des technologies adéquates peuvent favoriser une exploitation plus pérenne et plus écologique du datacenter. Et dans ce domaine, Axis est bien positionné.

Transformation digitale et rôle des caméras réseau
Les datacenters peuvent combiner des technologies de détection existantes pour améliorer les opérations au travers d'une business intelligence sophistiquée. Les données produites par les caméras Axis, employées comme capteurs intelligents, peuvent être intégrées aux systèmes modernes de gestion des infrastructures de datacenter (DCIM) et conduire à des gains d'efficacité, par exemple au niveau des solutions de refroidissement. Lorsqu'ils disposent d'informations précises, les techniciens sont en mesure d'agir immédiatement pour corriger les problèmes.

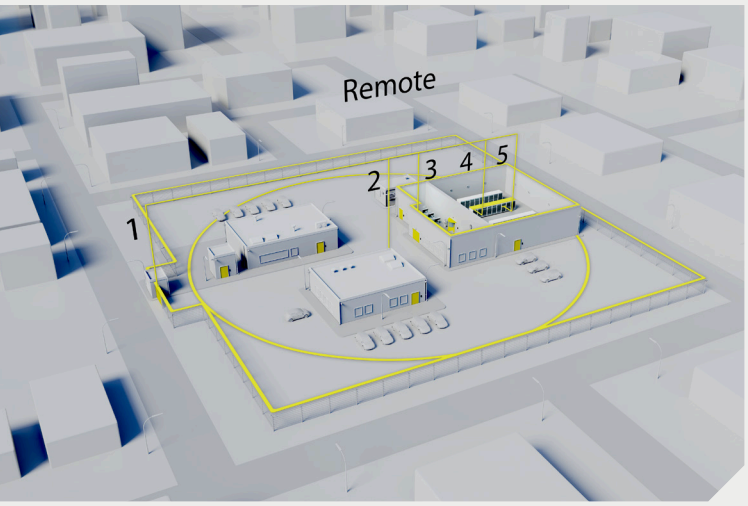
Renforcement de la sécurité physique par l'interopérabilité des dispositifs
Face à la hausse des menaces physiques, la sécurité des datacenters doit gagner en intelligence en recourant à des technologies connectées innovantes. Les solutions de sécurité physique Axis peuvent jouer un rôle central dans la protection du datacenter grâce à leur interopérabilité, pour aboutir à un système véritablement efficace et quasiment autonome qui renforce les moyens de défense du datacenter.

Nous espérons que le contenu de notre magazine vous sera utile pour faire progresser votre réflexion sur le sujet. Quelle que soit la problématique, Axis est résolu à collaborer avec ses partenaires et ses clients pour développer des solutions de pointe favorisant l'avènement d'un monde plus sûr et plus intelligent.

En vous souhaitant une année pleine de promesses,
Peter Dempsey, Responsable grands comptes, clients finaux – EMEA

Renforcement de la sécurité des datacenters par une approche à cinq niveaux

Avec le développement des services cloud et de l'informatique hyperscale, les utilisateurs dépendent toujours plus de la puissance et de la capacité colossales des datacenters. En parallèle, les nouvelles habitudes comportementales font exploser la consommation de données.



Le développement et la dissémination croissante des datacenters peuvent compliquer singulièrement la surveillance des opérations et le maintien d'un niveau élevé de sécurité. De son côté, le personnel est sans cesse plus occupé à protéger les ressources des menaces à la fois physiques et cyber. Il est vrai qu'une perturbation de l'activité peut s'avérer catastrophique : les périodes d'indisponibilité peuvent avoir de lourdes conséquences financières et pénaliser gravement les particuliers et entreprises qui comptent au quotidien sur la fluidité du transfert des données. La mise en place d'outils et technologies adéquats est donc déterminante pour assurer une protection complète et omniprésente. Les solutions doivent en plus être évolutives au rythme du développement et de la transformation des datacenters.

Sécurité complète du site, à l'intérieur et à l'extérieur

Les solutions audio et vidéo intégrées Axis peuvent protéger les datacenters et fluidifier les opérations. Notre approche à cinq niveaux englobe le périmètre, le site, les bâtiments, les salles de serveurs et les baies de serveurs. Elle fait appel à des produits de sécurité sur IP embarquant des fonctions d'analyse locale, pour aboutir à une solution véritablement intelligente qui assure une protection complète et sans angle mort. La détection et la résolution des incidents se simplifient, tandis que l'intégration de divers capteurs et caméras offre aux opérateurs une sérénité totale.

L'audio et la vidéo sur IP Axis contribuent à protéger le périmètre du datacenter, avec des caméras de vidéosurveillance, des caméras thermiques et des radars qui détectent le mouvement sur le site ou à proximité, en suivant les intrus potentiels qui s'approchent à pied ou à bord d'un véhicule. La diffusion automatique d'alarmes par haut-parleur peut dissuader les possibles contrevenants. Ces mêmes haut-parleurs peuvent aussi permettre aux opérateurs de s'adresser directement aux intrus en temps réel. Pilotées par de puissantes fonctions d'analyse, ces technologies sont extrêmement précises. Elles occasionnent ainsi moins de faux positifs et, par suite, une réduction des coûts.

Sur le site, des systèmes de contrôle d'accès utilisant la vidéosurveillance comme deuxième facteur d'authentification sont installés à tous les points d'entrée. Ils identifient, authentifient et autorisent les personnes, avec des fonctions de reconnaissance faciale pour gérer l'accès aux bâtiments, aux salles de serveurs et même aux baies de serveurs individuelles. L'audio sur IP peut également jouer un rôle pour se prémunir des méfaits de sources internes, au moyen d'alarmes déclenchées par des caméras réseau qui détectent toute activité inhabituelle dans les nombreux bâtiments du datacenter. L'accès à une baie de serveurs sans autorisation ou une tentative d'accès à une zone contrôlée à une heure indue peut compter parmi ces activités suspectes.

Lorsqu'un tel volume de données est en jeu, un système extrêmement sécurisé, mais aussi évolutif au rythme du développement du datacenter, est impératif. Car un dispositif vulnérable peut être la cible d'un piratage, de la part d'ennemis aussi bien de l'intérieur que de l'extérieur. Axis répond à ces problématiques par un renforcement continu de la cybersécurité de ses dispositifs, au travers de mises à niveau du firmware, de correctifs et de tests de maintenance.

Axis est idéalement placé pour accompagner le nouveau datacenter dans la protection de ses ressources et de ses locaux, grâce à toute une série de solutions réseau offrant communication chiffrée, filtrage d'adresses IP, amorçage sécurisé et signature de firmware. La méthode Axis s'assure que la cybersécurité n'est pas pensée après coup, mais au contraire prise en compte dès le départ.

5 niveaux

- Périmètre
- Site
- Bâtiments
- Salles de serveurs
- Baies de serveurs

Caméras réseau au service de la transformation digitale des datacenters

Les données sont des ressources très précieuses, mais seulement lorsqu'elles sont exploitées de manière efficace. Le cloisonnement des données, même s'il simplifie la gestion de systèmes individuels, représente de fait une occasion manquée. L'unification des données est la solution pour créer une Business Intelligence véritablement utile.

L'intégration des données et l'interaction des capteurs et actionneurs avec l'IA produisent des analyses exploitables et créatrices d'importantes synergies opérationnelles dans une grande variété de secteurs d'activité.

Des données bien analysées révèlent des liens les services et leurs utilisateurs, pour aboutir à un vaste système intégré en un tout efficace. Pourquoi le datacenter devrait-il faire exception ? Dans le contexte actuel, l'efficacité énergétique, la sécurité des ressources et la qualité de service sont des enjeux prioritaires. Or, les datacenters doivent composer avec une demande de calcul croissante due aux analyses de données toujours plus complexes sollicitées par les clients, ce qui accroît les besoins de dissipation thermique. La sécurité des bâtiments et la gestion des équipements sont souvent gérées séparément, mais les datacenters doivent exploiter toutes les ressources disponibles pour satisfaire la demande.

Réseaux intelligents : le nouveau paradigme

Heureusement, cette évolution nécessaire arrive à un moment où les outils capables de la concrétiser se sont largement démocratisés. Les objets connectés de l'univers IoT ont aujourd'hui la puissance nécessaire pour collecter, traiter et analyser des données localement. Le traitement en périphérie du réseau réduit nettement les besoins en bande passante, la quantité d'équipements de traitement externes et la latence globale (de 100-250 ms à 10-20 ms*), car il n'est plus nécessaire de faire transiter systématiquement de grands volumes de données vers des serveurs cloud.

De plus, les dispositifs IoT parlent enfin le même langage. La popularité croissante du protocole MQTT (Message Queue Telemetry Transport), qui complète les réseaux TCP/IP standard, permet désormais d'intégrer sans peine les données de ces dispositifs à des applications sur serveur ou dans le cloud. Comme le protocole MQTT est open source et repose sur des normes ouvertes, le développement d'intégrations de nouveaux terminaux ou d'automatismes pilotés par leurs données est grandement simplifié. Les systèmes de sécurité du datacenter n'ont plus aucune raison d'exister sur un réseau isolé de celui de ses capteurs DCIM (DataCenter Infrastructure Management).

Évolution du rôle de la caméra réseau

La nature ouverte du protocole MQTT offre la possibilité d'intégrer des données qui répondent aux demandes des systèmes DCIM modernes en utilisant les caméras réseau comme des capteurs intelligents. Le suivi de la température en est un exemple : Si un capteur de température interne détecte un point chaud dans une baie de serveurs, il transmet l'information à une caméra thermique, qui peut ensuite relayer une image bien documentée à un système de gestion vidéo pour indiquer précisément la localisation du problème au technicien. Une combinaison de données issues d'une variété de capteurs peut alors conduire à des gains d'efficacité, par exemple par l'ajustement des solutions de refroidissement pour optimiser la consommation d'énergie.

De nouvelles manières d'exploiter les données que recueillent les caméras réseau peuvent également réduire radicalement les coûts et la complexité du système DCIM. Les datacenters doivent gagner en efficacité dans tous les domaines possibles, et le recours aux caméras réseau pour une grande diversité d'applications pourrait être une stratégie judicieuse. De plus, lorsque des caméras sont déjà installées pour des raisons de sécurité, elles sont aussi mobilisables à des fins opérationnelles.

L'heure est venue de rendre le datacenter véritablement intelligent. Mais il n'est pas pour autant question de se débarrasser des solutions DCIM ou de remplacer des capteurs critiques. Concrètement, le but consiste à capitaliser sur chaque donnée pour créer de nouvelles opportunités, tout en tirant le maximum des solutions et dispositifs connectés les plus performants.

*www.ibm.com/blogs/internet-of-things/iot-5g-transforms/

Sécurité en 3D

Émergence de nouvelles menaces avec la démocratisation des drones.

Le marché des drones est en plein essor, et les entreprises qui exploitent ces appareils en tirent d'importants bénéfices opérationnels. Mais les prévisions de croissance[1] vont immanquablement poser des problèmes de sécurité. Aux vacances de Noël 2018, l'aéroport britannique de Gatwick a fermé pendant 33 heures, perturbant plus de 140 000 passagers. Malgré plusieurs témoins oculaires aux déclarations concordantes, il n'a pas été possible de confirmer la présence d'un drone[2].

Cet incident a mis en exergue un problème majeur. Un drone, disponible dans le commerce dès 200 euros environ, avait vaincu les moyens de protection périmétrique de l'aéroport, coûtant des millions d'euros à l'industrie aéronautique. Il faut dire que les drones peuvent transporter des charges utiles qui font froid dans le dos : caméra pour activités hostiles de reconnaissance, équipements d'interception de signaux Wi-Fi pour perturber les logiciels et les systèmes, armes biologiques… d'où l'impératif de prendre cette menace très au sérieux.

Détection, identification et localisation

Dans les datacenters, la protection contre les menaces de nature cyber et physique constitue un impératif critique, qui exige un niveau de sécurité élevé. Toute période d'indisponibilité peut avoir de lourdes conséquences financières et pénaliser gravement les particuliers et entreprises qui comptent au quotidien sur la fluidité du transfert des données.

Les systèmes modernes en réseau ont nettement fait progresser les moyens de protection périmétrique, en incorporant des caméras de surveillance, des caméras thermiques et des radars pour suivre les déplacements des intrus. Même si la sécurité du datacenter s'est considérablement renforcée ces dernières années, la prise en compte des nouvelles menaces est indispensable pour garder une longueur d'avance. Et aujourd'hui, ces menaces peuvent surgir du ciel.

Des logiciels spécialisés en complément des solutions réseau de sécurité physique peuvent aujourd'hui détecter les drones à partir des signaux radiofréquence (RF) qu'ils émettent. Ils peuvent identifier la marque et le modèle de plus de 200 drones professionnels, de loisirs ou à construire, et même localiser le pilote. Beaucoup plus fiable que les seuls yeux et oreilles des équipes de sécurité, cette technologie peut avertir de l'approche d'un drone et donner des indices précoces sur ses intentions.

> Un drone entre de bonnes mains est plein de promesses, mais comme d'autres matériels, un détournement de sa fonction est toujours possible.

Analyse et atténuation du risque lié aux drones

Une fois le drone détecté, le motif de sa présence reste à établir. Généralement, les datacenters se trouvent dans des zones interdites au survol. Les agents de sécurité ou les forces de l'ordre doivent être en mesure de faire rapidement la distinction entre un pilote distrait et un acteur mal intentionné. En localisant le drone et en détectant les signaux émis par l'équipement de son pilote, le personnel de sécurité peut être déployé pour avoir une conversation avec le contrevenant.

Dans les cas où l'incident est confirmé, une identification rapide est cruciale pour une prise de décision sans délai. Un logiciel de détection de drones, capable d'envoyer un signal à une caméra PTZ (panoramique/inclinaison/zoom), peut servir à suivre les mouvements du drone. Les images extrêmement nettes permettent de confirmer la teneur de sa charge utile pour distinguer les appareils inoffensifs des engins ennemis.

Solution de détection des drones issue d'un partenariat

Du fait de la menace grandissante que représentent les drones, Axis et son partenaire Dedrone se sont associés pour produire une solution intelligente de sécurité de l'espace aérien unique sur le marché. La solution doit son succès à la collecte de données : plus de 17 millions d'images de drones à ce jour ont servi à entraîner le logiciel de la caméra par ML/IA pour identifier avec précision les drones, même bien camouflés. Par ailleurs, des protocoles d'identification à distance, appelés RemoteID, fournissent des informations pour vérifier la légitimité d'un drone. Cette technique sert également à améliorer les capacités de détection des menaces.

Un drone entre de bonnes mains est plein de promesses, mais comme d'autres matériels, un détournement de sa fonction est toujours possible.

Après la mise en place d'une telle solution, la surveillance du ciel autour du datacenter est aussi efficace qu'au sol. En l'intégrant aux systèmes existants de gestion vidéo, la solution de détection des drones peut faire partie d'un système global intégré qui renforce la posture de sécurité générale.

[1] www.insiderintelligence.com/insights/drone-industry-analysis-market-trends-growth-forecasts/
[2] www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone

Renforcement de la sécurité physique

des datacenters par l'interopérabilité des dispositifs

On a beaucoup écrit sur le niveau de cybersécurité très élevé nécessaire à la protection des datacenters, mais leur sécurité physique reste un sujet d'inquiétude. Un article dans la presse aux États-Unis a fait état de l'arrestation d'un homme soupçonné d'avoir préparé une opération pour faire exploser un grand datacenter en Virginie*. En réfléchissant aux mesures à prendre pour atténuer ce type de menace, l'adoption de solutions de sécurité physique de pointe devient évidente. Ce qui l'est moins, c'est le potentiel de ces solutions dans la sécurisation et la protection lorsqu'elles sont interconnectées pour renforcer au maximum le dispositif de défense.

Innovation dans les radars et la vidéo sur IP

Les caméras réseau ont déjà atteint le point où l'analyse embarquée peut servir à catégoriser le mouvement (par exemple intrusion ou maraudage) et à différencier les personnes des véhicules et des objets sur le périmètre d'un site. La précision des caméras modernes est telle que le taux de faux positifs est très faible. De plus, le traitement en périphérie de réseau permet de transmettre uniquement les données les plus cruciales sur le réseau pour analyse, avec à la clé une prise de décision plus rapide, des gains de temps et des économies.

Les solutions de sécurité physique peuvent jouer un rôle crucial dans la protection du datacenter, mais c'est surtout leur interopérabilité qui les transforme en un système véritablement efficace et quasiment autonome. Par exemple, une solution associant radars et caméras peut détecter et classifier les mouvements en bordure de périmètre, activer une caméra thermique pour détecter une empreinte thermique et confirmer une présence humaine non autorisée. Ensuite, une caméra PTZ suit le mouvement, tandis qu'un haut-parleur IP diffuse un message de dissuasion préenregistré. Une sirène-stroboscope IP se déclenche si l'intrus continue d'avancer en produisant simultanément des éclats lumineux et une sirène en guise d'avertissement final.

Évidemment, les menaces peuvent avoir d'autres origines. À l'intérieur de l'installation, des caméras réseau exécutant localement une fonction d'analyse peuvent servir d'alerte précoce pour détecter des fuites de gaz ou de la fumée, tandis que les caméras et capteurs connectés peuvent identifier les fuites d'eau.

Les caméras thermométriques peuvent jouer un rôle déterminant pour détecter une hausse de la température en un point, signe éventuel d'un problème plus grave. Lorsqu'elles surveillent un groupe électrogène par exemple, une variation minime de la température peut déclencher une alarme sonore lorsqu'un seuil prédéterminé est atteint.

Les partenariats au service d'une protection complète

Au Royaume-Uni, le Centre pour la protection des infrastructures nationales (CPNI) a publié des directives et des normes pour tous les sites abritant des infrastructures nationales critiques. Les datacenters en font partie puisqu'ils fournissent des services jugés essentiels. Au travers d'un partenariat avec un fournisseur réputé de solutions de sécurité physique certifié par le CPNI, les responsables de datacenters sont assurés que les produits qu'ils choisissent sont de la meilleure qualité et capables de répondre aux critères les plus stricts.

En choisissant des outils à l'avant-garde de l'innovation, les sites des datacenters bénéficient de solutions connectées de sécurité physique autonomes, garantes d'une protection du plus haut niveau.

*www.bbc.co.uk/news/technology-56719618

Levier de réduction de l'empreinte carbone des datacenters pour une meilleure viabilité écologique

D'après les prévisions, le marché mondial des datacenters verts pèsera 142,8 milliards de dollars d'ici à 2026, soit une progression annuelle moyenne approchant les 20 %[1]. Ces datacenters doivent être en mesure d'assurer un stockage fiable et extrêmement sécurisé, tout en maximisant leur rendement énergétique pour abaisser leur empreinte environnementale. Cette ambition est d'autant plus nécessaire pour les signataires du Climate Neutral Datacenter Pact, qui s'engagent à atteindre la neutralité carbone de leurs datacenters d'ici à 2030[2].

Néanmoins, de nombreux datacenters doivent se réinventer totalement pour devenir suffisamment durables. Leur consommation d'énergie colossale et la chaleur extrême qu'ils dégagent sont les principaux leviers d'action pour réduire leur effet sur l'environnement. À juste titre, la pression monte pour les datacenters qui n'ont pas encore adhéré à des initiatives écologiques les incitant à améliorer leur empreinte carbone. Pour le responsable de datacenter, l'enjeu consiste à réduire l'empreinte écologique tout en continuant d'assurer un service irréprochable.

Cadres de développement durable et chaînes logistiques de confiance

Les datacenters affichant une plus grande sensibilisation aux effets potentiels de mesures positives sur l'environnement attirent davantage les entreprises également engagées dans la réduction de leur empreinte carbone[3]. En s'appuyant sur des initiatives et normes internationales comme le Pacte mondial des Nations-Unies, dont Axis est signataire[4], les entreprises ont toutes les cartes en main pour se rapprocher des objectifs de développement durable (ODD) édictés par l'ONU[5] et montrer que leurs actes correspondent à leur discours.

De fait, l'affiliation à un cadre internationalement reconnu révèle une convergence de valeurs communes. Dès lors, dans un contexte largement tourné vers la réduction des coûts, l'accès à des compétences techniques de haut niveau, l'amélioration de la fourniture de services et la course à l'innovation, l'établissement de partenariats devient indispensable. Lorsque les entreprises recherchent des alliances commerciales rapprochées, tous les acteurs de la chaîne logistique doivent souscrire à des valeurs communes pour établir la confiance.

Réduction de l'empreinte carbone et contribution aux objectifs écologiques

Les datacenters sont de vrais gouffres énergétiques, qui dégagent de très grandes quantités de chaleur. Ce sont des sujets de préoccupation pour les responsables de datacenter sensibles à l'environnement. La démarche de « verdissement » du datacenter n'est ni simple, ni rapide. Les gestionnaires de datacenters doivent examiner minutieusement les systèmes, produits et matériaux employés pour se rapprocher pas à pas des objectifs de développement durable et réduire progressivement leur empreinte carbone. Cette démarche peut passer par la sélection de fournisseurs qui mettent tout en œuvre pour modérer la consommation d'énergie de leurs produits et services.

Par exemple, les fonctions d'analyse locale dans les caméras réseau Axis, qui traitent les données vidéo à l'intérieur même des dispositifs, évitent la transmission permanente de données sur le réseau pour traitement, d'où une réduction de la consommation d'énergie et des besoins en bande passante. Autre atout en soutien d'un programme de réduction de l'empreinte carbone, la technologie Axis Zipstream[6] réduit les besoins en bande passante et en stockage de 50 % en moyenne.

Axis aide les datacenters à limiter leur effet sur l'environnement en proposant des solutions innovantes qui conjuguent sécurité de pointe et impact écologique minimal. Une sélection rigoureuse des matériaux et notre engagement de réduction des déchets dans nos processus démontre le sérieux de notre démarche en englobant la totalité de la chaîne de production. Nous sommes totalement impliqués pour accompagner les datacenters dans l'atteinte de leurs objectifs écologiques, tout en innovant pour un monde plus sûr, plus intelligent et plus durable.

Solutions pour datacenters recommandées

Caméras-radars combinés
Axis

Bénéficiez d'une protection contre les intrusions et d'une détection fiable 24 h/7 j sur un espace étendu grâce à la fusion de deux technologies puissantes : la vidéo et le radar. Ce dispositif unique offre un classement de pointe des objets fourni par le deep learning pour une détection et visualisation de haut niveau.

Caméras PTZ
Axis

Les caméras PTZ assurent une surveillance en temps réel de vastes zones grâce à leurs fonctions de panoramique, inclinaison et zoom. La série AXIS Q61 restitue les scènes avec fidélité et une qualité d'image parfaite dans toutes les directions, au-dessus comme en dessous de l'horizon. Cette série présente ainsi un avantage unique lorsque le terrain est légèrement accidenté. La série AXIS Q62 comporte des caméras renforcées qui supportent toutes les conditions météo. La série AXIS Q63 propose quant à elle un zoom et une mise au point laser rapides, même dans l'obscurité. Grâce à son mécanisme de séchage rapide Speed Dry, les images sont toujours claires et nettes par temps de pluie.

AXIS Q1961-TE
Thermal Camera

Cette caméra thermométrique sans halogène surveille les températures à distance et déclenche des événements en cas de dépassement de seuils prédéfinis. Idéale pour améliorer l'efficacité opérationnelle, robuste et résistante aux chocs, elle intègre des fonctions de cybersécurité et de détection précoce des départs de feu.

Contrôle d'accès
Axis

Axis fournit les équipements et les fonctions d'analyse permettant d'identifier, d'authentifier et d'autoriser l'accès aux bâtiments et aux locaux. Nos technologies de contrôle d'accès protègent les zones critiques ou vulnérables par authentification automatique (cartes d'accès, codes PIN, QR Codes) ou manuelle (vidéo et audio sur IP bidirectionnel).

Haut-parleurs réseau
Axis

Les haut-parleurs réseau Axis permettent de dissuader les activités indésirables et de faire fuir les fauteurs de troubles détectés par vos caméras, par exemple en les installant sur le périmètre d'un site. Ils peuvent également servir à diffuser des consignes vocales en cas d'urgence ou à prévenir d'un stationnement gênant.

Pourquoi Axis ?

À la pointe de la cybersécurité

Les cyberattaques sur les infrastructures ou le vol de données peuvent avoir des effets catastrophiques sur une ville. Que se passerait-il si les caméras régissant les feux de circulation étaient piratées ? La neutralisation de ce type de menaces compte parmi les priorités des pouvoirs publics. Or, Axis est un leader des solutions de sécurité, avec un historique irréprochable dans la sécurité, la protection et la conformité des données des villes intelligentes. Nous avons accumulé une grande expertise dans l'évaluation des risques et l'intégration des processus de protection des données à chaque niveau de notre offre, toujours en conformité avec les politiques, réglementations et législations actuelles et futures.

Une qualité omniprésente

Axis œuvre systématiquement dans une perspective de qualité. Tous nos produits sont conçus pour résister aux conditions difficiles, au vandalisme et aux fortes intempéries. Nos produits font l'objet d'essais rigoureux pour vérifier leur longévité et restituer des images nettes dans toutes les conditions. Notre démarche qualité se reflète dans les excellentes images HDTV que produisent nos caméras, à tel point qu'elles sont recevables comme preuves dans les tribunaux.

Le pouvoir des partenariats

La plateforme ouverte Axis est flexible, évolutive et facile à intégrer. Elle est compatible avec une multitude de systèmes de partenaires, de matériels d'autres marques et de logiciels d'autres éditeurs.

Technologies innovantes

Nous œuvrons sans relâche à réunir le meilleur des technologies et de l'imagination humaine pour renforcer les performances de nos produits. L'analyse et l'exploitation des données en périphérie de réseau gagnent rapidement du terrain et peut vous apporter de précieux éclairages.

En savoir plus sur les solutions Axis pour datacenters

www.axis.com/data-centers

À propos d'Axis Communications

En créant des solutions qui renforcent la sécurité et améliorent la performance des entreprises, Axis contribue à un monde plus intelligent et plus sûr. Leader de son secteur dans les technologies sur IP, Axis propose des solutions en vidéosurveillance, contrôle d'accès, visiophonie et systèmes audio. Ces solutions sont enrichies par des applications d'analyse intelligente et soutenues par des formations de haute qualité.

L'entreprise emploie environ 4000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et intégrateurs de systèmes du monde entier pour fournir des solutions sur mesure à ses clients. Axis a été fondée en 1984, son siège est situé à Lund en Suède.