DES ACCÈS SÉCURISÉS pour un système d'information mieux protégé !

Bernard Debauche, au sein de Systancia, détaille pour nous le positionnement de son entreprise dans la cybersécurité. Positionnée essentiellement dans la sécurisation des accès, l'entreprise propose des solutions performantes et des compétences reconnues sur ce segment. Entretien.

Bernard Debauche

Systancia est un éditeur de logiciels et de solutions de cybersécurité. Qu'est-ce que cela implique ?

Dans le très large domaine de la cybersécurité, Systancia est spécialisée dans l'accès Zero-Trust. Concrètement, nous permettons à tout collaborateur d'accéder à son environnement de travail en toute confiance dans un monde de zéro-confiance.

En effet, alors que le monde de la cybersécurité évolue, nous sommes également face à un changement de paradigme qui s'est accéléré avec la pandémie, la crise sanitaire et la généralisation du télétravail : nous sommes passés d'une sécurité dite périmétrique, construite autour de l'idée que nous sommes en sécurité « dedans » et en danger « dehors », à une sécurité Zero-Trust.

Pour accompagner cette évolution majeure, Systancia s'appuie sur :

- Des compétences techniques pointues ;
- Une démarche continue d'innovation pour être en capacité à proposer des solutions toujours plus efficaces et pertinentes ;
- Un positionnement cohérent au sein de l'écosystème de la cybersécurité qui nous permet d'interagir avec les autres acteurs du secteur.

Sur un marché qui a connu une très forte croissance au cours des dernières années, quelles sont vos forces et votre valeur ajoutée ?

Nous disposons d'un portefeuille de produits qui nous permet de couvrir à la fois la gestion des accès et l'infrastructure d'accès. Dans un monde Zero-Trust , le nouveau périmètre de sécurité repose sur l'identité ce qui implique de prendre en compte aussi bien la gestion des identités que celle de l'infrastructure d'accès.

Au cœur de notre ADN, on retrouve également deux aspects clés : la virtualisation et l'intelligence artificielle. Concrètement, la virtualisation d'applications dans la cybersécurité grâce à la technique d'isolation, nous permet d'isoler l'utilisateur et son poste du système d'information de l'entreprise.

En parallèle, nous capitalisons sur l'intelligence artificielle et le machine learning pour faire de l'analyse comportementale des personnes et des systèmes. Nous proposons ainsi une offre d'authentification comportementale qui permet d'authentifier l'utilisateur à partir de son utilisation de la souris et du clavier. Cela nous permet de dire s'il s'agit toujours bien de la même personne derrière l'écran que celle qui s'est authentifiée.

Grâce à notre capacité d'ingénierie, nos compétences technologiques et nos talents, nous innovons et nous sommes, par exemple, capables de faire de l'enregistrement de session web sans agent.

Avec vos solutions, quelles sont les problématiques et les attentes des entreprises que vous adressez ?

Au cœur de notre proposition de valeur, nous retrouvons la sécurisation de l'accès de l'utilisateur à son environnement de travail. Dans cette continuité, nous apportons des solutions sur des problématiques telles que :

- La sécurisation du télétravail grâce à la technologie Zero Trust Network Access ;
- L'accès de prestataires informatiques au système d'information de l'organisation, et notamment les accès à privilèges d'administrateurs du système d'information avec la technologie Privileged Access Management ;
- Le renforcement de l'authentification de manière la plus transparente possible avec la technologie Multi-Factor Authentication ;
- Le contrôle des accès aux ressources informatiques, à partir de l'identité des utilisa-

teurs, dans une politique de sécurité Zero-Trust en ayant recours à des technologies de gestion des identités, d'Identity and Access Management.

Comment intégrez-vous les évolutions connues par ce secteur et notamment la fréquence et l'intensité plus forte des cyberattaques ?

De par notre positionnement, nous n'intervenons pas sur la dimension détection et la réponse aux attaques. Notre action couvre essentiellement les solutions d'accès et leur sécurisation. Il est aujourd'hui reconnu de tous qu'en matière de cybersécurité, mieux vaut prévenir que guérir. C'est dans cette logique que nous proposons des solutions qui ne laissent pas passer les attaques. Par exemple, notre solution de télétravail sécurisé permet d'accéder, depuis un ordinateur personnel, à un PC du bureau, en empêchant la diffusion d'un potentiel programme malveillant présent sur l'ordinateur personnel. Notre solution agit comme une barrière contre les programmes malveillants (malware, ransomware) pour qu'ils ne puissent pas atteindre le système d'information de l'entreprise. Pour ce faire, nous utilisons notamment des technologies de rupture protocolaire, de filtrage des interactions…

En parallèle, quels sont vos enjeux et vos perspectives ?

Aujourd'hui, il y a deux constats majeurs : le sous-équipement des plus petites organisations et le suréquipement des grands comptes. D'ailleurs, une étude de Trend Micro indique que, en moyenne, les entreprises disposent de 29 produits de sécurité différents.

À partir de là, un des premiers enjeux est de consolider plusieurs produits ou services de cybersécurité au sein d'une même plateforme, de manière plus intégrée. Il s'agit aussi de rendre la cybersécurité plus accessible aux plus petites organisations : proposer une plateforme SaaS de cette typologie avec une expérience utilisateur unifiée et simplifiée permettra, in fine, d'atteindre cet objectif.

Un autre enjeu important tourne autour de la question du développement d'offres de partenaires fournisseurs de services managés de sécurité (MSSP, Managed Security Service Provider). Pour déployer de la cyber, il faut des compétences.

Les organisations ont généralement tendance à s'appuyer sur un partenaire qui dispose de ces compétences, et qui peut leur offrir un bouquet de services cyber, allant du SOC à des services d'accès. Dans cette démarche, nous donnons la possibilité à de tels MSSP de compléter leur offre avec des services d'accès sécurisés très compétitifs.

"Dans le très large domaine de la cybersécurité, Systancia est spécialisée dans l'accès Zero-Trust. Concrètement, nous permettons à tout collaborateur d'accéder à son environnement de travail en toute confiance dans un monde de zéro-confiance."

EN BREF

- *Création il y a 20 ans*
- *Un positionnement dans le secteur de la cybersécurité depuis 10 ans*
- *Plus de 140 collaborateurs*
- *Plus de 600 clients majoritairement en France, mais également dans une vingtaine de pays*