DES SOLUTIONS DE CYBERSÉCURITÉ performantes et simples à déployer

Acteur reconnu à l'échelle internationale sur le segment de la sécurisation des accès et des identités numériques, *Wallix* accélère sa croissance sur un marché de la cybersécurité en pleine explosion et affiche de très fortes ambitions de développement. *Le point avec son PDG et fondateur Jean-Noël de Galzain.*

Jean-Noël de Galzain

La cybersécurité est un sujet qui est au cœur de toutes les préoccupations. Qu'avez-vous pu observer ?
En 2021, le coût de la cybercriminalité a été évalué à 6 000 milliards de dollars. À horizon 2026, on estime que ce chiffre va doubler. À titre comparatif, le poids de la cybercriminalité est actuellement équivalent à celui de la troisième économie mondiale. Jusque-là, les cyberattaques relevaient du coup médiatique, de l'exploit personnel ou technologique. Aujourd'hui, derrière ces attaques, il y a une véritable professionnalisation des cyberattaquants et une certaine organisation de la cybercriminalité, qui non seulement s'apparente de plus en plus au crime organisé, mais qui a également des répercussions importantes sur le plan géopolitique.
Au cours des dernières années, la nature des attaques a aussi considérablement évolué. Parmi les plus répandues, on retrouve les ransomware avec plus de 600 millions d'attaques en 2021, soit le double de l'année précédente. Nous avons aussi assisté à une extension de la surface d'attaque, c'est-à-dire une hausse du nombre de portes d'entrée potentielles pour les hackers. Ce phénomène est la conséquence directe de l'accélération de la digitalisation de nos sociétés et de nos entreprises qui s'appuient sur des systèmes toujours plus interconnectés et interdépendants.
Historiquement, au début du développement de l'informatique, le but était de protéger les ordinateurs avec des antivirus. Avec l'émergence d'internet et des réseaux, l'idée a été de créer des forteresses autour des entreprises grâce aux firewall et aux logiciels de VPN qui contrôlaient l'accès aux entreprises. Depuis le début des années 2020, on s'inscrit de plus en plus dans une logique de Zero Trust, une philosophie qui consiste à dire qu'il ne faut pas faire confiance à personne, aussi bien à l'intérieur qu'à l'extérieur de l'organisation. Dans cette logique, les accès ou les autorisations ne doivent être donnés qu'aux personnes qui en ont strictement besoin pendant la durée où elles en ont réellement besoin. Ce changement de paradigme s'accompagne d'une phase de transition avec le passage d'une informatique hébergée dans l'entreprise vers une informatique hébergée dans le cloud. D'un point de vue de cybersécurité, cela implique entre autres de mettre en place des systèmes de gestion et de contrôle des identités, des autorisations et des accès beaucoup plus stricts.

Dans ce cadre, quel est le positionnement de Wallix ?
Wallix est un éditeur de logiciels qui permettent aux entreprises et aux organisations de reprendre le contrôle de leur accès afin de relever les défis de leur transformation numérique de manière sécurisée. Aujourd'hui, Wallix opère dans plus de 90 pays et emploie près de 250 personnes. En 2022, nous avons réalisé un chiffre d'affaires de près de 25 millions d'euros et avons accompagné près de 2 000 clients dans le monde.
Notre mission est d'aider les entreprises à faire face à l'explosion de la surface d'attaque et à la multiplicité des identités et des points d'accès à gérer et à contrôler. Dans le passé, seuls les administrateurs informatiques avaient besoin d'accéder à des ressources critiques. Aujourd'hui, cela n'est plus le cas. Par exemple, les développeurs, pour mettre à jour des applications et des logiciels, ont besoin d'accéder à des sites qui sont en production et sur lesquels il y a des transactions à fort impact. De plus en plus, les entreprises optent pour un hébergement hybride de leurs systèmes avec des infrastructures en interne et pour le recours au cloud. Et à cela s'ajoutent des intervenants externes toujours plus nombreux qui accèdent aux systèmes

de l'entreprise et une multiplication des points d'accès, des terminaux, des PC, des téléphones et des serveurs.
Au-delà, pour les entreprises, il s'agit aussi de sécuriser leurs opérations ou Operational Technology (OT), c'est-à-dire la technologie qui intervient dans les systèmes industriels de production, de gestion d'infrastructures, mais aussi dans les systèmes médicaux. Ces entités, qui s'appuient sur des systèmes opérationnels ouverts vers l'extérieur, sont de plus en plus exposées aux menaces et aux risques cyber. Nous avons, en effet, tous entendu parler des hôpitaux qui ont été victimes de cyberattaques et de ransomware ! Cette sécurisation de l'OT est un de nos principaux leviers de différenciation et représente un des enjeux clés en matière de cybersécurité sur le court et le moyen terme.
Très souvent, les ressources qui opèrent ces systèmes ne maîtrisent pas forcément les enjeux relatifs à la cybersécurité. Fort de ce constat, Wallix place ainsi la simplicité et l'accessibilité de ses solutions au cœur de sa vision afin de contribuer à l'adoption des bonnes pratiques pour prévenir le risque cyber.

Quel est le rôle de la sécurisation des accès dans la chaîne de valeur de la cybersécurité ?

En matière de cybersécurité, aujourd'hui, il y a deux approches : la protection, d'une part, et les systèmes de détection et de réponse, d'autre part. Face à l'ampleur de la menace, il est évident que les entreprises doivent opter pour une combinaison de ces deux dimensions.
Plus particulièrement, dans le volet protection, on retrouve quatre briques : la gestion des identités, la gestion des accès (authentification, identification biométrique...), l'administration et la gouvernance des identités qui sont des solutions qui permettent aux entreprises de définir leur politique d'accès pour les utilisateurs internes et externes et sa gestion dans la durée (arrivée, évolution et départ des collaborateurs...), la gestion des accès à privilège. Cette dernière brique est au cœur de nos solutions et nous permet d'offrir aux entreprises un très fort niveau de sécurité pour sécuriser l'accès ; enregistrer l'activité des utilisateurs sur le système ; auditer et assurer la conformité réglementaire ; gérer les mots de passe.

Quels sont vos forces et vos principaux vecteurs de différenciation ?

En matière de gestion des accès à privilèges aussi appelée Priviledged Access Management (PAM), Wallix est un acteur reconnu sur le marché pour sa fonctionnalité de gestion des sessions, c'est-à-dire l'enregistrement de l'activité des utilisateurs sur le réseau pour analyser leurs comportements, détecter les failles et assurer la conformité aux politiques de sécurité. Nous sommes un des six acteurs leaders en matière de PAM selon Gartner, mais aussi le seul acteur européen de ce palmarès.
Alors que les entreprises poursuivent la digitalisation de leurs accès, notre maîtrise des technologies PAM nous permet de proposer un très haut niveau de sécurité pour la gestion d'accès de l'ensemble des utilisateurs. En effet, notre solution couvre l'ensemble des fonctionnalités attendues par les clients. En parallèle, notre offre est certifiée par les principaux organismes européens, dont l'ANSSI en France. Wallix est aussi le seul acteur du segment PAM à être certifié CSPN. Nous sommes aussi actuellement en cours de certification BSI. La certification est un important levier de différenciation alors que les différentes réglementations imposent aux opérateurs de services essentiels en Europe de mettre en œuvre des solutions de cybersécurité certifiées.
Comme précédemment mentionné, au cœur de notre valeur ajoutée, on retrouve l'importance que nous accordons à la facilité de déploiement de nos solutions. Nous disposons, en effet, de brevets sur l'architecture de notre solution qui nous permettent de la déployer sans avoir à faire intervenir des agents sur les serveurs. Nous fournissons à nos clients des solutions packagées qui peuvent être installées directement sur un serveur. Cela permet, par ailleurs, d'optimiser les coûts pour nos clients.
Enfin, on retrouve aussi notre positionnement sur l'OT avec des fonctionnalités particulières que nous avons développées en interne pour appréhender ces systèmes industriels. On peut notamment citer la technologie Universal Tunneling qui permet d'encapsuler les protocoles industriels pour permettre aux tiers mainteneurs d'accéder au système de façon sécurisée.

Et pour conclure, quelles sont vos perspectives ?

Nous avons de très fortes ambitions de développement. En 2021, nous avons annoncé notre plan stratégique Unicorn 25 qui s'articule autour de plusieurs objectifs que nous nous sommes fixés à horizon 2025. Nous visons notamment un chiffre d'affaires de 100 millions d'euros en 2025 et, pour ce faire, nous nous concentrons sur quatre axes porteurs : la croissance intrinsèque du marché de la cybersécurité et du PAM ; le développement à l'international ; le renforcement de notre offre en matière d'OT avec notre nouvelle marque OT.security et notre volonté de proposer aux industriels des solutions de cybersécurité by design ou par défaut ; une offre complète qui intègre des briques complémentaires pour permettre à nos clients d'avoir une vision globale et unifiée de la sécurité de leur système d'information.