INTÉGRATION ET AUTOMATISATION : l'avenir de la cybersécurité

Acteur majeur de la cybersécurité, ***Fortinet*** se caractérise par une approche unifiée qui apporte une synergie dans les éléments de sécurité tout en offrant une simplicité d'utilisation pour les professionnels. ***Christophe Auberger, évangéliste cybersécurité***, nous explique la spécificité de cette approche.

Christophe Auberger

Bio express
Après avoir travaillé dans la mise en place de systèmes de contre-mesures de la Marine nationale, Christophe Auberger a fait sa carrière dans les systèmes d'information et la cybersécurité. Il a rejoint Fortinet en 2005, où il est aujourd'hui évangéliste cybersécurité.

"Dans les systèmes complexes, même au-delà de la cybersécurité, la configuration est capitale : la meilleure solution du monde reste inefficace si elle est mal configurée."

La cybersécurité relève-t-elle pour vous exclusivement des systèmes d'information ou bien a-t-elle pris une plus grande ampleur ?
Nous avons toujours eu une approche globale. La cybersécurité est une fonction transverse. C'est un peu comme la qualité. Nous avons toujours besoin de spécialistes dans un domaine, mais il faut se garder d'une approche trop restrictive : si nous confions la sécurité uniquement aux équipes chargées des systèmes d'information ou même de la sécurité, cela ne fonctionne pas. Aujourd'hui, c'est devenu un enjeu stratégique pour tous, d'autant que l'adoption du numérique par les organisations s'est généralisée. Un système d'information qui n'est pas fonctionnel va nécessairement soit arrêter la production, soit la perturber suffisamment pour créer des impacts majeurs dans le fonctionnement de l'entreprise, sans parler des préjudices économiques et d'image.

Dans ce contexte, comment le problème se pose-t-il pour une organisation ?
La cybersécurité devient un enjeu stratégique alors même que le système d'information est de plus en plus exposé, parce que les entreprises sont contraintes de l'ouvrir aux fournisseurs ou prestataires, de donner accès à des collaborateurs extérieurs, à des partenaires, à des clients, etc. On se retrouve donc à une croisée des chemins. Du fait des nouveaux usages, des nouvelles façons de travailler, les entreprises ont plongé dans le numérique, augmentant considérablement la surface d'attaque pour les cybermenaces. Le milieu s'est structuré et professionnalisé. Cet écosystème de cyber attaquants fonctionne, et il est très efficace. Prenons l'exemple des rançongiciels : on estime qu'aujourd'hui qu'un peu plus d'un quart des victimes payent la demande de rançon. Les organisations se trouvent donc en quelque sorte prises dans un étau. D'un côté, il faut être de plus en plus ouvert, plus performant, plus interopérable, et de l'autre la pression de la menace est de plus en plus forte, pilotée par des groupes criminels ou même par des États dans le cadre d'un espionnage industriel, d'une guerre économique, d'une tentative de déstabilisation. La cybersécurité est donc devenue un enjeu primordial pour tout type d'organisation, quel que soit l'échelle ou le secteur.

Comment réussir à se protéger dans l'environnement que vous décrivez ?
Nous avons constaté que, pendant longtemps, les approches des organisations se faisaient en silo. Les entreprises ont déployé des processus, des personnes, des technologies pour se protéger, mais sans véritable synergie interne. Les choix se portaient vers les meilleures technologies ou considérées comme telles, avec des pare-feux, des filtrages de flux, des systèmes IPS ou IDS qui surveillaient les tentatives d'intrusion, des systèmes anti-malwares, etc. Or, ces technologies peuvent être pertinentes dans leur domaine, mais si elles ne communiquent pas entre elles, l'ensemble demeure inefficace. Par conséquent, la charge des équipes augmente, et la complexité aussi. Or, la sécurité doit rester simple pour être efficace. Quand elle devient compliquée, elle remplit moins son rôle.
Nous avons donc conçu une approche qui puisse s'intégrer dans une sorte de framework et qui apporte une synergie entre ces fonctions. Nous concevons des solutions de cybersécurité avancées et complètes, telles des firewalls de nouvelle génération, des systèmes de sandboxing, de détection d'intrusion, et notre force réside dans ce que ces éléments s'intègrent

dans une architecture commune que l'on appelle Fortinet Security Fabric, plateforme où l'on vient "brancher" tous les outils de sécurité entre eux. Cette conception intégrée a une importance vitale : elle permet d'apporter de la simplicité, et une capacité de gouvernance centralisée sur l'ensemble des fonctions de sécurité de l'organisation.

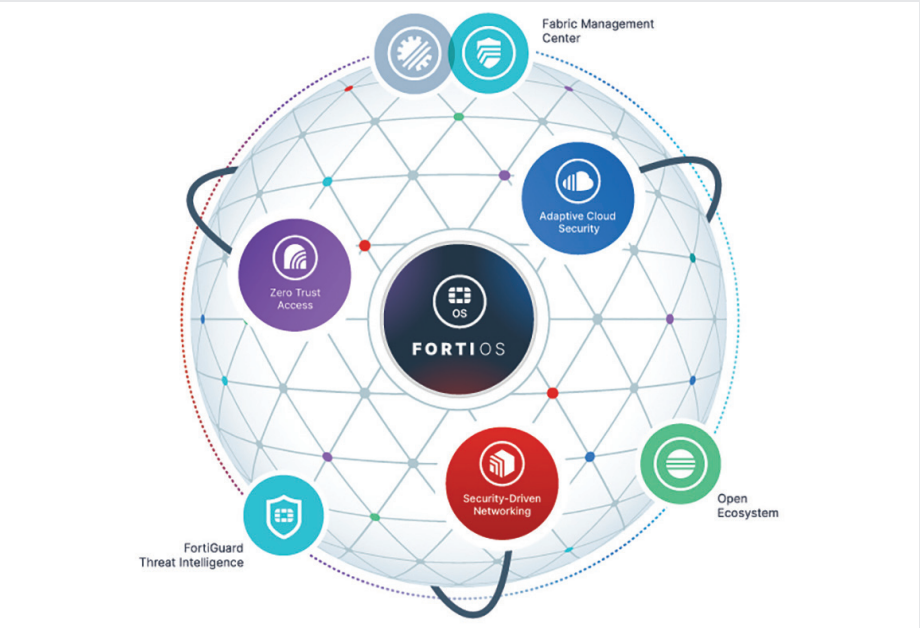
Cette plateforme est-elle dédiée exclusivement aux outils Fortinet ?

Elle fonctionne avec nos solutions, bien évidemment, mais aussi avec les solutions d'autres éditeurs. L'idée de fond est de rendre possible une automatisation et une intégration de la sécurité qui en masque la complexité et permette aux clients d'avoir une gestion et une visibilité de bout en bout.

Une tendance forte aujourd'hui va même encore plus loin : c'est la convergence réseau et sécurité, avec des offres comme le SD-WAN ou SASE, qui intègrent à la fois les réponses aux problématiques de sécurité, et la sécurisation des flux. Aujourd'hui, les clients ont besoin d'une infrastructure de communication souple, flexible, agile pour répondre aux enjeux des métiers. Il y a eu un changement essentiel ces dernières années : ce sont les métiers qui pilotent l'informatique, et les DSI sont au service des métiers. Il faut donc de notre côté être capable de s'adapter rapidement. La tendance ira toujours plus vers une intégration de la sécurité de bout en bout. On parle beaucoup depuis quelques années du security by design. On en est encore loin, mais il y a des avancées, des percées, qui témoignent de la prise de conscience de ces enjeux à tous les niveaux de l'organisation.

Faut-il refondre la structure des systèmes d'information ?

Aujourd'hui, nous ne maîtrisons plus les systèmes d'information, à cause de l'adoption du cloud et de la mobilité des utilisateurs, notamment. Les frontières du système d'information sont floues, mouvantes : on a du mal à les définir. En termes de cybersécurité, la seule bonne approche consiste à se concentrer sur la donnée. C'est elle qui a de la valeur, elle qui sera chiffrée, qui peut être volée. Et cette donnée peut être aujourd'hui dans un centre de données privé, virtualisé ou non, dans le cloud public, chez un collaborateur de l'entreprise, chez moi... C'est donc sur elle qu'il faudra travailler pour pouvoir la protéger, où qu'elle se trouve. Et cela nécessite d'avoir une vision transverse de la sécurité, avec un pilotage intégré.



C'est une vision qui semble très partagée dans le secteur de la cybersécurité...

On en parle beaucoup, mais est-ce que les entreprises sont vraiment capables de déployer leurs systèmes de sécurité de manière automatique, de les activer, de les configurer à mesure que les infrastructures bougent ? C'est d'une importance primordiale, car les entreprises ont énormément de mal à recruter en cybersécurité, et à retenir leurs talents. L'automatisation est donc un enjeu lié aux ressources humaines, et elle permet aussi de dégager du temps pour l'analyse du risque proprement dite : le but est de ne soumettre aux analystes humains que ce qui a un score de probabilité d'attaque élevé.

Quels sont vos grands axes de développement actuels ?

En premier lieu, ce qui tourne autour de l'automatisation et de l'intégration. Ensuite, nous nous servons des développements de l'intelligence artificielle dans différents domaines : d'abord pour faire du profilage (analyse comportementale). Nous utilisons également le deep learning pour la gestion des vulnérabilités et des malwares, ce qui nous permet parfois de les détecter avant même qu'ils n'apparaissent ; mais aussi pour configurer les équipements. Dans les systèmes complexes, même au-delà de la cybersécurité, la configuration est capitale : la meilleure solution du monde reste inefficace si elle est mal configurée. En plus d'être complexes, les environnements évoluent : il faut donc revoir régulièrement les configurations.

Fortinet est une société américaine, mais avec une forte présence en France. Quels sont les atouts que vous tirez de cette particularité ?

Fortinet est effectivement une entreprise internationale, implantée partout dans le monde. Cela nous permet à la fois de bénéficier d'une synergie au niveau global, d'avoir un niveau de recherche et développement très avancé et d'être au plus près des problématiques locales de nos clients et de nos partenaires, pour apporter des solutions personnalisées.

EN BREF

9 043 employés, dont près de 400 en France. Fondée en 2000, avec un siège social à Sunnyvale, Californie, Fortinet propose des solutions de cybersécurité intégrées sur l'ensemble de l'infrastructure IT.