

## Des solutions et une architecture de sécurité Fortinet pour sécuriser le passage à la 5G

*La Security Fabric de Fortinet offre l'évolutivité, la visibilité et le contrôle nécessaires aux environnements cloud, ainsi que des performances optimales et la sécurisation des réseaux 4G en évolution, des services liés à l'IoT et de la plateforme de mobilité 5G.*

*« Avec la 5G, l'innovation transforme les infrastructures mobiles en une plateforme, véritable moteur de création de valeur et d'innovation pour les services. Tout au long de cette transformation, l'architecture et les solutions de sécurité éprouvées de Fortinet déploient une sécurité évoluée pour les différents cas d'usage des réseaux LTE, LTE-A et 5G. Les infrastructures mobiles sont ainsi sécurisées, des réseaux d'accès radio RAN aux environnements cloud des opérateurs. De leur côté, les clients bénéficient de performances et de capacités de fiabilité carrier-grade, ainsi que d'une évolutivité, d'une visibilité et d'un contrôle optimisés pour le Cloud. »*

**John Maddison, Executive Vice President, Produits et Solutions, Fortinet**

### **L'essentiel :**

Fortinet (NASDAQ: FTNT), un leader des solutions de cybersécurité automatisées, intégrales et intégrées, annonce de nouvelles fonctionnalités pour sécuriser l'évolution vers la 5G, proposées par un panel de solutions dédiées à la sécurité des cœurs de réseau mobiles et des infrastructures cloud. La technologie de processeur SPU virtuel et les systèmes de sécurité évoluée et hautes performances de Fortinet comptent parmi ces solutions. Avec ses promesses d'une connectivité plus rapide, d'une évolutivité optimale et de nouvelles opportunités commerciales, la 5G impactera profondément la mobilité et la transformation numérique. Fortinet propose à ses clients une sécurité évoluée et des systèmes hautes performances offrant une fiabilité optimale, une visibilité granulaire et un contrôle précis, autant d'atouts pour sécuriser les cœurs de réseau mobiles, les environnements cloud dédiés au Edge Computing (Edge Cloud) et les infrastructures de l'Internet des Objets (IoT).

### **La 5G, un vecteur d'opportunités...Et de risques**

La 5G apportera la connectivité nécessaire à toutes les facettes de nos vies. Pour de nombreux cas d'usage à venir, dont certains s'affichent vraiment futuristes, à l'instar des véhicules autonomes, des expériences immersives de réalité virtuelle ou augmentée ou des villes connectées, il semblerait que les niveaux attendus de performances, de latence et de rapidité ne soient pas encore au rendez-vous. Inévitablement, ces différents cas d'usage seront interconnectés. Cependant, la prise en charge d'un volume élevé de connexions, associé à des performances nécessaires et à une latence ultra-faible n'est pas encore une réalité sur le terrain.

Avec la 5G et les évolutions majeures à venir en matière de bande passante, de connectivité et de cas d'usage, les opportunités d'innover sont nombreuses : la plateforme mobile devient un levier de création de valeur et d'innovation pour les services. Plus que jamais, les opérateurs de réseaux mobiles évolueront vers un rôle de facilitateur de business, dans un contexte sécurisé. À titre d'exemple, de

nouvelles opportunités commerciales se présenteront aux fournisseurs de services dans les domaines de l’IoT : automatisation des processus de production, télémétrie industrielle, systèmes d’alerte en urgence, chirurgie assistée par robotique, streaming vidéo en 4K UHD et davantage. Cependant, ces innovations entraîneront un impact plus lourd des attaques de déni de service, des menaces évoluées et autres cyber-attaques ciblant le cœur de réseau en lui-même. La sécurité est devenue un impératif pour protéger et exploiter des réseaux 4G et 5G en pleine évolution. Ces nouveaux cas d’usage de service exigent des fonctionnalités de sécurité qui ne se limitent pas au pare-feu, ainsi qu’un respect des objectifs de haute disponibilité et de qualité d’expérience, tels que spécifiés dans les accords de niveau de service SLA.

### **Les atouts de la sécurité Fortinet pour la 5G**

Fortinet propose des solutions de sécurité conçues sur mesure pour répondre aux défis des opérateurs migrant leur cœur de réseau afin de proposer des services 4.5G et 5G. Ces solutions définissent un framework de sécurité qui optimise les coûts de lancement et d’exploitation de nouveaux services, fait émerger de nouvelles opportunités commerciales, neutralise les menaces avancées et assure le respect des objectifs SLA.

Les fournisseurs de services tireront pleinement parti de ces atouts grâce aux systèmes de sécurité évolués et performants de Fortinet. Ces derniers apportent aux opérateurs mobiles une meilleure visibilité fondée sur un traitement analytique pertinent des données de sécurité, ainsi que la possibilité de neutraliser les menaces de sécurité externes et internes qui pèsent lourdement sur les infrastructures et les services réseau.

La plateforme de sécurité de Fortinet invite les fournisseurs de services 5G à capitaliser sur les avantages suivants :

- **Protection évoluée pour le cœur de réseau mobile et les environnements cloud des opérateurs télécoms** : optimisées par la technologie Virtual SPU de Fortinet, les fonctions VNF (Virtual Network Functions) de FortiGate renforcent sensiblement les performances de la sécurité applicative, grâce à une optimisation des tâches de sécurité et des technologies de dernière génération qui accélèrent le traitement des paquets. Ces fonctions VNF légères sont activées en quelques secondes et permettent aux fournisseurs de services de protéger leurs réseaux virtualisés et plateformes cloud, à un coût parfaitement maîtrisé. De plus, les pare-feux nouvelle-génération FortiGate 7000, prêts pour la 5G, bénéficient d’une accélération SPU et apportent aux opérateurs des fonctions d’inspection SSL et une sécurité applicative performante, dans le cadre d’une protection intégrée de type inline. Ensemble, ces solutions Fortinet offrent le meilleur en termes d’évolutivité et de capacités pour protéger les infrastructures 5G contre les attaques sophistiquées sur la couche applicative et les nombreuses attaques par déni de service, menées de l’intérieur ou de l’extérieur du cœur mobile ou du réseau de l’opérateur.
- **Agilité et sécurité** : Fortinet propose une intégration étroite avec de nombreux fournisseurs de solutions NFV et SDN dédiées aux infrastructures virtuelles. Pour offrir une sécurité de bout en bout à l’aide de services 5G innovants, comme le network slicing et multi-access edge computing (MEC) notamment, les fonctions VNF doivent être fournies en temps réel, instanciées rapidement et opérationnelles sur l’ensemble du périmètre réseau. Pour un déploiement et une utilisation efficaces et agiles de ces ressources de sécurité, Fortinet propose des intégrations

avec des fournisseurs de plateformes NFV tels que Lenovo, les systèmes d'orchestration NFV (MANO) proposés par Amdocs, Ericsson, Ciena, UBiqube, NoviFlow et les contrôleurs SDN comme VMware NSX, Nokia Nuage, Cisco ACI et NoviFlow.

- **Visibilité en profondeur et contrôle sur les services IoT sur les edge clouds** : les objets connectés déployés à grande échelle utilisent généralement des systèmes d'exploitation légers dont les fonctions de sécurité sont minimales. Ces dispositifs sont donc souvent vulnérables aux tentatives de piratage et aux attaques par botnet. Pour maîtriser les risques, les données de ces endpoints et les dispositifs en eux-mêmes doivent être parfaitement protégés. De plus, les fournisseurs de service offrant des services IoT via une plateforme cloud doivent s'assurer du cloisonnement de leurs environnements multi-tenant, de la sécurité de leurs containers et VM et de la protection de leurs applications Web. Fortinet FortiGate NGFW VNF et FortiWeb WAF VNF protègent la plateforme edge cloud. FortiSIEM offre une visibilité intégrale sur le traitement analytique et la corrélation de données de sécurité, ainsi d'une visibilité complète pour identifier les objets connectés pendant que FortiGate découvre et assure le profiling de tous les dispositifs connectés et applique un contrôle précis sur les différentes classes d'objets connectés.

### Disponibilité

La Security Fabric et les solutions de Fortinet dédiées à la sécurité des réseaux mobiles des opérateurs, de l'IoT et des services applicatifs sont d'ores et déjà disponibles.

### Verbatims de marché

*“La collaboration technologique et stratégique de Lenovo avec Fortinet - axée sur l'intégration de la plateforme NFVi de Lenovo et la sécurité optimale de Fortinet – offre une solution intégrée agile, flexible et sécurisée pour répondre aux besoins changeants des CSPs (Communication Service Providers).”*

**Charles Ferland, vice president & general manager, Telco chez Lenovo Data Center Group**

*“Partenaire technologique Fabric-Ready de Fortinet et leader d'orchestration multi domaines, nous sommes ravis de nous associer à Fortinet en vue d'architectures sécurisées MEC (Mobile edge computer) et 5G. La solution commune UBiqube et Fortinet permet l'insertion et l'automatisation de fonctionnalités de sécurité pour tout service de 5G, comme l'IoT ou le M2M.”*

**Nabil Souli, PDG chez UBiqube**

*“NoviFlow et Fortinet s'engagent auprès de leurs clients à accélérer l'innovation pour leur apporter des solutions de premier rang. En tant que partenaire technologique Fabric-Ready de Fortinet, nous offrons à nos clients une protection de premier rang, assurée par la Security Fabric, pour ainsi sécuriser la migration vers la 5G. Notre solution commune associe NoviFlow et les technologies Fortinet pour garantir des performances élevées et des services évolutifs en temps réel, au sein d'un environnement réseau SDN programmable. C'est ainsi que nous répondons aux besoins des réseaux des opérateurs et des fournisseurs de services. La solution est indiquée pour les environnements d'envergure et favorise une évolutivité économique et dynamique qui dimensionne les capacités selon une demande très fluctuante.”*

**Domonique Jodoin, President et CEO chez NoviFlow Inc.**

## Ressources complémentaires

- Pour plus d'information sur cette annonce, merci de consulter notre [blog](#)
- Consultez l'étude [5G Security Survey](#) par Heavy Reading
- Consultez notre livre blanc [Securing 4G, 5G and Beyond](#)
- Pour en savoir davantage sur comment [sécuriser le passage à la 5G](#) avec Fortinet
- Plus d'information sur notre système d'exploitation [FortiOS](#), Forti Carrier OS, les fonctions [VNFs de FortiGate](#), la gamme des pare-feux nouvelle-génération [FortiGate](#) et FortiCarrier, [les services de sécurité FortiGuard](#), le pare-feu d'application web [FortiWeb](#) et les plateformes d'information et de gestion d'événements [FortiSIEM](#)
- Découvrez ce qu'est la [Security Fabric](#) de Fortinet et la [troisième génération de la sécurité réseau](#)
- Consultez notre [blog](#) pour découvrir le tout dernier rapport de sécurité Fortinet Global Threat Landscape ou en savoir davantage sur [FortiGuard Labs](#) et les [services de sécurité](#) FortiGuard

## À propos de Fortinet

Fortinet (NASDAQ: FTNT) assure la sécurité des entreprises, fournisseurs de services et administrations parmi les plus grandes au monde. Fortinet apporte à ses clients une protection intelligente et transparente, véritable ligne de défense d'une surface d'attaque qui s'étend. Cette sécurité affiche des performances pérennes, adaptées aux réseaux découplés actuels et à venir. Seule l'architecture Security Fabric de Fortinet est capable de déployer une sécurité sans compromis pour relever les défis de sécurité les plus critiques au sein des environnements réseaux, applicatifs, cloud ou mobiles. Fortinet est le leader parmi de nombreuses appliances de sécurité commercialisées dans le monde. Plus de 375 000 clients mondiaux font aujourd'hui confiance à Fortinet pour les protéger. Pour en savoir davantage : <http://www.fortinet.com>, le [blog](#) Fortinet ou [FortiGuard Labs](#).