

Défis imposés par le marché

Afin de répondre aux attentes des entreprises modernes, il est nécessaire de mettre en œuvre plus rapidement les modifications du réseau:

- Complexité** - Les topologies complexes viennent s’ajouter à la complexité des configurations de dispositifs réseau et ralentissent l’implémentation des modifications du réseau – généralement, il s’écoule au moins une semaine entre l’ouverture d’un ticket et son implémentation.

- Modifications constantes** - Les applications métier changent au quotidien et nécessitent la modification concomitante de la configuration du réseau.

- Collaboration** - Les équipes chargées respectivement des applications et du réseau ne parlent pas le même langage technique, et les requêtes de modification sont souvent mal comprises. Par conséquent, des erreurs sont commises et de nombreuses modifications doivent être effectuées à nouveau, ce qui entraîne une perte de temps.

Ces réalités engendrent deux sortes de risques:

- Connectivité** - Les changements de configuration qui entravent les connexions essentielles peuvent provoquer un temps d’arrêt ou une panne.

- Conformité et sécurité** -Tout nouvel accès au réseau octroyé peut entraîner une violation des stratégies de conformité et des risques de sécurité pour le réseau.

Tendances du marché

Les trois tendances actuelles de l’informatique sont les suivantes:

- Centre de données virtualisé/défini par logiciel (SDDC)**
- Informatique en nuage**
- VEC (Apportez Votre Équipement personnel de Communication)**

Les modifications constantes de la sécurisation du réseau sont inhérentes à ces modèles car des applications et dispositifs nouveaux sont constamment déployés. Tufin accroît la valeur ajoutée de ces initiatives en accélérant la connectivité, ce qui permet une modification centralisée et automatisée du réseau tout en préservant la sécurité du processus.

L’évolution constante des menaces provoque encore et toujours une demande croissante en sécurité. Les pare-feu, tant classiques que de nouvelle génération, restent le dispositif de sécurisation fondamental, ce qui explique leur expansion. Ils doivent donc être gérés et surveillés, et garantir la mise en application des stratégies de sécurité sur l’ensemble du réseau afin de minimiser l’exposition de ce dernier.

Acheteurs cibles

- Hauts responsables** - DSI, RSSI, directeurs de services informatiques, de l’ingénierie, du réseau et de la technologie

- Exploitation réseau** - V.-P./dir./resp. des opérations réseau, dir./resp. de la sécurité réseau, resp. des pare-feu, architectes réseau, chefs de projet réseau, dir./architectes de l’automatisation.

- Sécurité** - Dir./resp. des opérations de sécurité, architectes/resp. de la sécurité, dir./resp. de la sécurité informatique, chefs de projet sécurité, équipes Menaces et vulnérabilités, ingénieurs sécurité

Tufin en bref

Année de création: 2005

Bureaux: Amérique du Nord, Europe et Asie-Pacifique

Clients: plus de 1 300, répartis dans plus de 50 pays

Principaux secteurs: finances, télécommunications, énergie et bâtiment, vente au détail, administrations, secteur pharmaceutique, transport et sociétés d’audit

Partenaires commerciaux: plus de 240 dans le monde entier

Programme de formation et de certification: Plus de 1 600 participants du monde entier aux cours Tufin Certified Security Expert (TCSE), le seul programme de formation dédié à la maîtrise des solutions d’orchestration des stratégies de sécurité

Partenaires technologiques: Check Point, Cisco, Juniper, Fortinet, F5, Palo Alto Networks, McAfee, BMC, Blue Coat et Linux IPTables, entre autres more

Récompenses

SC Magazine

- Présentation et analyse de produit (5 étoiles sur 5) en 2013

Network Products Guide 2013

- Vainqueur des catégories ‘Entreprise la plus innovante’

‘Meilleure expansion commerciale’ et ‘Entreprises à suivre’

Info Security Products Guide 2013

- Médaille de bronze des ‘Global Excellence Awards’ pour SecureApp

Info Security Products Guide 2014

- Médaille d’or des ‘Global Excellence Awards’
- Médaille d’or (Amérique Latine) et médaille de bronze (États-Unis) de ‘Tomorrow’s Technology Today’ en 2014
- Médaille d’or dans la catégorie ‘Meilleur déploiement en EMEA’ de SIX



SecureTrack

Bref argumentaire

Les réseaux d’entreprise actuels comportent des milliers de dispositifs hétérogènes dont les nombreuses stratégies de sécurité complexes sont régulièrement modifiées afin de répondre aux besoins des activités. La solution de gestion coordonnée des pare-feu et dispositifs réseau SecureTrack™ permet aux responsables du réseau et de la sécurité de surveiller et d’analyser les stratégies de sécurité de pare-feu provenant de multiples fournisseurs, d’en optimiser et recertifier les règles, ainsi que de suivre les modifications afin de garantir une conformité constante.

Principales fonctionnalités

- Gestion centralisée et unifiée de tous les pare-feu et routeurs provenant des fournisseurs leaders
- Nettoyage des règles - détection des règles et objets non utilisés dans les configurations des pare-feu et dans les listes de contrôle d’accès des routeurs
- Détection, alertes et rapports sur les modifications
- Conformité constante aux normes, notamment PCI DSS et SOX
- Rapports d’audit intégrés
- Intelligence de la topologie du réseau, pour une configuration rapide et précise
- Analyse de l’impact des risques avant configuration des modifications dans les stratégies
- Documentation et recertification des règles

Principaux avantages

- Visibilité et contrôle centralisés des modifications réseau dans les environnements complexes
- Analyse précise et efficace des modifications de la sécurité réseau, pour une réduction des temps d’arrêt
- Accélération de la préparation des audits
- Garantie du respect des stratégies de l’entreprise par toutes les stratégies et modifications de la sécurité réseau, pour une gestion efficace des risques



SecureChange

Bref argumentaire

Les organisations informatiques sont confrontées chaque semaine à des dizaines de demandes de modification de la configuration réseau. Il leur est quasiment impossible de suivre la cadence et d’assurer un service rapide tout en garantissant la sécurité et la conformité de chaque modification, ainsi que la disponibilité constante des applications. SecureChange™ permet aux entreprises de relever ce défi en automatisant les modifications de configuration des pare-feu et routeurs du réseau, de la conception à la vérification en passant par l’exécution, et ceci en évaluant l’impact des risques de manière proactive avant la mise en œuvre de toute modification.

Principales fonctionnalités

- Automatisation de la conception des modifications, en fonction de la topologie
- Analyse proactive de l’impact des modifications, simulation de l’impact sur les risques et sur la conformité des modifications proposées, avant et après implémentation
- Possibilité d’automatisation de l’implémentation des modifications des pare-feu
- Flux d’opérations personnalisés illimités
- Intégration aux systèmes de tickets et d’assistance, notamment avec Remedy et ServiceNow

Principaux avantages

- Réduction considérable de la durée d’implémentation des modifications réseau
- Mise en application coordonnée des processus pour une modification plus rapide de la sécurité réseau
- Processus rapide, précis et vérifiable d’application de la sécurité réseau
- Aucun compromis entre efficacité opérationnelle et sécurité
- Minimisation de l’impact des risques pour les modifications réseau



SecureApp

Bref argumentaire

Les tendances actuelles telles que la virtualisation et l’informatique en nuage accélèrent la fréquence et la cadence de déploiement des applications. En conséquence, les professionnels de la sécurité réseau consacrent désormais la majorité de leur temps à la mise en œuvre de modifications liées aux applications et au diagnostic des problèmes de connectivité réseau. La solution automatisée Tufin SecureApp™ permet aux entreprises de définir, mettre à jour, surveiller et supprimer des applications et des services du réseau afin d’accélérer la fourniture des services, d’assurer la continuité des activités et de simplifier les opérations réseau.

Principales fonctionnalités

- Facilité de définition et de déploiement de la connectivité des applications sur le réseau
- Automatisation de la découverte des applications
- Surveillance de l’état de connectivité des applications et résolution des problèmes
- Rapidité d’intégration et de mise hors service des applications

Principaux avantages

- Visibilité et contrôle de la connectivité des applications sur l’ensemble du réseau
- Flexibilité des activités grâce à l’accélération du déploiement, de la migration et de la mise hors service des applications
- Amélioration de la communication entre les équipes applications et les équipes réseau
- Amélioration de la continuité des activités et réduction du temps moyen de reprise pour les arrêts des applications liés au réseau

Réponses aux objections

Nous ne disposons pas du budget nécessaire/Cela nous reviendrait trop cher.

Le ROI de la solution est très élevé. L’accélération de la fourniture de services informatiques par la mise en œuvre plus rapide des modifications renforce la rentabilité globale de l’entreprise. Outre la garantie d’efficacité opérationnelle, chaque modification est comparée aux stratégies de conformité et de risque de l’entreprise afin de veiller à l’absence de risque dissimulé sur vos réseaux et d’éviter les temps d’arrêt des applications par suite d’une modification du réseau.

Nous allons développer SecureApp/SecureChange nous-mêmes.

Autrefois, en l’absence de solution, les entreprises tentaient d’en développer une elles-mêmes. Nous sommes les pionniers du secteur et en avons créé les standards de référence, en développant notre solution plus rapidement et en l’adaptant aux besoins de tous les clients : nous avons investi des années de développement dans nos produits et poursuivons leur extension. Nous possédons l’expertise requise en matière d’analyse de la topologie du réseau et d’assistance pour les pare-feu des divers fournisseurs. Nous sommes également en mesure d’intégrer nos fonctionnalités avancées à l’aide de nos services (API), afin de mettre nos capacités uniques à la disposition de votre solution développée en interne.

Nous ne faisons appel qu’à un ou deux fournisseurs de pare-feu. Même si vous recourez à un seul fournisseur de pare-feu : est-ce que votre logiciel actuel de gestion des pare-feu vous avertit si les modifications apportées (ou sur le point de l’être) sont incorrectes, ou si elles risquent de violer des normes de sécurité de votre entreprise, ou encore si elles introduisent de nouveaux risques dans votre réseau ? Les fournisseurs de pare-feu vous permettent d’apporter des modifications, mais ne vous informent ni sur leur pertinence, ni sur leur éventuel impact. Nous proposons des fonctionnalités de gestion et d’analyse bien supérieures à celles des fournisseurs de pare-feu, par exemple la simulation de l’impact des demandes de modification sur la sécurité, la conformité et les temps d’arrêt. Nous pouvons également étendre la gestion de la sécurité des pare-feu aux processus automatisés, afin de diminuer le nombre d’erreurs humaines et d’améliorer l’efficacité.

Je n’ai pas le temps de réaliser une démonstration de faisabilité, je dois déjà migrer les pare-feu et en installer de nouveaux, en préparation d’un audit.

Vous pouvez utiliser SecureTrack sur un nombre réduit de pare-feu, ce qui ne vous prendra que quelques heures. Vous constaterez immédiatement la valeur de cette solution pour la gestion, la surveillance et la vérification de vos pare-feu. Vous avez également la possibilité d’utiliser SecureTrack lors du processus de migration : vous bénéficierez ainsi d’une visibilité accrue et pourrez nettoyer les bases de règles du pare-feu et définir de nouveaux jeux de règles améliorés.

Je suis persuadé que les logiciels de gestion de Check Point, Palo Alto, Fortinet ou encore Juniper peuvent également accomplir tout ce que vous affirmez pouvoir faire.

Est-ce que votre logiciel de gestion des pare-feu actuel vous avertit si les modifications apportées (ou sur le point de l’être) sont incorrectes, ou si elles risquent de violer des normes de sécurité de votre entreprise, ou encore si elles introduisent de nouveaux risques dans votre réseau ? Les fournisseurs de pare-feu vous permettent d’apporter des modifications, mais ne vous informent ni sur leur pertinence, ni sur leur éventuel impact. Est-ce que votre logiciel de gestion actuel établit votre topologie en y incluant tous les autres dispositifs réseau ? Tufin possède d’excellentes capacités de coordination de l’ensemble des stratégies de sécurité, indépendamment du fournisseur, afin de vous aider à gérer l’intégralité de votre réseau via un système centralisé.

Nous ne faisons pas confiance à un système qui effectue des modifications automatiques sur nos pare-feu, ou nous ne sommes pas autorisés à utiliser un tel système.

SecureTrack n’apporte aucune modification à votre pare-feu, mais se limite à surveiller les activités et à envoyer des alertes afin de renforcer la gestion des risques et le contrôle des modifications réseau. Avec SecureChange, vous pouvez choisir de ne pas implémenter l’intégralité d’une modification, tout en bénéficiant d’une simulation des risques et de recommandations qui peuvent ensuite être mises en œuvre manuellement.

Nous disposons déjà d’un système de tickets, pourquoi aurions-nous besoin d’un autre?

Votre système de tickets actuel n’analyse pas l’impact des risques engendrés par les modifications réseau avant leur implémentation, et il ne vérifie pas non plus si la modification a été implémentée telle que souhaité. Nous intégrons les systèmes de tickets leaders afin de relayer le processus en charge lorsqu’une demande d’accès au réseau est soumise.

Nous n’avons pas le temps de mettre en place une telle solution, nous nous en sortons bien avec notre processus actuel.

Combien de vos projets sont-ils en suspens parce que l’équipe informatique est trop occupée ? Tufin peut vous aider à reprendre le contrôle sur les modifications et à gagner du temps, même durant la démonstration de faisabilité. Avec l’aide de nos services professionnels, l’installation ne sera qu’une question de jours. Grâce à ses flux d’opérations flexibles, cette solution prend en charge vos processus actuels et en garantit la mise en application et la documentation à fins d’audit.

Vous n’intégrez pas la gestion des vulnérabilités.

Cela figure sur notre feuille de route, et nos API ouvertes nous permettent d’intégrer toutes sortes de solutions. Si vous recherchez la solution la plus complète pour des modifications sécurisées et précises du réseau pouvant également être automatisées, Tufin a déjà fait ses preuves dans plus de 1 300 entreprises.

Les flux d’opérations sont gérés par un autre service, nous ne sommes chargés que des modifications aux pare-feu.

Nous sommes en mesure d’intégrer des systèmes de flux d’opérations existants. Nous pouvons concevoir la modification réseau recommandé afin d’en garantir une implémentation précise, ce qui réduit les risques d’exposition inutile du réseau ou de temps d’arrêt.

Nous possédons un outil d’automatisation du déploiement des applications et n’avons donc pas besoin de SecureApp

Cet outil prend-il en charge l’aspect sécurité ? Tufin dispose d’un avantage indispensable en matière de sécurité réseau, celui de comprendre et gérer les besoins des applications en matière de connectivité réseau.

Nous ne souhaitons pas apporter de modifications à nos processus de travail et flux d’opérations actuels.

Les flux d’opérations personnalisables de Tufin peuvent être configurés de manière à refléter vos processus de travail existants. L’avantage est que Tufin veille à la mise en application réelle de chaque demande de modification et fournit des détails pour l’audit.

En quoi cela améliorera-t-il la sécurité de mon entreprise?

La suite Orchestration de Tufin réduit au minimum l’exposition du réseau aux risques inutiles. Les réseaux actuels sont segmentés et extrêmement complexes, avec des technologies provenant de multiples fournisseurs et des centaines de règles. Tufin assure la surveillance et l’alerte en cas de modifications sur les pare-feu et les dispositifs du réseau, et analyse en continu les risques concernant les violations des stratégies, avant et après modification.

Bref argumentaire

Pour les entreprises dont les activités nécessitent de vastes et complexes réseaux en changement constant, il est devenu essentiel de concilier des déploiements rapides avec des modifications sécurisées du réseau. La suite Orchestration de Tufin, solution leader sur le marché, permet d'implémenter les modifications du réseau en une journée au lieu d'une semaine, avec une précision et une sécurité optimisées grâce à l'automatisation et aux analyses.

- **SecureTrack™** Gestion unifiée des pare-feu
- **SecureChange®** Automatisation des modifications du réseau
- **SecureApp™** Gestion de la connectivité des applications

La suite Orchestration de Tufin est une solution complète d'automatisation de la conception, de la mise en œuvre et de l'audit des modifications de la sécurité réseau, de la couche applications à la couche réseau. Elle permet de réduire au minimum les erreurs, assurant ainsi une fourniture de service rapide et une amélioration de la sécurité, de la conformité et de la disponibilité des applications de l'entreprise.



- Quel est votre processus d'audit des pare-feu ? Quelles sont les ressources mobilisées pour la collecte d'informations ? Ou'est-ce qui motive les modifications de votre réseau ?
- Combien de pare-feu possédez-vous ?
- A quoi ressemble votre environnement de pare-feu ? Quelles sont les difficultés auxquelles vous vous heurtez lors de l'implémentation d'une demande de modification du réseau ?
- What does your firewall change process and approval cycle look like ?

Avantages

- **Accélération de la fourniture de services et amélioration de l'agilité du réseau:** Réduction d'une semaine à un jour du temps consacré aux modifications de sécurité et aux audits, grâce à l'automatisation et aux analyses
- **Prévisibilité** de l'impact des risques et de la violation potentielle des stratégies lors d'une modification du réseau, afin de minimiser l'exposition du réseau et d'en renforcer la sécurité et la conformité
- **Amélioration de la précision** des modifications réseau, pour des performances et une sécurité accrues
- **Garantie de la continuité des activités** grâce à la réduction des temps d'arrêt des applications et du réseau, ainsi que du temps moyen de reprise
- **Gouvernance informatique et conformité permanente** aux normes de sécurité de l'entreprise et du secteur
- **Visibilité et contrôle centralisés** odes stratégies de sécurité réseau et des configurations des équipements, pour une gestion uniforme des modifications réseau

Questions de qualification

- Quel est votre processus d'audit des pare-feu ? Quelles sont les ressources mobilisées pour la collecte d'informations ? Ou'est-ce qui motive les modifications de votre réseau ?
- Combien de pare-feu possédez-vous ?
- A quoi ressemble votre environnement de pare-feu ? Quelles sont les difficultés auxquelles vous vous heurtez lors de l'implémentation d'une demande de modification du réseau ?
- What does your firewall change process and approval cycle look like ?

En quoi Tufin est-il unique ?

- **Solution la plus complète en matière de gestion des modifications pour la sécurité du réseau** Unification du suivi et des alertes en cas de modification
- **Gestion** de la connectivité des applications
- **Automatisation** des modifications
- **Automatisation complète des modifications de bout-en-bout** Apf ouvertes garantissant l'interopérabilité avec les systèmes existants tout au long du processus
- **Prise en charge de l'immense** majorité des dispositifs pour une mise en œuvre automatique
- **Recommandations** de stratégies en fonction d'une topologie et d'une analyse des bases de règles précises
- **Vérification** automatique et piste d'audit
- **Contrôle et visibilité unifiés des stratégies de sécurité du réseau** Surveillance et gestion intégrées des modifications (documentation automatique des règles)
- **Mellieure visibilité** de l'impact des modifications tout au long du processus
- **Surveillance** et analyse en temps réel des modifications

Capacités fondamentales

- **Conception, vérification** et mise en œuvre automatisées des modifications de la connectivité réseau afin de minimiser les risques
- **Contrôle** centralisé des stratégies de sécurité et des processus de gestion des modifications sur l'ensemble des dispositifs du réseau
- **Analyse** proactive des risques et de la conformité, et simulation de l'impact pour chaque modification de la sécurité réseau, avant et après son implémentation
- **Coordination** et mise en corrélation du suivi et des rapports sur les modifications de la configuration du réseau
- **Modèle** de connectivité des applications qui mappe et automatise l'interface entre chaque application et le réseau
- **Analyse** de la topologie réseau qui simule la connectivité sur l'ensemble du réseau

Solution Index

Votre problème	La solution de Tufin	Votre problème	La solution de Tufin
Accélération du déploiement des applications	Tufin facilite le déploiement des applications et la gestion des modifications les concernant, telles que la migration d'un serveur. Tufin propose aux équipes responsables des applications une méthode simple pour définir leurs besoins, ainsi que des flux d'opérations automatisés pour la conception, l'implémentation et le contrôle des modifications réseau requises. Caractéristiques principales: <ul style="list-style-type: none">• Portail en libre-service SecureApp• Flux d'opérations automatisés et personnalisables• Gestionnaire des modifications (en fonction de la topologie)• Mise en œuvre des modifications	Implémentation et mise en application de la stratégie de sécurité, en tout lieu et à tout instant	Orchestration Suite offre une boucle fermée pour la mise en application d'une stratégie de sécurité hermétique – de la définition des besoins aux modifications des activités, en passant par le processus automatisé de modification, d'audit et de surveillance constante avec alertes. Caractéristiques principales: <ul style="list-style-type: none">• Analyse automatique des risques et de la conformité• Conception et mise en œuvre des modifications• Suivi en temps réel des modifications• Documentation et recertification des règles• Rapports d'audit
Conformité avec PCI DSS, SOX et autres normes et réglementations	Tufin analyse proactivement la conformité de toutes les modifications des stratégies de sécurité en fonction de vos normes organisationnelles et réglementaires AVANT la mise en œuvre de ces modifications. En outre, Tufin surveille continuellement toutes les modifications en temps réel et vous alerte en cas d'élément suspect. Caractéristiques principales: <ul style="list-style-type: none">• Tableau de bord de conformité / PCI DSS• Analyse automatique de la conformité dans SecureChange• Personnalisation de la stratégie de sécurité de l'entreprise• Rapports d'audit instantanés	Évaluation anticipée de l'impact d'une modification	vant l'implémentation des modifications, Tufin Orchestration Suite en vérifie l'impact et effectue une analyse proactive des risques et de la conformité. Vous évitez ainsi les erreurs, les interruptions de service ou les corrections a postériori. Caractéristiques principales: <ul style="list-style-type: none">• Gestionnaire des modifications avec identification des cibles• Intelligence de la topologie• Analyse des risques et de la conformité• Suivi en temps réel des modifications et envoi d'alertes
Respect des accords de niveau de service pour les modifications du réseau et accélération de l'implémentation de celles-ci	Grâce à Tufin, vous pouvez apporter des modifications à la sécurité en un jour, au lieu d'une semaine. Orchestration Suite procure une technologie d'automatisation et des outils puissants et intelligents tout au long du processus de modification, de la demande à la vérification des modifications, en passant par leur conception et leur implémentation. Caractéristiques principales: <ul style="list-style-type: none">• Portail en libre-service• Gestionnaire des modifications• Mise en œuvre automatique• Vérification automatique	Audits réussis bien plus rapidement et aisément	Orchestration Suite réduit jusqu'à 80 % les temps de préparation aux audits. Elle permet de respecter constamment des normes telles que PCI DSS et SOX grâce à une analyse proactive de la conformité effectuée avant modification, et à des vérifications automatiques de la conformité lors des révisions des stratégies. Caractéristiques principales: <ul style="list-style-type: none">• Tableau de bord de conformité / PCI DSS• Stratégies d'entreprise personnalisables• Rapports d'audit pour PCI DSS, entre autres• Piste d'audit intégrale avec comptes-rendus complets
Réduction des temps d'arrêt du réseau et des applications, garantie de la continuité des activités	Avant l'implémentation des modifications, Tufin Orchestration Suite en vérifie l'impact et effectue une analyse proactive des risques et de la conformité. Toutes les modifications sont automatiquement suivies et vous êtes alerté en cas de problèmes pouvant affecter la disponibilité du réseau ou des applications. Caractéristiques principales: <ul style="list-style-type: none">• Gestionnaire des modifications avec identification des cibles• Intelligence de la topologie• Analyse des risques et de la conformité• Suivi en temps réel des modifications et envoi d'alertes	Réduction des frais opérationnels par l'automatisation des tâches manuelles répétitives	Orchestration Suite automatise les tâches manuelles de routine susceptibles d'entraîner des erreurs, contraindre à recommencer l'opération ou engendrer une baisse de la productivité. Elle permet également d'automatiser intégralement la conception, l'implémentation et la vérification des modifications des stratégies. Caractéristiques principales: <ul style="list-style-type: none">• Concepteur de stratégies• Mise en œuvre des modifications• Rapports d'audit• Documentation et recertification des règles
Amélioration de la communication entre les équipes chargées respectivement du réseau, des applications et de l'exploitation	Orchestration Suite facilite la communication entre les équipes chargées des applications, de la sécurité et de l'exploitation. Elle permet de combler l'écart entre les besoins en connectivité des applications et la configuration des stratégies sur chaque dispositif réseau, ce qui simplifie le processus de justification et de recertification des règles des stratégies. Caractéristiques principales: <ul style="list-style-type: none">• Portail de demande d'accès en libre-service• Référentiel d'applications• Documentation et recertification des règles• Rapports	Élimination des failles de sécurité engendrées par des règles de stratégies non utilisées ou trop permissives	Grâce à Tufin SecureTrack, vous pouvez détecter rapidement et aisément les points faibles de vos stratégies de pare-feu dues à des règles non utilisées, imbriquées (masquées) ou trop permissives. Il est possible de nettoyer les stratégies et les listes de contrôle d'accès afin de faciliter leur gestion et leur respect. Caractéristiques principales: <ul style="list-style-type: none">• Suivi des modifications en temps réel• Nettoyage/optimisation des stratégies• Nettoyage des règles permissives• Automatisation des modifications

Réunion

1

- Planifiez la réunion de qualification
- Qualifiez les prospects (points faibles, budget, niveau d'urgence) en cas de projet actif
- Si le projet n'est pas actif (par exemple, si la réunion résulte d'un « appel à froid ») ne vous concentrez PAS sur la qualification. Vendez la valeur de la solution et trouvez un point d'accroche – parlez des réussites des autres clients et des bénéfices qu'ils ont tiré de Tufin
- Créez une démonstration et validez les points faibles, le niveau d'urgence et le budget. Quels sont les éléments nécessaires pour progresser ?
- Enregistrez le prospect sur le portail dédié Deal Registration Portal et planifiez une démonstration de faisabilité (POC)

Évaluation

2

- Installez la machine VMware et l'équipement fournis
- Dirigez le client ou le partenaire vers le chapitre Installation du Guide utilisateur et vers la liste des fonctionnalités dans le test d'acceptation
- Assurez-vous de l'existence de critères de tests définis par un accord mutuel
- En cas de problème, contactez support@tufin.com
- Essayez de limiter l'évaluation à un mois

Conclusion de l'accord

3

- Pour les grands comptes, effectuez le calcul du ROI en fonction de l'infrastructure du client afin d'établir une analyse de rentabilité – niveau managérial uniquement
- Débutez l'entretien commercial
- Contactez un représentant de Tufin pour calculer le ROI
- Livre blanc de Forrester : "Total Economic Impact" (Impact économique global)
- Vidéos du produit