

ELEMENTAL SECURITY PLATFORM

COMPLIANCE AUTOMATION

**AUTOMATISATION DE LA MISE EN CONFORMITE
D'UN PARC INFORMATIQUE**

SOMMAIRE

1	PREAMBULE	3
2	LA SOLUTION ELEMENTAL SECURITY PLATFORM	4
3	ARCHITECTURE DU PRODUIT ESP	5
	3.1 SERVEUR ET AGENTS ESP	6
	3.2 GENERATION DE RAPPORTS	8
4	SPECIFICATIONS TECHNIQUES ESP	9
5	EN RESUME	10

1 PREAMBULE

Les Responsables Informatiques d'aujourd'hui doivent faire face, **d'un côté** aux exigences d'un système informatique (SI) qui devient de plus en plus complexe, éclaté géographiquement, en changement permanent et **de l'autre côté** aux exigences d'une hiérarchie qui veut s'assurer que ce même SI répond à des règles strictes de sécurité et d'utilisation en conformité avec différentes réglementations imposées par le domaine d'activité de l'entreprise.

Pour s'assurer de la conformité et de la sécurité des serveurs et des stations de travail de l'entreprise, le département informatique, doit aujourd'hui pouvoir disposer d'une bonne visibilité des ressources informatiques exploitées pour faire un inventaire quotidien afin de déceler les non-conformités et d'appliquer en temps réel des actions pour corriger les écarts.

Actuellement, il n'est pas facile de pouvoir automatiser à l'aide d'un seul outil un travail, de mesure et de 'reporting' des écarts de conformité qui est fastidieux et souvent réalisé de façon manuelle ou à l'aide de solutions inadaptées.

Les politiques de sécurité ne sont pas évidentes à créer, car elles exigent une parfaite connaissance des systèmes et technologies sous-jacentes, de l'organisation de l'entreprise, et de ce fait, elles sont rarement implémentées. Enfin, elles doivent être transparentes et sans contraintes au regard du développement économique de l'entreprise.

Il est important d'avoir une bonne visibilité pour surveiller et comprendre de manière continue ce qu'il se passe sur le réseau pour en déduire une tendance, car rien ne reste figé. Même si l'état du réseau était connu lundi, vendredi il aura changé. Le renouvellement des équipements fait qu'une entreprise possédant 10 000 ordinateurs se voit changer en moyenne 400 systèmes par mois. Ce nombre peut être encore plus élevé en considérant des éventuelles fusions et des acquisitions d'entreprises, une croissance rapide de l'activité, la mobilité du personnel, les changements d'architecture de réseau, de nouveaux services, etc ..

Elemental Security Platform (ESP) est un progiciel d'entreprise qui permet aux directions informatiques d'assurer un contrôle permanent de la conformité du SI (serveurs et stations de travail) par rapport à des standards reconnus.

2 La Solution Elemental Security Platform

Elemental® est un pionnier dans la gestion de conformité de sécurité. L'entreprise a été fondée vers la fin de 2002 pour fournir un outil capable d'établir le lien entre les politiques de sécurité documentées et le véritable état des différents ordinateurs sur le réseau.

C'est un des rares produits dans l'industrie qui unifie la gestion de politique de sécurité sur un parc hétérogène de serveurs et de postes de travail. ESP met en œuvre des politiques de sécurité à des niveaux multiples afin de mesurer et de contrôler le risque tout en permettant la re-médiation automatisée de la configuration des équipements et de leur accès au réseau.

En utilisant ESP (reconnu par les professionnels et fortement récompensé), les organisations peuvent aligner au niveau de leur informatique une sécurité adaptée pour les utilisateurs et les systèmes avec des objectifs exigeants de développement économique. Les entreprises peuvent utiliser un produit unique pour collecter, de manière compréhensible et mesurable, les données correspondantes à leur politique de sécurité et prouver ainsi leur conformité.

Le système ESP est composé d'une application serveur Web, d'une base de donnée et de multiples agents (jusqu'à 10000 par serveur) à déployer sur les machines à protéger dans le but d'automatiser la conformité de l'ensemble. Les agents sont disponibles pour les environnements Windows, Linux RedHat, Solaris, Mac, AIX, HP-UX.

Plusieurs modèles de politiques sont prédéfinis dans le système, mais des politiques sur mesure peuvent être développées à partir de ces modèles contenant déjà plus de 2500 règles. Les modèles de politique (Policy Templates) disponibles sont :

➤ Best practices – standards industriel / branche d'activité:

- CIS AIX,
- CIS HP/UX,
- CIS Mac OS x,
- CIS Solaris 10,
- CIS Solaris,
- CIS Win 2k,
- CIS Win 2kpro,
- CIS Win 2ks,
- CIS Win 2003,
- CIS Win 2003 dc,
- CIS Win XP,
- CIS RHEL,
- ESP NSA Solaris

➤ Regulatory policies – réglementations :

- FISMA,
- HIPAA,
- PCI,
- SOX,

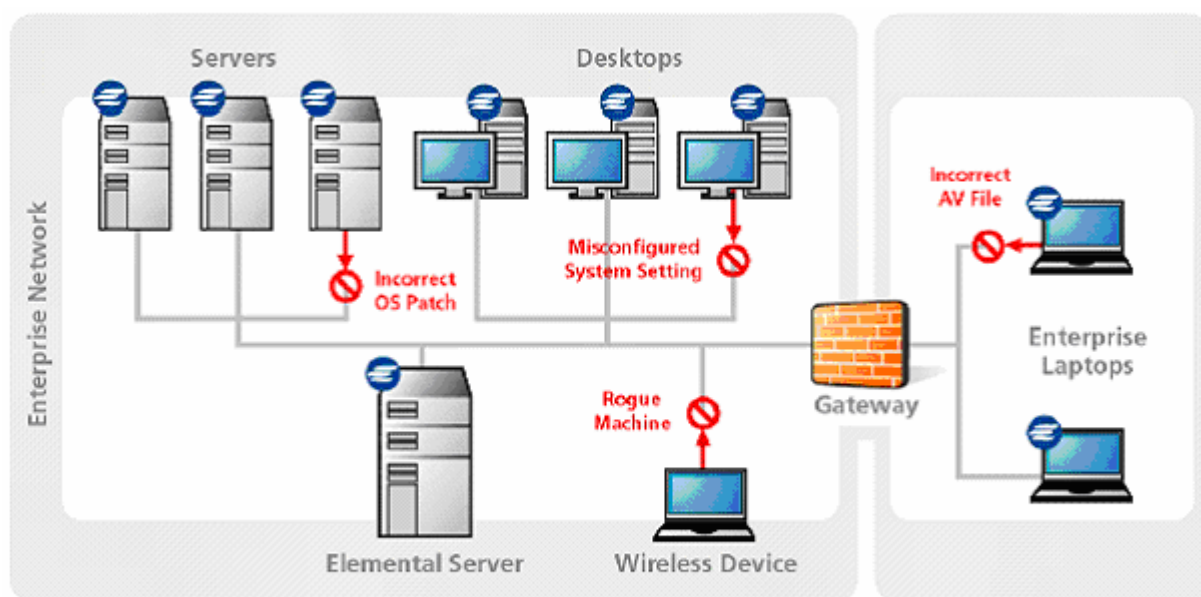
3 Architecture du produit ESP


Sur le papier, la politique de sécurité semble être maîtrisée. Dans la réalité, il y a un grand écart entre la documentation et le statut réel des ressources informatiques.

Cet écart est dû en parti au fait que l'infrastructure de communication, les systèmes d'exploitation et les applications de l'entreprise évoluent continuellement afin de maintenir une compétitivité économique et qu'il est difficile pour l'entreprise d'adapter, d'appliquer et de contrôler la politique de sécurité dans un environnement dynamique.

ESP propose un système basé sur une architecture *agent - serveur* permettant de gérer de manière centralisée et unifiée la politique de sécurité et de contrôler le cas échéant l'accès au réseau. Cet outil donnera une réelle métrique de ce qui *est* ou *n'est pas* conforme aux règles de sécurité prédéfinies et ceci à différents niveaux (OS, matériel, logiciel, réseau).

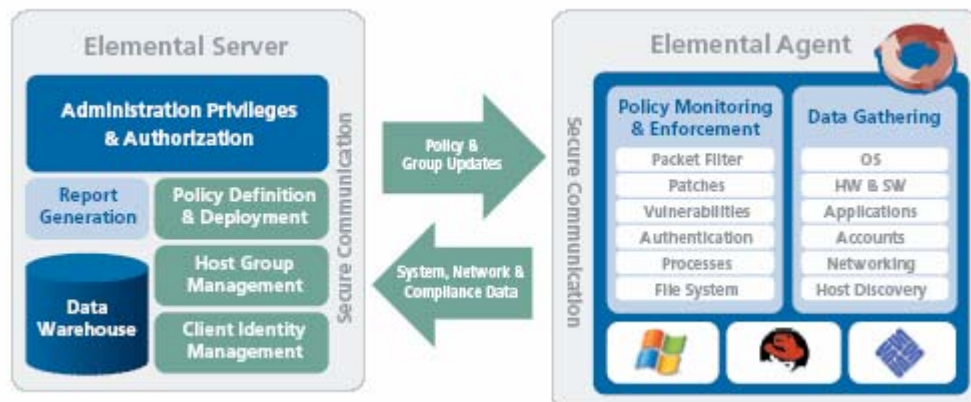
Voici un exemple de déploiement :



 Protected with an Elemental Agent

3.1 Serveur et Agents ESP

Le schéma suivant décrit le rôle respectif de l'agent et du serveur.



L'agent ESP fonctionne de manière transparente, sécurisée et optimisée sur des postes de travail ou des serveurs (Windows, Solaris, Red Hat Linux, IBM, Mac, HP). Il recueille des informations détaillées sur la configuration de l'ordinateur observé et surveille les interfaces réseaux pour profiler leur activité. Il écoute passivement le trafic réseau et a la capacité de découvrir des ordinateurs inconnus (sans agent) en fournissant des informations relatives à leur activité réseau.

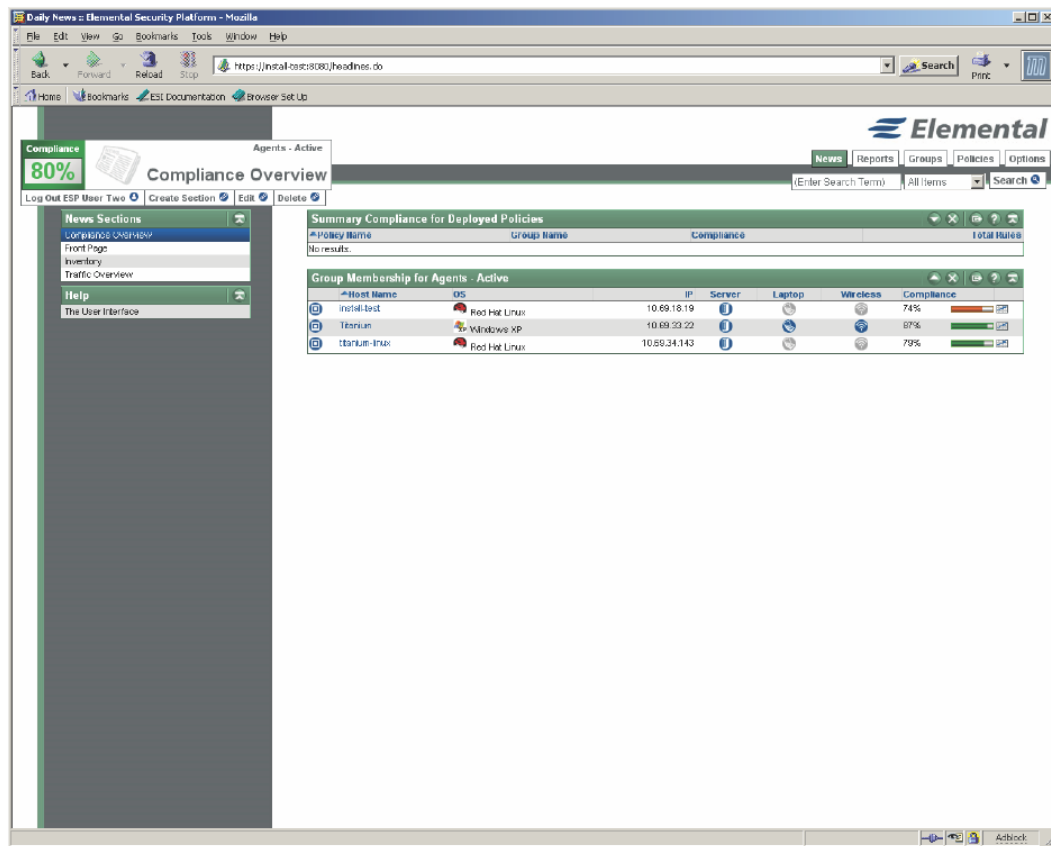
Les ordinateurs sont dynamiquement regroupés en fonctions des attributs mis en jeux. Ces regroupements sont employés pour automatiser la distribution des politiques de sécurité. L'agent supporte à la fois les configurations et la couche réseau des ordinateurs.

L'agent ESP propose également un filtrage de paquets qui permet de limiter les communications entre les ordinateurs, d'interdire à une application de communiquer sur certains ports, ou bien d'isoler les ordinateurs non autorisés.

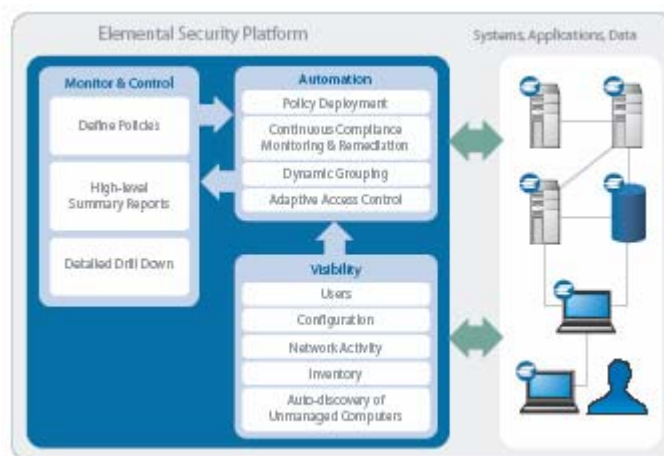
ESP met en œuvre un ensemble riche de plus de 150 attributs qui décrivent en détail la configuration de l'ordinateur et de son activité réseau. Ces attributs portent sur le logiciel d'exploitation, les groupes de matériel et de logiciel, l'activité de réseau, l'utilisation d'application, l'activité sans fil, la présence de l'agent et la conformité aux politiques assignées.

ESP Server Manager est basé sur une architecture trois tiers : Client (Agent ou console d'administration), Serveur Web et Base de Données. Le système est développé autour des technologies J2EE. Son interface homme-machine est accessible à distance. ESP Server Manager gère les politiques de sécurité et les groupes d'agents, vérifie la conformité de ces politiques, fourni des rapports (en option PCI, Sarbanes et Oxley, HIPAA, ..ou personnalisés) représentant les écarts et/ou changements, et facilite la mise en œuvre des actions correctives. De plus, il est possible de simuler une politique de sécurité et d'en mesurer l'impact. Enfin, ESP Server Manager gère les privilèges des différents utilisateurs du système.

Voici un exemple visualisant le pourcentage de conformité de la politique de sécurité :



Enfin, la communication entre l'agent et ESP Server Manager est sécurisée (SSL) et optimisée (répartition de charge, trafic incrémental). Le contact est maintenu par un protocole de type 'heartbeat'. Les interruptions de communications, ne perturbent pas les données collectées ou les données à transférer.

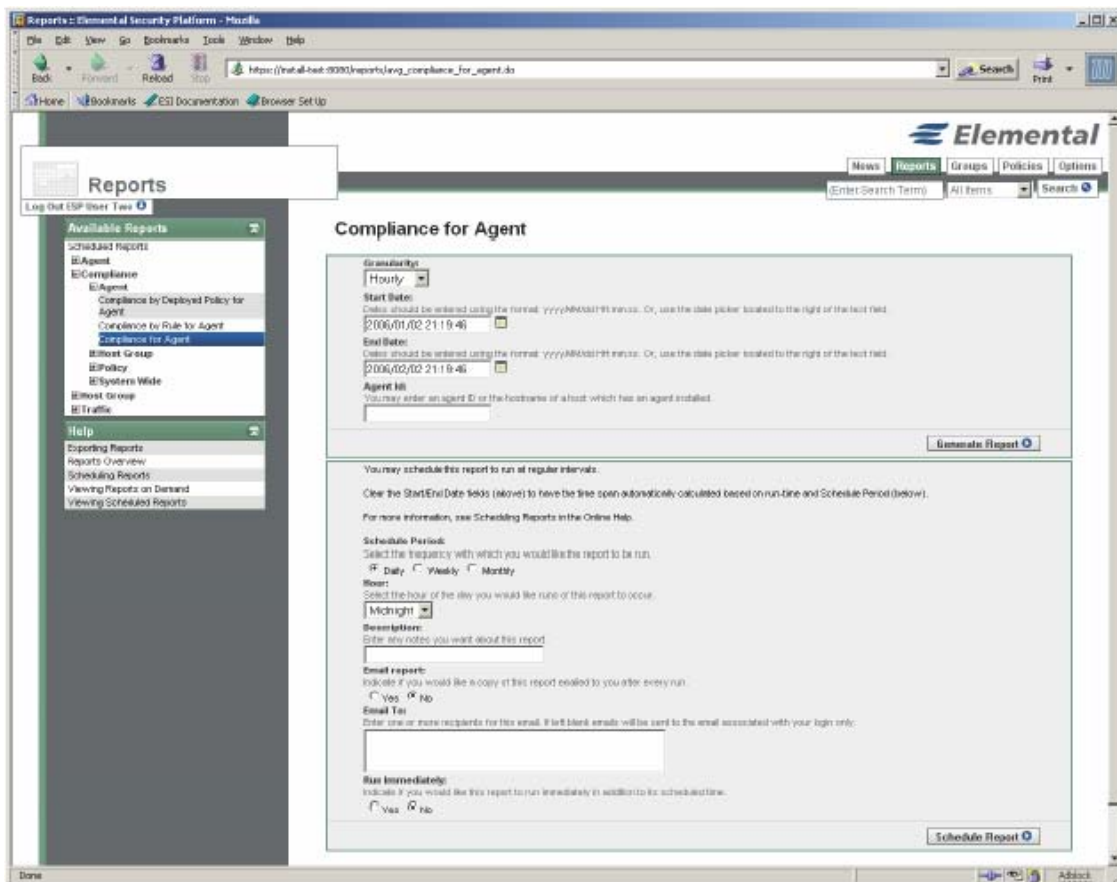


3.2 Génération de Rapports

ESP fournit un ensemble hiérarchique de vues permettant de faire l'état de vos ressources et du réseau. Les rapports montrent à quel point les dispositifs sur le réseau sont conformes aux politiques déployées. Des rapports peuvent être produits en temps réel et peuvent être le résultat de filtres et/ou combinaisons de plusieurs requêtes, et être exportés (csv, xml, email, ..).

En plus des rapports traditionnels tels que les événements (alarmes envoyées par le système), le trafic (octets, protocole), l'observations sur le réseau (nouveaux serveurs sur le réseau, serveurs de confiance), la conformité (avec métrique associée), il est possible de définir des rapports personnalisés : exemple de groupe ou sous groupe de hosts (serveurs Solaris pour application financière en relation avec SoX et en fonction de leur localisation géographique).

Ce qui est important c'est d'afficher ce qui a provoqué le changement (manque de conformité). L'accent a été mis sur l'organisation de l'information pour faciliter la logique d'un raisonnement, comme le montre l'écran suivant :



4 Spécifications Techniques ESP

Les caractéristiques des plates-formes supportant la solution ESP sont :

Serveur ESP

Red Hat Enterprise Linux 9 EL2.1, EL3 ou EL4, sur un serveur possédant les caractéristiques minimum suivantes :

Ressource	1-500 agents	500-5 000 agents	> 5 000 agents
CPU	1-2 CPUs	2-4 CPUs	4-6 CPUs
	Pentium 4, 3Ghz	Pentium 4, 3Ghz	Pentium 4, 3Ghz
RAM	1G	2G	4G

Ou Sun Microsystems Solaris 10, sur un serveur possédant les caractéristiques minimum suivantes :

Ressource	1-500 agents	500-5 000 agents	> 5 000 agents
CPU	1 CPU	2 CPUs	4 CPUs
	550 Mhz SPARCv9	550 Mhz SPARCv9	550 Mhz SPARCv9
RAM	1G	2G	4G

Notes :

- NIC Card FastEthernet minimum
- Java 2 JDK, vers. 1.5.0_07 (ou supérieure)

Console d'exploitation et d'administration

La console comporte une interface web : Internet Explorer 6.0, Mozilla v1.4, Firefox v1.0

Système Décisionnel

La Base de Données (Oracle 9i or 10g Enterprise Edition) peut cohabiter avec ESP Server Manager sur la même machine ou bien être hébergée sur un autre serveur ayant les caractéristiques suivantes :

Ressource	1-500 agents	500-5 000 agents	> 5 000 agents
CPU	1-2 CPUs	2-4 CPUs	4-6 CPUs
	Pentium 4, 3Ghz	Pentium 4, 3Ghz	Pentium 4, 3Ghz
RAM	1G	2-4G	4-6G

Note :

- 200GB d'espace de stockage pour 1000 agents, prendre 50GB supplémentaire par tranche de 1000 agents additionnels.

Agents ESP

Windows 2000 Pro,
Windows 2000 Server,
Windows 2003, Server,
Windows XP Professional SP1 and SP2
Sun Solaris 8 and 9 (SPARC)
Red Hat Enterprise Linux 2.1/3/4
IBM AIX 5.2/5.3
Mac OS X 10.3/10.4
HP-UX 11i (itanium)

Capacité (ESP V3.1)

ESP Server Manager peut gérer jusqu'à 10000 agents

5 En résumé

Elemental Security Platform permet :

- de découvrir et mettre en quarantaine les systèmes non conformes ou non autorisés
- de mesurer les écarts par rapport à une politique de sécurité
- de bloquer l'accès au réseau en cas de non conformité
- de contrôler les communications entre les systèmes, utilisateurs et départements
- de fournir une parfaite visibilité de tous les systèmes et de l'état de leur interconnexion

ESP donnera à votre organisation une réelle visibilité sur les configurations et comportements des postes de travail et serveurs tout en décelant les non conformités par rapport à la politique de sécurité de votre entreprise.