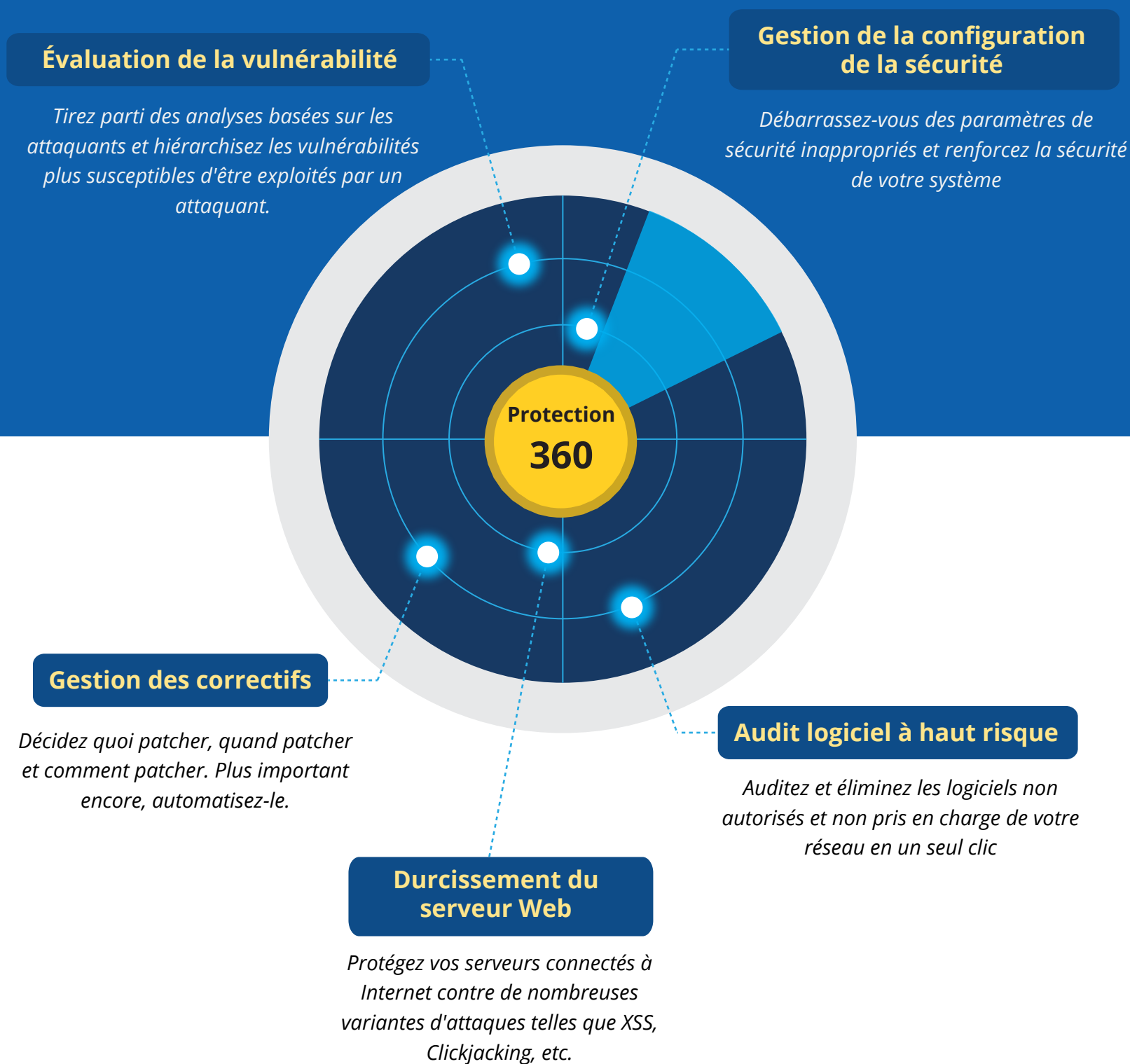


Réduisez votre surface d'attaque grâce à une gestion proactive des vulnérabilités



Le défi d'aujourd'hui

Gartner prédit que «99% des vulnérabilités exploitées d'ici la fin de 2020 continueront d'être celles connues des professionnels de la sécurité et de l'informatique au moment de l'incident.» Le manque de sensibilisation et l'absence d'un moyen centralisé de faciliter la cyberhygiène ont fait de nombreuses organisations vulnérables aux cyberattaques. De plus, **22316 nouvelles failles de sécurité** ont été révélées en 2019, et plus d'un tiers d'entre elles disposaient d'un exploit. Face à la montée en flèche de ces chiffres, les organisations doivent mettre en œuvre une approche stratégique pour hiérarchiser et gérer les vulnérabilités, car toutes les vulnérabilités ne présentent pas le même risque.

La solution

Vulnerability Manager Plus de ManageEngine est un logiciel de gestion des vulnérabilités axé sur la priorisation pour les entreprises, offrant une gestion intégrée des correctifs. Il s'agit d'une solution stratégique pour vos équipes de sécurité, offrant une visibilité, une évaluation et une correction complètes des menaces et des vulnérabilités sur tous vos actifs informatiques (serveurs, ordinateurs de bureau, ordinateurs portables, machines virtuelles, serveurs DMZ et périphériques itinérants) à partir d'une seule console.



Comment Vulnerability Manager Plus renforce la position de sécurité de votre réseau

Évaluation de la vulnérabilité

- ◆ Identifiez les vulnérabilités ainsi que leur contexte, comme le CVSS et les scores de gravité, pour déterminer la priorité, l'urgence et l'impact.
- ◆ Restez au courant si le code d'exploitation a été divulgué publiquement pour une vulnérabilité.
- ◆ Gardez un œil sur la durée de résidence d'une vulnérabilité sur votre réseau. Filtrez les vulnérabilités en fonction du type d'impact et de la disponibilité des correctifs.
- ◆ Obtenez des recommandations sur les vulnérabilités de haut niveau obtenues en fonction des facteurs de risque ci-dessus.
- ◆ Tirez parti d'un onglet dédié aux vulnérabilités révélées publiquement et zero-day, et utilisez des solutions de contournement pour les atténuer avant l'arrivée des correctifs.
- ◆ Isolez et identifiez les vulnérabilités des actifs critiques, à savoir les bases de données et les serveurs Web qui contiennent des données critiques et effectuent des opérations commerciales cruciales.

Gestion de la configuration de sécurité

- ◆ identifiez les erreurs de configuration dans les systèmes d'exploitation, les applications et les navigateurs, et remettez-les en conformité.
- ◆ Auditez votre pare-feu, votre antivirus et l'état de BitLocker.
- ◆ Empêchez les tentatives de force brute en appliquant des politiques de mot de passe complexes, de verrouillage de compte et de connexion sécurisée.
- ◆ Assurez-vous que les paramètres de protection de la mémoire, tels que la protection contre l'écrasement de la gestion des exceptions structurées, la prévention de l'exécution des données et la randomisation de la disposition de l'espace d'adressage, sont activés.
- ◆ Mettez fin aux protocoles hérités avec des risques qui l'emportent sur les avantages.
- ◆ Gérez les autorisations de partage, modifiez les contrôles des comptes utilisateurs et désactivez les protocoles hérités pour réduire votre surface d'attaque.
- ◆ Modifiez en toute sécurité les configurations de sécurité sans interrompre les opérations commerciales en examinant les avertissements de déploiement critiques

Configuration matérielle requise pour l'agent

Processeurs	Vitesse du processeur	Taille de la RAM	Espace disque dur
Intel Pentium	1.0 GHz	512 Mo	100 Mo

Configuration matérielle du serveur

Nombre d'appareils gérés	Serveurs utilisés	Processeur	RAM	Espace disque dur
1 à 250	Serveur Vulnerability Manager Plus	Intel Core i3 (2 core/4 thread) 2.0GHz 3 Mo cache	2Go	5Go
251 à 500	Serveur Vulnerability Manager Plus	Intel Core i3 (2 core/4 thread) 2.4GHz 3 Mo cache	4Go	10Go
501 à 1,000	Serveur Vulnerability Manager Plus	Intel Core i3 (2 core/4 thread) 2.9GHz 3 Mo cache	4Go	20Go
1,001 à 3,000	Serveur Vulnerability Manager Plus	Intel Core i5 (4 core/4 thread) 2.3GHz 6 Mo cache	8Go	30Go
3,001 à 5,000	Serveur Vulnerability Manager Plus	Intel Core i7 (6 core/12 thread) 3.2GHz 12 Mo cache	8Go	40Go
	Serveur SQL	Intel Core i7 (6 core/12 thread) 3.2GHz 12 Mo cache	8Go	30Go
5,001 à 10,000	Serveur Vulnerability Manager Plus	Intel Xeon E5 (8 core/16 thread) 2.6GHz 20 Mo cache	16Go	60Go
	Serveur SQL	Intel Xeon E5 (8 core/16 thread) 2.6GHz 20 Mo cache	16 Go	40Go
10,001 à 20,000	Serveur Vulnerability Manager Plus	Intel Xeon E5 (8 core/16 thread) 2.6GHz 40 Mo cache	32Go	120Go
	Serveur SQL	Intel Xeon E5 (12 core/24 thread) 2.7GHz 30 Mo cache	32Go	80Go

Si vous gérez plus de 1000 ordinateurs, nous vous recommandons d'installer Vulnerability Manager Plus sur une machine Windows Server

Logiciels requis

OS pris en charge pour le serveur
Windows 7 / 8 / 8.1 / 10 / Servers 2003 / 2003 R2 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016

OS pris en charge pour les agents

Windows OS	Windows Server OS	Mac OS	Linux OS
Windows 10	Windows Server 2016	10.15	Ubuntu 10.04 et versions ultérieures
Windows 8.1	Windows Server 2012 R2	10.14	Debian 7 et versions ultérieures
Windows 8	Windows Server 2012	10.13	CentOS 6 & 7
Windows 7	Windows Server 2008 R2	10.12	Red Hat 6 & 7
Windows Vista	Windows Server 2008	10.11	SUSE Enterprise Linux 11 et versions ultérieures
Windows XP	Windows Server 2003 R2	10.10	
	Windows Server 2003	10.9	
		10.8	

Tarification

Édition gratuite

Gestion complète des vulnérabilités pour **20 postes de travail** et **5 serveurs**

Édition Professionnelle

À partir de **695\$/an** pour **100 ordinateurs**

Édition Entreprise

À partir de **1195\$/an** pour **100 ordinateurs**

Pour plus de détails

www.vulnerabilitymanagerplus.com

vulnerabilitymanagerplus-support@manageengine.com

Sans frais: **+1-888-720-9500**