Explorer votre parcours de sécurité : Un guide pour les PME

Découvrez comment l'utilisation de la plateforme Intel vPro® avec le logiciel ESET Endpoint Security peut aider votre organisation à se protéger des menaces de cybersécurité.

intel®

ESET® Digital Security
Progress. Protected.

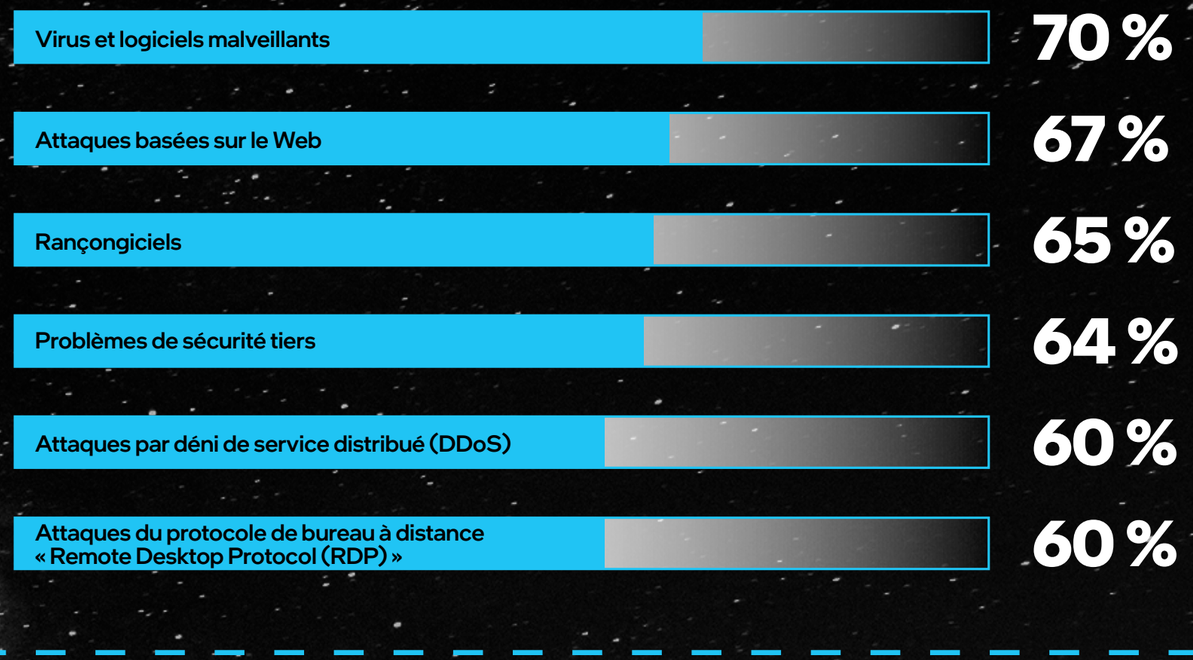
Contenu :

Les acteurs malveillants cherchent des moyens d'attaquer

Si les progrès technologiques ont permis aux PME de se développer, ils ont également favorisé l'émergence de menaces plus avancées sur la sécurité. En 2022, une enquête a démontré que 70 % des propriétaires de petites et moyennes entreprises (PME) en Amérique du Nord et en Europe ont rapporté que leur préoccupation principale en matière de sécurité au cours des 12 mois suivants concernait les virus et les logiciels malveillants. Ceux-ci étaient suivis de près par les attaques basées sur le Web, les rançongiciels et les problèmes de sécurité tiers.[1]

Étant donné leur taille et les ressources dont elles disposent, il n'est pas surprenant que 74 % de ces entreprises estiment être plus vulnérables aux cyberattaques que les entreprises de plus grande taille.[1] Une raison expliquant cette vulnérabilité tient au fait que ces organisations ont moins de protections en place pour empêcher les attaques, ce qui en fait des cibles attrayantes pour les acteurs malveillants.

Principales préoccupations des dirigeants de PME en matière de cybersécurité pour les 12 mois suivants[1]



Des difficultés nombreuses tout au long du parcours

Si vous êtes confronté à des menaces de rançongiciels en constante évolution, combinées à des limitations budgétaires et à des politiques commerciales changeantes, vous n'êtes pas seul. Quelles difficultés en matière de cybersécurité vous tiennent éveillé la nuit, de même que les autres dirigeants de PME? D'après les PME sondées, les principales difficultés incluent le manque de sensibilisation à la cybersécurité des employés (43 %), les vulnérabilités de l'écosystème partenaire (34 %) et la poursuite du travail hybride ou à distance (32 %).[1] En outre, 70 % des PME reconnaissent que leurs investissements dans la cybersécurité n'arrivent pas à suivre le rythme des menaces, en particulier lorsque les modèles opérationnels évoluent, par exemple avec le passage au travail hybride.[2]

43 %

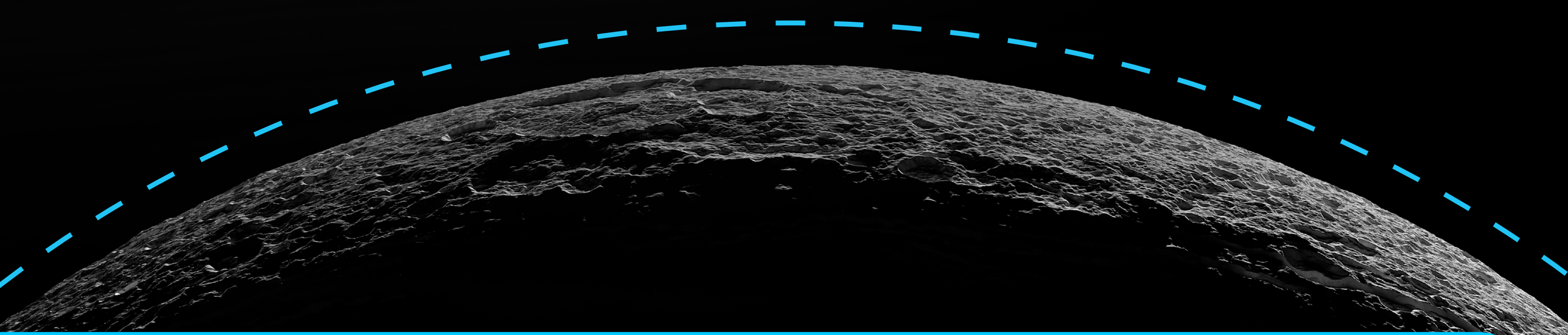
Manque de **sensibilisation à la cybersécurité** de la part des employés[1]

34 %

Vulnérabilités dans l'**écosystème partenaire/fournisseur**[1]

32 %

Poursuite du travail **hybride ou à distance**[1]



La sécurité commence par Intel

Les dirigeants de PME semblent prêts à intensifier leur action et à protéger leur organisation. Parmi les sondés, 65 % utilisent actuellement ou prévoient d'utiliser des solutions de cybersécurité avancées, y compris EDR, XDR ou MDR, semblables à celles proposées par la gamme complète de solutions de sécurité d'ESET.[1]

Les PME peuvent encore améliorer leur cybersécurité en tirant profit des fonctionnalités de sécurité assistées par matériel de la plateforme Intel vPro et d'ESET Endpoint Security.

La plateforme Intel vPro inclut Intel® Threat Detection Technology (Intel® TDT), une suite de technologies qui ajoute la détection assistée par matériel des rançongiciels et autres menaces avancées.

ESET a intégré Intel TDT à sa plateforme et a ainsi obtenu accès à une myriade de données uniques de télémétrie matérielle. Ces données améliorent la capacité d'ESET Endpoint Security à détecter la présence de menaces avancées comme les rançongiciels cachés dans des machines virtuelles.

Éclairez le parcours

La plateforme Intel vPro et ESET Endpoint Security forment un cadre qui vous permet de naviguer à travers les difficultés liées à la cybersécurité. ESET Endpoint Security et Intel TDT offrent une visibilité accrue et une protection renforcée contre une large variété de menaces sur la sécurité et leurs effets sur votre entreprise, qui vont de la perte de données aux répercussions financières et à la perte de confiance des clients.[1]

Intel TDT détecte les rançongiciels grâce à l'unité de surveillance des performances (PMU) d'Intel, qui se situe sous les applications, le système d'exploitation et même les couches de virtualisation, pour regrouper la télémétrie de l'UC au fur et à mesure de son exécution. Avec Intel TDT, la plateforme de protection de terminal d'ESET peut surveiller les comportements malveillants pour aider à détecter les nouvelles variantes et à réduire les zones d'ombre.

Principales conséquences des attaques pour les entreprises[1]

29 %
Perte de données

23 %
Répercussions financières

18 %
Perte de confiance des clients

Restez mieux protégé grâce à Intel et ESET

En tant que dirigeant d'une PME, vous avez peut-être le sentiment d'être lancé dans une odyssée sans fin en matière de sécurité Pour vous aider à surmonter les difficultés auxquelles vous êtes confronté, ESET et Intel proposent une solution capable de renforcer vos défenses de cybersécurité et d'offrir une protection contre les menaces nouvelles et inconnues.

Avec la plateforme Intel vPro, vous pouvez bénéficier de performances professionnelles, d'une sécurité assistée par matériel et de fonctionnalités de gestion à distance. Et ESET Endpoint Security offre à la fois des performances élevées et une détection préventive des menaces, tout en aidant à limiter les faux positifs.

Naviguez avec confiance à travers votre parcours de sécurité, aussi périlleux qu'il puisse sembler, grâce à la plateforme Intel vPro et à ESET Endpoint Security. Découvrez-en plus sur eset.com/us/eset-and-intel-keep-smbs-safe/.

intel®

[1] ESET. « Rapport d'opinion 2022 sur la sécurité numérique des PME d'ESET : les cyberrisques poussent les PME à adopter des solutions d'entreprise. » 2022. welivesecurity.com/wp-content/uploads/2022/11/eset_smb_digital_security_sentiment_report.pdf.

[2] ESET. « ESET publie une nouvelle étude sur les PME, démontrant que les investissements dans la cybersécurité ne parviennent pas à suivre le rythme des menaces. » eset.com/us/about/newsroom/press-releases/eset-releases-new-smb-research-finds-cybersecurity-investments-not-keeping-pace/.

Imprimé aux États-Unis 0223/MG/PRW/PDF Veuillez recycler 354267-001US