INFORMATION TECHNOLOGY
INTELLIGENCE CONSULTING

Rapport international 2021 d'ITIC sur la sécurité des serveurs et de leurs systèmes d'exploitation

Juin 2021

Table des matières

Synthèse

Pour la troisième année consécutive, les grandes entreprises ont désigné les serveurs stratégiques d'IBM, de Lenovo, de Huawei et de Hewlett-Packard Enterprise (dans cet ordre de classement) comme les plates-formes les plus sécurisées du secteur. Sur ces serveurs, le nombre de violations de données ayant abouti est resté très faible, et ils se sont aussi avérés les plus difficiles à pirater.

C'est ce qui ressort des résultats de la nouvelle enquête internationale d'ITIC sur la sécurité des serveurs. L'enquête a comparé les caractéristiques et les fonctions de sécurité de 15 plateformes de serveurs différentes. Cette enquête indépendante, réalisée sur le Web, a permis d'interroger plus de 1 100 entreprises dans le monde, dans 28 secteurs verticaux différents, entre janvier 2021 et la mi-juin 2021.

Les plates-formes de serveurs d'IBM, de Lenovo, de Huawei, de HPE et de Cisco ont confirmé leur supériorité sur le plan de la fiabilité et de la sécurité, malgré une forte hausse des cyberattaques et des violations de données (42 %) lors de la pandémie mondiale de COVID-19 au cours des 18 derniers mois.

Les meilleurs serveurs, emmenés par IBM Z, IBM POWER, Lenovo ThinkSystem et Huawei KunLun (dans cet ordre), ont tous enregistré des records de performances respectifs en matière de sécurité et de fiabilité/disponibilité pendant la pandémie. Ils ont obtenu les meilleurs résultats sur le plan de la sécurité parmi les 15 principales plates-formes de serveur, dans chaque catégorie de sécurité définie dans l'enquête d'ITIC, notamment :

- Le plus petit nombre de cyberattaques/de violations de données ayant réussi.
- Le plus faible temps d'arrêt total non planifié du serveur, ***tous motifs confondus***, mais aussi le plus faible temps d'arrêt non planifié du serveur à la suite d'un incident de sécurité.
- Le meilleur temps moyen de détection (MTTD) entre le début de l'attaque et le moment où la société a isolé le serveur et l'a arrêté.
- Le meilleur temps moyen de réparation (MTTR) nécessaire à la restauration d'un fonctionnement complètement opérationnel des serveurs, des applications et des réseaux.
- Le volume le moins important constaté de données perdues, volées, détruites, endommagées ou modifiées en conséquence directe d'une violation des données de sécurité (par exemple, attaques par rançongiciels, hameçonnage ou arnaque au président, avec usurpation de l'identité d'un chef d'entreprise).
- Le montant le moins important de pertes monétaires résultant d'une cyberattaque réussie.
- La fiabilité maximale de la sécurité intégrée du serveur (capacité à émettre des alertes ou des avertissements ainsi qu'à repousser les cyberattaques et les violations de données).

Les serveurs stratégiques de Hewlett-Packard Enterprise (HPE) et de Cisco ont également attesté d'une sécurité élevée et se classent parmi les cinq distributions les plus sûres. À l'autre extrémité du panel, les serveurs en marque blanche se sont à nouveau avérés les plus poreux, enregistrant le nombre maximum d'infractions à la sécurité réussies.

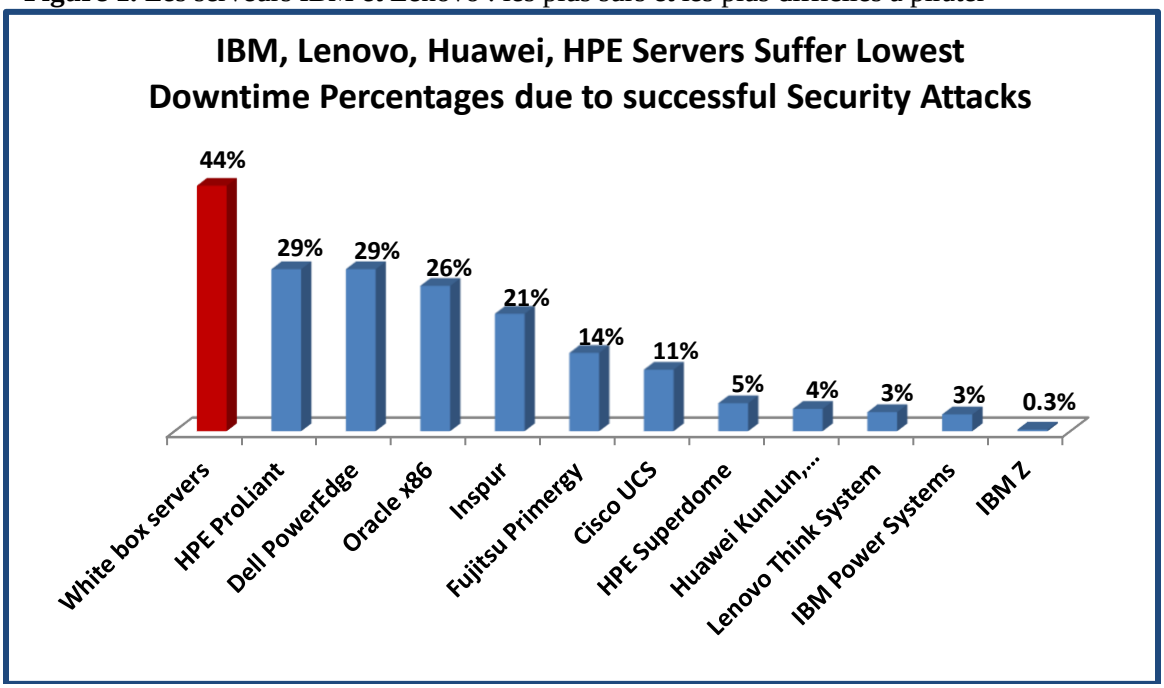
La nouvelle enquête internationale d'ITIC sur la sécurité révèle également que les serveurs IBM, Lenovo, Huawei et HPE stratégiques ont connu les plus faibles pourcentages de durée d'immobilisation due à des cyberattaques et à des violations de données ayant réussi (**Voir la Figure 1).**

Le grand système IBM Z a surpassé toutes les autres distributions de serveurs. Il relève d'une catégorie réellement hors normes, car il a obtenu des notes record de sécurité et de fiabilité dans la nouvelle enquête d'ITIC.

Les violations de données n'ont abouti que sur un infime pourcentage des serveurs IBM Z haut de gamme : - 0,3 %. Parmi les autres grandes plates-formes matérielles, seulement trois pour cent (3 %) des utilisateurs d'IBM Power Systems et de Lenovo ThinkSystem ont signalé la réussite d'une cyberattaque sur leurs systèmes. Moins de quatre pour cent (4 %) des clients du serveur Huawei KunLun et cinq pour cent (5 %) du serveur HPE Integrity Superdome ont pour leur part signalé une violation de sécurité réussie entre janvier 2021 et la mi-juin 2021.

Les cyberattaques ont réussi sur un peu plus d'un serveur Cisco sur 10, soit 11 %. Les matériels de Cisco se sont avérés extrêmement performants, surtout si l'on considère que de nombreux serveurs UCS sont déployés dans des sites éloignés et en périphérie du réseau, lieux qui constituent souvent la première ligne de défense et subissent le gros des cyberattaques. Les serveurs en marque blanche ont été les plus vulnérables aux infractions de sécurité. 44 % des répondants à l'enquête ITIC ont indiqué que ces systèmes avaient été piratés avec succès.

Figure 1. Les serveurs IBM et Lenovo : les plus sûrs et les plus difficiles à pirater



Source : Rapport international 2021 d'ITIC sur la sécurité des serveurs et de leurs systèmes d'exploitation

Dans l'ensemble, les résultats de l'enquête d'ITIC indiquent que l'écart se creuse clairement sur le plan de la sécurité et de la fiabilité des serveurs entre les plateformes les plus performantes et les offres les moins sécurisées. La pandémie mondiale a déclenché une vague de violations de données, d'attaques par rançongiciels, de hameçonnages, de compromission des e-mails professionnels (BEC), d'arnaques au président et d'autres cyberattaques en lien avec le COVID-19 qui, à l'heure actuelle, se poursuivent sans relâche.

Les résultats de la nouvelle enquête de l'ITIC indiquent que la fiabilité et la sécurité sont inextricablement liées, voire symbiotiques. Les violations de la sécurité et des données compromettent immédiatement le temps d'activité et la disponibilité des serveurs, des applications et des réseaux. Les cyberattaques et les violations de données sont coûteuses et dangereuses. Ils compromettent la propriété intellectuelle des entreprises ainsi que celle de leurs partenaires commerciaux, de leurs clients et de leurs fournisseurs. Une cyberattaque réussie peut également exposer les données personnelles des employés.

Ce n'est pas un hasard si les cinq plateformes de serveurs les plus fiables, à savoir IBM Z, IBM Power Systems, Lenovo ThinkSystem, les serveurs KunLun et Fusion de Huawei, le Superdome Integrity de HPE et le serveur Cisco UCS (dans cet ordre) s'enorgueillissent d'une sécurité exceptionnelle.

Introduction

La pandémie mondiale a déclenché une vague de violations de données, d'attaques par rançongiciels, de hameçonnages, de compromission des e-mails professionnels (BEC), d'arnaques au président et d'autres cyberattaques en lien avec le COVID-19 qui, à l'heure actuelle, se poursuivent sans relâche. Ces attaques ont concerné tous les secteurs verticaux, ciblant une myriade de dispositifs et de logiciels d'entreprise et grand public.

Rien ni personne n'est à l'abri. Une sécurité d'infrastructure robuste et inhérente s'impose donc.

La nouvelle enquête d'ITIC révèle que, dans l'ensemble, 73 % des répondants redoutent que leur entreprise ne soit victime d'une attaque ciblée par des pirates professionnels au cours des 12 à 18 mois à venir. Cette projection coïncide avec la fin des cours en distanciel et le retour généralisé en présentiel des élèves et des enseignants du primaire, du secondaire et du supérieur. De même, de nombreuses entreprises et agences gouvernementales opèrent une transition vers un mode de télétravail hybride, à titre de mesure sanitaire.

Les conclusions de l'enquête d'ITIC sont étayées par diverses agences du gouvernement fédéral américain, qui ont émis de multiples alertes au risque de cybersécurité depuis début 2020. Ces agences sont notamment le FBI (Federal Bureau of Investigation, le CISA (Cybersecurity and Infrastructure Security Agency) du Département de la Sécurité intérieure des États-Unis, et le bureau OCIE (Office of Compliance Inspections and Examinations) de la SEC (Securities and Exchange Commission).

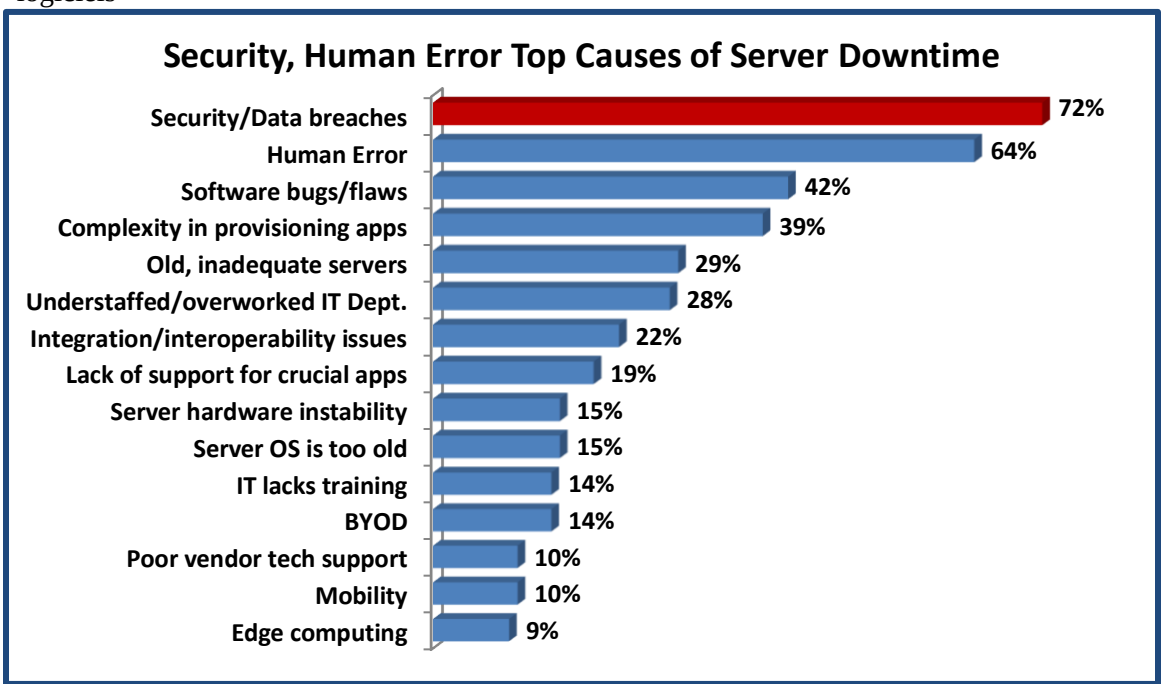
Les menaces de cybersécurité liées au COVID-19 sont les suivantes : escroqueries ciblant les prestations de chômage et les aides de l'État, fraudes dans le secteur de la santé et de la banque, fraudes visant les personnes âgées, et fraudes en lien avec les crypto-monnaies et le gouvernement, selon les alertes du FBI publiées en mai et juin. Le FBI note avoir également observé des cas de « ...criminels se livrant à des comportements prédateurs en ligne à l'encontre d'enfants suivant des cours à distance pendant la pandémie. »

Les solides résultats en matière de sécurité enregistrés par IBM, Lenovo, Huawei, HPE et Cisco (dans cet ordre) sont d'autant plus remarquables qu'ils coïncident avec l'apogée de la pandémie mondiale de COVID-19. Environ 40 % des répondants ont déclaré que leurs serveurs, leurs systèmes d'exploitation et leurs applications professionnelles stratégiques avaient été victimes de cyberattaques réussies depuis la survenue de la pandémie début 2020. Ce chiffre correspond à une augmentation de neuf points de pourcentage par rapport aux 31 % enregistrés au cours des seuls six derniers mois, et d'une forte hausse de 21 points de pourcentage par rapport aux 19 % d'entreprises qui avaient déclaré que leurs serveurs avaient

été victimes de cyberattaques réussies (Enquête internationale ITIC 2020 sur la sécurité des serveurs et de leurs systèmes d'exploitation).

La sécurité est un enjeu technologique et opérationnel qui affecte toutes les entreprises. Environ 72 % des répondants ont cité les violations de sécurité et de données comme les plus grandes menaces pesant sur la fiabilité de l'écosystème des serveurs, des applications, des centres de données, de la périphérie du réseau et du cloud **(voir la Figure 2)**. Les cyberattaques sont plus ciblées, plus envahissantes et plus pernicieuses. Elles sont conçues pour infliger un maximum de dommages et de pertes à leurs victimes, qu'il s'agisse d'entreprises ou de consommateurs.

Figure 2. Les principales causes des immobilisations : la sécurité, l'erreur humaine et les bogues logiciels



Source : Enquête internationale 2021 d'ITIC sur la sécurité des serveurs et de leurs systèmes d'exploitation

Tour d'horizon des menaces : les failles de sécurité et les violations de données, menaces majeures les plus coûteuses pour la fiabilité.

Les violations de données sont une véritable manne qui fournit le gros de son activité à la communauté en plein essor des pirates professionnels. Une cyberattaque réussie est coûteuse à bien des niveaux. En 2020, le coût d'une violation des données s'élevait en moyenne à 3,86 millions de dollars, selon l'étude intitulée

« 2020 Cost of a Data Breach Study » menée conjointement par IBM et le Ponemon Institute.[1] Cela représente un accroissement de 10 % depuis 2015. Les coûts réels varient en fonction de la durée et de la gravité des cyberattaques. Les attaques par rançongiciels continuent sur leur puissante lancée.

Elles sont en outre très coûteuses. L'attaque du 7 mai 2021 par rançongiciel menée par les pirates DarkSide a conduit à la fermeture de l'oléoduc Colonial Pipeline pendant six jours[2]. Cet oléoduc fournit 45 % du gaz et du diesel à la côte Est des États-Unis, du New Jersey jusqu'à la Floride. L'arrêt de l'oléoduc a provoqué des pénuries de gaz dans plusieurs États, dont la Floride, la Caroline du Nord et la Virginie. La cyberattaque n'a pris fin que lorsque le PDG de Colonial Pipeline, Joseph Blount, a accepté de payer aux pirates une rançon de 4,4 millions de dollars. Blount a déclaré au Wall Street Journal qu'il avait autorisé le paiement de la rançon de 4,4 millions de dollars parce que l'équipe dirigeante n'était pas certaine de la gravité de l'intrusion dans ses systèmes, et ignorait par conséquent combien de temps serait nécessaire pour rétablir le fonctionnement de l'oléoduc.

L'attaque par rançongiciel contre le Colonial Pipeline n'est qu'un exemple parmi tant d'autres. Elle met en évidence les vulnérabilités, les risques et le coût élevé associés aux cyberattaques réussies. Le cas du Colonial Pipeline souligne une fois de plus la nécessité de disposer d'une infrastructure de sécurité robuste et de qualité irréprochable. Les serveurs sont des éléments fondamentaux de tout réseau d'entreprise et de tout écosystème.

Un rapport de DTEX Systems révèle que « seulement 30 % des entreprises étaient préparées à sécuriser un passage complet au télétravail ». L'étude de DTEX Systems révèle également que près de 75 % des entreprises s'inquiètent des risques de sécurité introduits par les utilisateurs en télétravail. 73 % des entreprises ont admis n'avoir qu'une visibilité partielle, voire nulle, de l'activité des utilisateurs si leur réseau privé virtuel est désactivé par les télétravailleurs. Un autre résultat alarmant est que les télétravailleurs utilisent leur ordinateur portable de travail pour leur usage personnel. 25 % des personnes interrogées reconnaissent que cela augmente le risque d'infection de drive-by-downloads (téléchargements furtifs), et 15 % déclarent que leurs entreprises sont plus sensibles aux attaques par hameçonnage.

L'enquête d'ITIC indique que le coût horaire des temps d'arrêt continue de grimper. Il dépasse désormais 300 000 $ pour 89 % des PME et des grandes entreprises. Dans l'ensemble, 42 % des PME et des grandes entreprises interrogées ont déclaré qu'en moyenne, une seule heure d'immobilisation coûte plus d'un

[1] « 2020 Cost of a Data Breach Study », IBM and the Ponemon Institute. URL : https://www.ibm.com/security/data-breach

[2] « Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom », The Wall Street Journal, 19 mai 2021. URL : https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

million de $ à leur entreprise. Dans le pire des scénarios, une violation des données qui se produit pendant les pics d'utilisation et qui interrompt des opérations métier cruciales pour l'entreprise peut leur coûter plusieurs millions de dollars par minute. Toute entreprise victime d'une indisponibilité prolongée de plusieurs heures ou de plusieurs jours à la suite d'une attaque ciblée par rançongiciel est quasiment certaine d'encourir des dommages se chiffrant en millions de dollars.

Outre les pertes monétaires évidentes dues à la baisse de la productivité et à l'interruption des opérations, les entreprises doivent aussi tenir compte du nombre d'heures de main-d'œuvre et des effectifs des professionnels (responsables IT et administrateurs de la sécurité) devant participer aux tâches de résolution et de remise totale en service. Les entreprises doivent également déterminer si des données ou de la propriété intellectuelle ont été perdues, volées, endommagées, détruites ou modifiées. Elles doivent également y ajouter le coût des litiges éventuels, ainsi que les amendes ou les sanctions civiles ou pénales potentielles découlant des incidents de sécurité et des violations de données. Certains coûts, tels que l'atteinte à la réputation d'une entreprise, sont incalculables et peuvent entraîner une perte de contrats et d'activités.

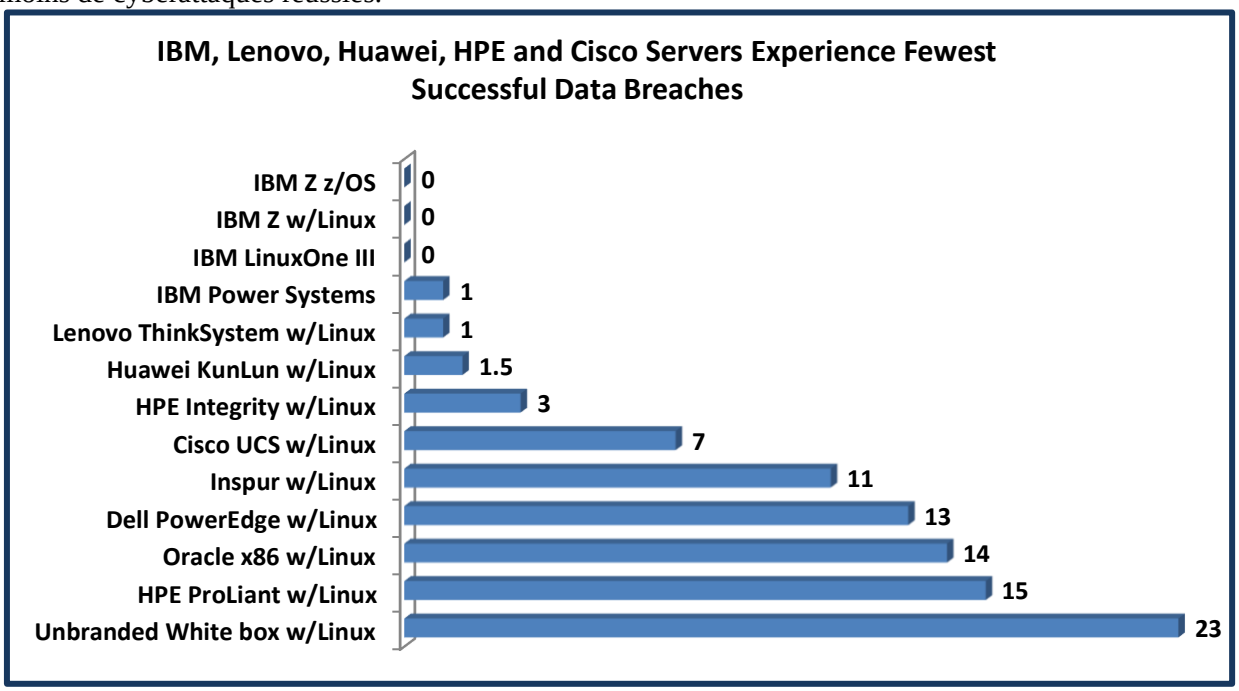
Les pirates sélectionnent leurs cibles avec une grande précision et sont prompts à profiter de chaque opportunité. La pandémie de COVID-19 en est un excellent exemple. Les pirates informatiques ont immédiatement ciblé les télétravailleurs et les étudiants en distanciel suivant des cours en ligne ou sur Zoom. Ils ont privilégié ces cibles vulnérables : autorités locales et régionales, académies scolaires de petite et de moyenne taille, hôpitaux, cliniques, cabinets médicaux et succursales bancaires ne disposant pas forcément d'un système de sécurité sur site activé en permanence, ni de la présence d’administrateurs IT, et qui peuvent ne pas avoir installé de dispositifs de sécurité récents.

Les fournisseurs de serveurs : IBM, Lenovo, Huawei et HPE redoublent d'efforts sur la sécurité

Sans surprise, des fournisseurs tels qu'IBM, Lenovo, Huawei et HPE, qui obtiennent régulièrement les meilleures notes en matière de fiabilité de leurs serveurs, figurent également parmi les plateformes matérielles les plus sûres. Ces fournisseurs, et plus récemment Cisco, ont fait de la sécurité des serveurs une priorité majeure. Lenovo a par ailleurs étendu cette priorité aux ordinateurs personnels et aux ordinateurs portables. Ils ont investi massivement dans le renforcement de la sécurité inhérente à leurs offres de produits au cours des dernières années. Ainsi, lorsque la pandémie a frappé, ils disposaient déjà d'une robuste sécurité intégrée qui leur a été très utile.

Comme l'indique le **Graphique 3**, ce sont les plateformes de serveur les plus sécurisées qui ont subi le moins de cyberattaques réussies. Les répondants utilisant IBM Z avec z/OS et Red Hat Enterprise Linux (RHEL) et IBM LinuxONE III ont tous déclaré que ces plates-formes n'avaient subi aucune cyberattaque réussie au cours des 16 mois écoulés. Ils sont suivis par les serveurs IBM Power Systems et Linux ThinkSystem (une cyberattaque chacun) ; puis Huawei KunLun (deux cyberattaques en moyenne) ; puis HPE Integrity (trois violations réussies) et Cisco UCS (sept violations de données). Les serveurs en marque blanche sont les plus poreux, avec une moyenne de 20 violations de données réussies au cours des 16 derniers mois.

Figure 3. Les serveurs d'IBM, de Lenovo, de Huawei, de HPE et de Cisco sont ceux qui connaissent le moins de cyberattaques réussies.



Source : Rapport international 2021 d'ITIC sur la sécurité des serveurs et de leurs systèmes d'exploitation

Données et analyse : résultats de la qualité de la sécurité par fournisseur

Pour récapituler, l'Enquête internationale 2021 d'ITIC sur la sécurité des serveurs et de leurs systèmes d'exploitation constate que les serveurs IBM Z, IBM Power Systems, Lenovo ThinkSystem et les serveurs KunLun et Fusion de Huawei (dans cet ordre) ont obtenu les meilleurs résultats dans toutes les catégories de sécurité, notamment :

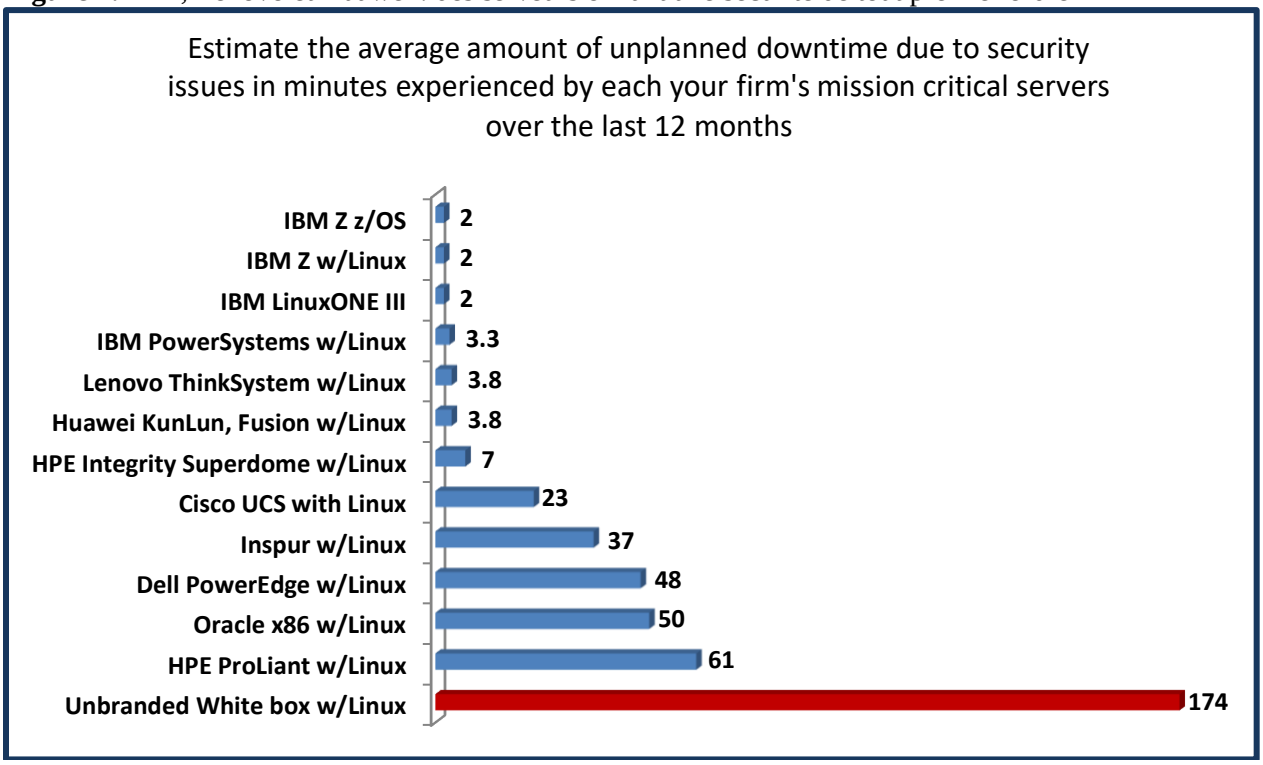
- Le plus petit nombre de cyberattaques/de violations de données **ayant réussi**.
- Le plus faible temps d'arrêt total non planifié du serveur, ***tous motifs confondus***, mais aussi le plus faible temps d'arrêt non planifié du serveur à la suite d'un incident de sécurité.
- Le meilleur temps moyen de détection (MTTD) entre le début de l'attaque et le moment où la société a isolé le serveur et l'a arrêté.
- Le meilleur temps moyen de réparation (MTTR) nécessaire à la restauration d'un fonctionnement complètement opérationnel des serveurs, des applications et des réseaux.
- Le volume le moins important constaté de données perdues, volées, détruites, endommagées ou modifiées en conséquence directe d'une violation des données de sécurité (par exemple, attaques par rançongiciels, hameçonnage ou arnaque au président, avec usurpation de l'identité d'un chef d'entreprise).

- Le montant le moins important de pertes monétaires résultant d'une cyberattaque réussie.
- La fiabilité maximale de la sécurité intégrée du serveur (capacité à émettre des alertes ou des avertissements ainsi qu'à repousser les cyberattaques et les violations de données).

Comme le montre **la Figure 4**, les serveurs stratégiques IBM Z, IBM Power Systems, Lenovo ThinkSystem et Huawei KunLun sont ceux qui ont subi le moins de temps d'arrêt non planifié en conséquence directe d'incidents de sécurité et de violations de données.

En moyenne, les serveurs IBM Z et IBM LinuxONE III ne comptabilisent que 2 minutes chacun en moyenne de temps d'arrêt non planifié en raison de problèmes de sécurité. Ils sont talonnés par les serveurs IBM POWER8 et IBM POWER9, qui ont subi un peu plus de 3 minutes d'arrêts non planifiés par serveur suite à un problème de sécurité. Les serveurs Lenovo ThinkSystem et Huawei KunLun et Fusion ont subi chacun une moyenne de 3,8 minutes de temps d'arrêt non planifié lié à des incidents de sécurité. Une fois de plus, les serveurs en marque blanche, dont beaucoup exécutent des versions sans licence de systèmes d'exploitation de serveur et d'applications logicielles, ont accumulé 174 minutes (presque 3 heures) de temps d'arrêt directement attribuable à des problèmes de sécurité. Traduits en chiffres, ce constat permet d'établir que les serveurs IBM Z sont jusqu'à 87 fois plus sécurisés et fiables que les serveurs en marque blanche, tandis que les IBM POWER8 et POWER9 sont jusqu'à 58 fois plus sécurisés que les serveurs en marque blanche.

Figure 4. IBM, Lenovo et Huawei : des serveurs offrant une sécurité de tout premier ordre



Source : Rapport international 2021 d'ITIC sur la sécurité des serveurs et de leurs systèmes d'exploitation

Le temps moyen de détection, un baromètre vital

Les cyberattaques et les violations de données font partie de la vie de l'entreprise à l'ère numérique. À un moment donné, toute entreprise, ainsi que ses principaux serveurs stratégiques, ses systèmes d'exploitation de serveur et ses applications, seront victimes d'une tentative de violation des données, qui parfois réussira.

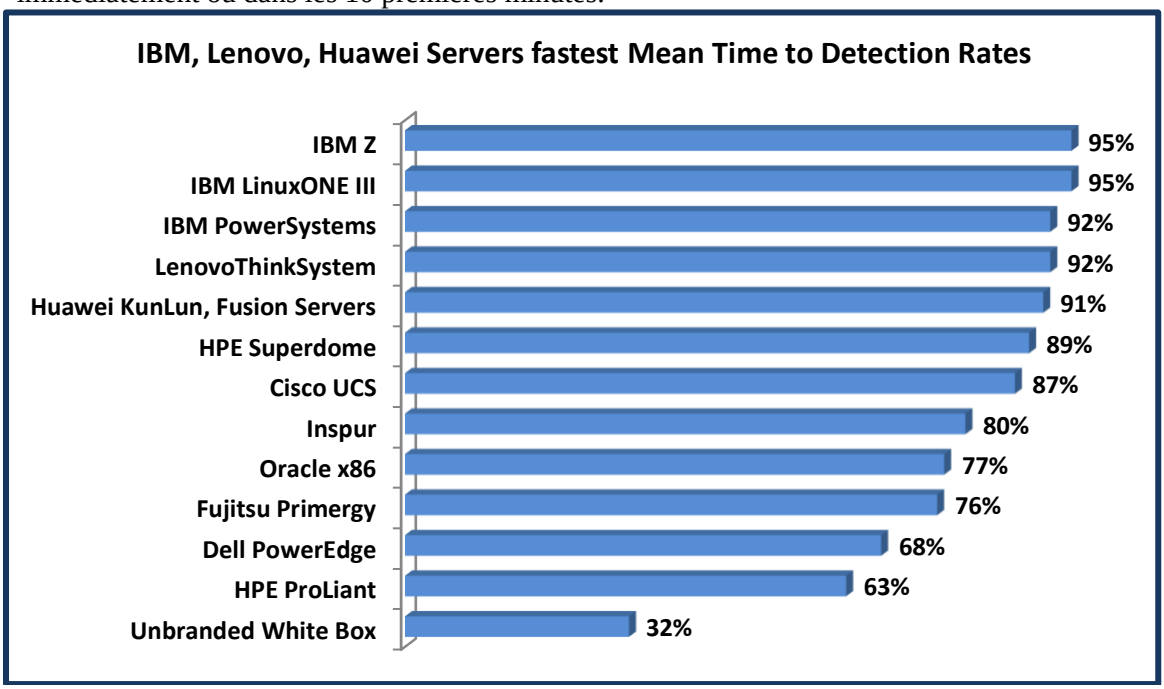
Les entreprises doivent pouvoir compter sur une sécurité robuste et intégrée de l'infrastructure et des serveurs, capable de reconnaître le danger, d'envoyer des alertes et des alarmes et d'isoler les menaces. Il est primordial que l'entreprise soit bien préparée et qu'elle dispose d'une équipe bien entraînée de professionnels de la sécurité et d'administrateurs IT.

Plus les serveurs et les logiciels de l'entreprise peuvent détecter rapidement un problème de sécurité et y répondre, plus elle aura de chances d'isoler et de déjouer l'attaque ***avant*** qu'elle puisse infiltrer l'écosystème du réseau, interrompre les transactions de données et les opérations quotidiennes et accéder aux données sensibles et à la propriété intellectuelle.

La Figure 5 montre qu'une fois de plus, les serveurs IBM Z, IBM Power Systems, Lenovo ThinkSystem, Huawei KunLun et Fusion, HPE Superdome et Cisco UCS (dans cet ordre) ont brillamment déjoué les cyberattaques. Ces serveurs ont obtenu les meilleurs pourcentages de temps moyen de détection (MTTD) parmi toutes les plateformes de serveurs.

Une proportion écrasante de répondants utilisant IBM Z et IBM LinuxOne III (95 %) ont indiqué que leurs serveurs étaient capables de détecter une tentative de violation de sécurité « immédiatement ou dans les 10 premières minutes » de la cyberattaque et de l'arrêter. Ils étaient suivis dans l'ordre par les distributions IBM Power Systems, Lenovo ThinkSystem et Huawei KunLun. 92 % des utilisateurs de chacune de ces plateformes ont déclaré pouvoir reconnaître et repousser une violation de sécurité « immédiatement ou dans les 10 premières minutes ». La rapidité avec laquelle les serveurs d'infrastructure stratégique, les systèmes d'exploitation et les applications critiques peuvent déjouer une cyberattaque augmente d'autant plus les chances de l'entreprise de réduire, voire éviter totalement une durée d'immobilisation, ou d'échapper à un vol, une modification, un endommagement ou une compromission des données et de la propriété intellectuelle.

Figure 5. Plus de 90 % des serveurs IBM, Lenovo et Huawei détectent les attaques de sécurité immédiatement ou dans les 10 premières minutes.



Source : Rapport international 2021 d'ITIC sur la sécurité des serveurs et de leurs systèmes d'exploitation

Résultats de la qualité de la sécurité par fournisseur

Sécurité IBM - Points clés de l'enquête

- **Les serveurs IBM Z** continuent d'obtenir les meilleures notes de toutes les plateformes de serveur en termes de fiabilité, d'accessibilité, de performances et de sécurité prises dans leur globalité. La famille IBM Z (« Z » signifiant zéro durée d'immobilisation) surpasse constamment **tous** ses concurrents dans toutes les catégories de fiabilité. Elle se caractérise en outre par le plus faible coût total de possession et par le retour sur investissements le plus rapide. Les serveurs z13, z14 et z15 Systems ont obtenu les meilleurs résultats sur le plan de la fiabilité/disponibilité, de la disponibilité des applications et de la sécurité globale, calculés en minutes réelles d'arrêt non planifié par serveur et par an. Les distributions du grand système IBM z et IBM LinuxONE attestent toutes les deux d'une tolérance réelle aux pannes de seulement 0,60 - soit moins d'une minute d'***arrêt non planifié*** par serveur et par an en raison de défauts du serveur, contre 0,74 seconde en moyenne pour les plateformes Z et LinuxONE (voir l'enquête internationale 2019 d'ITIC sur la fiabilité des serveurs). Bien que la différence de 0,14 seconde de durée d'immobilisation par serveur semble négligeable, elle réduit en fait l'immobilisation de près de 19 %. En outre, elle abaisse le coût total de possession de l'IBM Z et de LinuxONE de 230 $. Le résultat permet de passer de 1 232 $ par serveur/par minute en 2019 à 1 002 $ par serveur/ par minute, selon la nouvelle enquête internationale 2021 d'ITIC sur la sécurité des serveurs. Globalement, l'IBM Z n'enregistre que 4,32 secondes de durée mensuelle d'immobilisation, soit

un arrêt quasi-imperceptible. Compte tenu de la recrudescence des cyberattaques et des violations de données, la sécurité exceptionnelle du serveur IBM Z se révèle tout aussi importante. Le Z continue d'enregistrer le plus faible pourcentage de violations de données réussies entre janvier et mi-juin 2021 : moins de 1 %. En outre, les utilisateurs d'IBM Z et de LinuxONE III ont également signalé un temps moyen de détection (MTTD) record. 95 % des entreprises ayant répondu à l'enquête d'ITIC déclarent ainsi que leurs administrateurs IT et leurs responsables de la sécurité ont pu détecter et arrêter les cyberattaques sur ces plateformes. Aussi bien sur le plan individuel que collectif, ces résultats soulignent le succès des offres Z et LinuxONE III. Les plateformes ont également été optimisées suite à l'acquisition de Red Hat par IBM en 2019, qui a entraîné une augmentation significative des charges de travail Linux sur les plateformes Z et LinuxONE. L'équipe dirigeante d'IBM a déclaré publiquement que la compagnie avait observé une hausse de 55 % des MIPS (millions d'instructions par seconde) Linux. Elle a également observé que 92 de ses 100 grands clients IBM Z exécutent des charges de travail Linux. Dans l'ensemble, 100 à 200 nouveaux déploiements de la plateforme Z ont lieu par an, selon IBM.

- **Le système LinuxONE III** d'IBM est basé sur la plateforme IBM Z. Il est destiné spécialement aux environnements de cloud hybride et utilise le chiffrement omniprésent d'IBM Z. La plateforme LinuxONE III et l'IBM z15 intègrent également IBM Hyper Protect Data Controller, qui assure une protection et une confidentialité transparentes de bout en bout au niveau des données. IBM Hyper Protect Data Controller permet aux entreprises de chiffrer les données, d'accorder et de révoquer l'accès aux données, et d'en conserver la maîtrise, même lorsqu'elles sont retirées du système d'enregistrement**.** Résultat : IBM LinuxONE III figure parmi les serveurs qui ont obtenu les meilleures évaluations sur le plan de la sécurité et de la fiabilité dans l'enquête 2021 d'ITIC. 95 % des entreprises utilisant LinuxONE III détectent et stoppent les violations de données « immédiatement ou dans les 10 premières minutes » de l'attaque.
- **IBM Power Systems** : 92 % des clients utilisant IBM Power Systems ont déclaré que leurs responsables de la sécurité et leurs administrateurs IT pouvaient détecter et déjouer les attaques « immédiatement ou dans les 10 premières minutes » d'une violation. Les systèmes IBM POWER9 scale-out (par ajout) d'IBM sont commercialisés depuis trois ans. Les serveurs Power10 de nouvelle génération devraient faire leur arrivée à l'automne 2021. IBM modernise et met à jour en permanence cette gamme et accorde une importance toute particulière aux performances, à la prise en charge des charges de travail stratégiques et de l'analytique évoluée, aux bases de données en mémoire et à la sécurité intégrée. Tous les modèles Power Systems sont prêts pour le cloud. Les IBM Power Systems intègrent la sécurité dans toutes les couches de la pile : processeur, systèmes, microprogramme, système d'exploitation et hyperviseur. Grâce au chiffrement accéléré intégré à la puce, les données sont protégées, qu'elles soient en mouvement ou au repos. Selon IBM, son hyperviseur PowerVM ne présente aucune faille de sécurité connue. Les serveurs POWER9 sont également prêts pour le cloud et incluent des fonctions intégrées de virtualisation PowerVM. Les serveurs POWER9 scale-out (par ajout) sont conçus pour être intégrés aux stratégies cloud et d'IA des entreprises. Ils offrent les hautes performances et les fonctions RAS (fiabilité, disponibilité et facilité de maintenance) requises pour prendre en charge des charges de travail critiques telles que les bases de données Db2 et Oracle d'IBM ainsi que le protocole SAP HANA. Le Power10 a un format 7nm caractérisé par son efficacité énergétique et sa performance. IBM a estimé que ces caractéristiques permettraient de tripler l'efficacité énergétique, la capacité de charge de travail et la densité de conteneur par rapport au POWER9. En outre, les prochains serveurs Power10 intègreront également toute une série de fonctionnalités avancées, notamment la prise en charge de clusters de mémoire de l'ordre de plusieurs pétaoctets.

Ceci permettra à la fonction cloud de gérer des charges de travail très exigeantes en mémoire. Le Power10 comportera également des fonctions de sécurité matérielles similaires au chiffrement de mémoire transparent pour la sécurité de bout en bout. Le processeur IBM Power10 est conçu pour offrir des performances de chiffrement nettement plus rapides, car il quadruple le nombre de moteurs de chiffrement AES (Advanced Encryption Standard) par cœur par rapport à l'IBM POWER9. Il répond ainsi aux normes très exigeantes d'aujourd'hui et aux futures normes cryptographiques, telles que la cryptographie post-quantique (QSC) et le chiffrement totalement homomorphe. Il apporte également de nouvelles améliorations à la sécurité des conteneurs.

Sécurité Lenovo - Points clés de l'enquête

- **Les serveurs Lenovo ThinkSystem** ont obtenu les meilleurs pourcentages de temps moyen de détection (MTTD) parmi tous les serveurs Intel x86. En effet, 92 % des répondants au sondage ont déclaré que leurs responsables de la sécurité et leurs administrateurs IT avaient détecté et stoppé les tentatives de cyberattaque et de violation des données immédiatement ou dans les 10 premières minutes de l'agression. Ce n'est pas un hasard. Au cours des sept années écoulées depuis le rachat par Lenovo de l'activité des serveurs x86 d'IBM et des dix années depuis son rachat de la gamme de PC et d'ordinateurs portables d'IBM, Lenovo a fait de la sécurité une priorité absolue. L'optimisation de ses serveurs et de ses ordinateurs de bureau a été constante : Lenovo améliore et fortifie continuellement les performances, la fiabilité et la sécurité de ses serveurs, de ses PC et de ses ordinateurs portables. Le service technique et le support clients de Lenovo sont également de très grande qualité. Les serveurs ThinkSystem de Lenovo ont continué d'améliorer leur fiabilité, affichant en moyenne leur meilleure disponibilité à ce jour : 1,51 minute de durée d'immobilisation par serveur due à des problèmes matériels. Tout comme IBM, Lenovo a construit et exécuté une approche tactique et stratégique de la sécurité à la fois brillante et efficace. En 2018, Lenovo a dévoilé la technologie avancée ThinkShield de sécurité de bout en bout conçue pour ses PC et ses ordinateurs portables. ThinkShield a permis aux PC et aux serveurs Lenovo de bien résister à la recrudescence des cyberattaques au cours des trois dernières années. Pendant la pandémie mondiale de COVID-19, lorsque de nombreux établissements et entreprises ont opté pour le télétravail ou l'enseignement en distanciel, les responsables de la sécurité et les administrateurs IT ont eu toutes les peines du monde à faire face aux violations de données. La solution de sécurité ThinkShield de Lenovo apporte une aide cruciale. ThinkShield, par exemple, joue un rôle prédominant sur le ThinkSystem SE350. Ce modèle est le premier serveur Edge spécialement conçu par Lenovo. Il est destiné à la périphérie du réseau pour distribuer une bande passante optimale, renforcer la sécurité et écourter les temps d'arrêt.
  Le ThinkSystem SE350 est un serveur à faible encombrement. Il mesure 1,75 pouces de haut, 8,1 pouces de large et 14,9 pouces de profondeur et peut être monté sur une paroi, installé sur une étagère ou placé dans une armoire. Le ThinkSystem SE350 offre également des performances élevées. Il est basé sur le processeur Intel Xeon-D et est équipé de 256 Go de mémoire RAM et de 16 To de stockage SSD interne. Le ThinkSystem SE350 est équipé de dispositifs de sécurité physique étendus : panneau de verrouillage, détection d'intrusion, système anti-falsifications et stockage chiffré. Il propose un logiciel de déploiement sans contact. La stratégie globale de Lenovo associe l'innovation à des systèmes de centres de données fiables, flexibles et sécurisés. Il s'agit d'une stratégie judicieuse qui a également des ramifications importantes pour les serveurs et les réseaux de Lenovo et, en fin de compte, pour ses entreprises clientes. L'erreur humaine est de loin la principale cause des indisponibilités des serveurs. Les utilisateurs finaux sont

traditionnellement le maillon le plus faible de l'ensemble de la chaîne de sécurité. C'est une réalité qui a particulièrement été mise en évidence lors de la pandémie mondiale de COVID-19, pendant laquelle un pourcentage important de personnes ont télétravaillé ou ont suivi un enseignement à distance. Il est donc logique que Lenovo renforce la sécurité des ordinateurs en plus de celle des serveurs. Lenovo applique des normes, des politiques et des procédures de sécurité rigoureuses dans ses installations de fabrication et dans sa chaîne d'approvisionnement mondiale. Les ingénieurs qualité de Lenovo se réservent le droit d'effectuer un audit des fournisseurs de confiance de la société à tout moment, ce qui permet à Lenovo de mieux contrôler et connaître la sécurité des composants de ses appareils. ThinkShield offre également une sécurité au niveau de la conception. Il inclut un système BIOS et un microprogramme sécurisés, ainsi que des filtres de confidentialité et des obturateurs de la caméra des ordinateurs portables, qui contribuent à réduire le « piratage visuel » lorsque des utilisateurs mobiles se rendent dans des lieux publics. ThinkShield protège les identités et les données d'identification des utilisateurs. Il propose des fonctionnalités d'authentification certifiées FIDO et une intégration à Intel Authenticate, avec jusqu'à 7 facteurs d'authentification. Le ThinkShield est également doté d'une protection Smart USB basée sur le BIOS, qui fonctionne en configurant les ports USB de façon à ce qu'ils ne répondent qu'aux claviers et aux périphériques de pointage. Lenovo souligne également que ses plates-formes ouvertes de serveur, de stockage, de mise en réseau et de gestion des systèmes s'intègrent de manière transparente aux environnements existants et plus anciens. Lors d'entretiens en personne avec des analystes d'ITIC, les clients de Lenovo ont cité la facilité du déploiement et de l'intégration, ainsi que la compatibilité avec les versions antérieures, comme facteurs contribuant à la fiabilité et à la stabilité sous-jacentes de la plateforme ThinkSystem. Les utilisateurs de Lenovo ont également fait l'éloge du service après-vente et du support. Le système de conception de Lenovo prend en charge les bases de données stratégiques, les applications d'entreprise, l'analytique des big data et les environnements cloud et virtuels. Ces deux systèmes intègrent de nombreuses fonctions de tolérance aux pannes et des options de haute disponibilité dans un module sans capot à haute densité, optimisé pour les armoires. Le module minimise l'espace nécessaire à la prise en charge des opérations massives de l'informatique en réseau. La maintenance est simplifiée, car le système n'a jamais besoin d'être retiré de l'armoire. En août 2020, Lenovo a présenté plusieurs nouveaux modèles de ses serveurs mono-socket ThinkSystem basés sur les processeurs de la série AMD EPYC 702 d'Advanced Micro Devices. Les nouveaux ajouts au portefeuille de serveurs de Lenovo sont conçus spécifiquement pour gérer les charges de travail en constante évolution et grosses consommatrices de données, telles que la sécurité vidéo, le stockage défini par logiciel et le renseignement réseau. Ils prennent également en charge les environnements virtualisés et de périphérie du réseau, dans lesquels la sécurité est primordiale. Il en résulte une solution qui associe puissance et efficacité pour les clients qui privilégient l'équilibrage entre d'une part, la capacité de traitement et la sécurité, et d'autre part, une évolutivité simple. Selon Lenovo, les deux nouveaux serveurs ThinkSystem « offrent les performances d'un serveur à deux sockets pour le prix d'un serveur mono-socket » et peuvent réduire d'environ 73 % les coûts de licence logicielle des clients et d'environ 46 % le coût total de possession.

Sécurité Cisco UCS - Points clés de l'enquête

- **Le serveur UCS (Unified Computing System)** de Cisco se maintient en bonne posture : il a conservé les 2,3 minutes de durée d'immobilisation du serveur, obtenues pour la première fois lors de la mise à jour semestrielle de l'enquête internationale 2020 d'ITIC sur les serveurs et les systèmes d'exploitation de serveurs. De janvier à la mi-juin 2021, les serveurs de Cisco se sont régulièrement maintenus à 2,3 minutes de durée d'immobilisation par serveur. Ce n'est pas une mince affaire si l'on considère que de nombreux serveurs Cisco UCS sont déployés en périphérie du réseau, en première ligne des cyberattaques. Malgré cela, 87 % des répondants utilisant Cisco UCS ont déclaré pouvoir détecter, isoler et stopper les cyberattaques immédiatement ou dans les 10 premières minutes. Ils ont également indiqué que les serveurs ont subi sept (7) cyberattaques réussies chacun au cours des 18 derniers mois. En réponse à l'augmentation des violations de données, Cisco a commencé à publier le guide Cisco UCS Hardening Guide. Ce document peut être téléchargé gratuitement. Il contient des informations détaillées qui aident les utilisateurs à sécuriser les dispositifs de la plateforme Cisco UCS pour améliorer la sécurité du réseau. Structuré autour des trois plans qui catégorisent les fonctions d'un périphérique réseau, ce document fournit une vue d'ensemble de chaque fonction logicielle de Cisco UCS et contient des références à la documentation connexe. En outre, Cisco a introduit plusieurs mises à niveau de la gestion et des performances visant à améliorer le coût total de possession et à accélérer l'installation et le déploiement. Cisco affirme que son serveur UCS permet une réduction de 86 % du câblage et une application des accès en quelques minutes (contre plusieurs jours ou semaines auparavant), tout en réduisant les dépenses d'investissement de plus de 40 %. Les fabricants garantissent aux utilisateurs une compatibilité de 100 % entre les composants. L'équilibrage de charge ne pose aucun problème.

Sécurité HPE - Points clés de l'enquête

- **La gamme de serveurs Superdome** de HPE (y compris les modèles Integrity et Flex) offre également une fiabilité élevée de 99,999 % et de 99,9999 % pour une majorité (92 %) de ses clients. 89 % des répondants utilisant un serveur HPE ont déclaré que leurs entreprises ont découvert et stoppé les violations de sécurité « immédiatement ou dans les 10 premières minutes ». Les données de l'enquête d'ITIC montrent que les serveurs HPE Superdome ont subi chacun trois (3) cyberattaques réussies au cours des 18 derniers mois. Cela place les plates-formes matérielles HPE dans les cinq premiers systèmes les plus sécurisés. Le portefeuille du Superdome bénéficie également de la forte stabilité intrinsèque des matériels HPE. Pour HPE, la sécurité, l'innovation en matière de fonctionnalités/performance, le service technique après-vente et le support clients sont des priorités majeures. Une telle approche est essentielle dans une ère numérique de plus en plus insécurisée, complexe et interconnectée. HPE est bien implanté dans les entreprises toutes tailles confondues, des PME aux plus grandes multinationales. Le serveur HPE Superdome Flex offre des fonctions RAS (fiabilité, disponibilité et facilité de maintenance) et une sécurité de bout en bout pour protéger les charges de travail vitales. Le serveur HPE Superdome Flex, par exemple, peut évoluer jusqu'à 32 sockets. C'est 2,3 fois l'évolutivité des serveurs de la génération précédente. Il dispose également d'une conception en mémoire et d'une capacité de mémoire de 768 Go, soit 48 To téraoctets sur une seule plateforme. Le serveur HPE Superdome Flex a une conception modulaire qui évolue de manière flexible de 4 à 32 sockets, par incréments de 4 sockets. Selon HPE, le serveur Superdome Flex a un prix d'entrée de gamme plus avantageux pour les charges de travail stratégiques à 4 sockets. Son coût d'acquisition est

inférieur de 45 % à celui des modèles précédents. HPE met également l'accent sur la fiabilité, en affirmant que les fonctions intégrées de fiabilité, de disponibilité et de facilité de maintenance du serveur Superdome Flex offrent une disponibilité de 99,999 %. Selon HPE, le serveur Superdome Flex réduit également les erreurs humaines grâce à son moteur d'analyse de gestion prédictive des erreurs. La sécurité et l'erreur humaine sont deux problèmes étroitement liés qui affectent la sécurité et la fiabilité. Ce moteur prédit les défaillances matérielles et déclenche une réparation automatique sans qu'il soit nécessaire de recourir à une intervention humaine ou de faire intervenir un opérateur. L'approche « Firmware First » de HPE cantonne les erreurs au niveau du microprogramme, y compris les erreurs de mémoire, avant qu'une interruption ne puisse se produire au niveau de la couche du système d'exploitation. HPE assure également la continuité des charges de travail Linux avec HPE Serviceguard for Linux (SGLX), sa solution de mise en cluster à haute disponibilité pour la reprise après incident. Elle permet aux entreprises de protéger leurs serveurs exécutant Linux contre une multitude de défaillances de l'infrastructure et des applications dans des environnements physiques ou virtuels, quelle que soit la distance.

Sécurité Huawei - Points clés de l'enquête

- Au cours des cinq dernières années, Huawei, dont le siège social se trouve à Shenzhen, en Chine, s'est imposé comme l'un des cinq principaux meilleurs fournisseurs mondiaux de serveurs, grâce à ses serveurs stratégiques haut de gamme KunLun et à ses serveurs généralistes Fusion x 86. D'après les deux enquêtes internationales 2021 d'ITIC, l'une sur la fiabilité des serveurs et des systèmes d'exploitation, et l'autre sur la sécurité des serveurs, les serveurs KunLun et Fusion de Huawei figurent également parmi les trois plateformes matérielles les plus fiables et les plus sécurisées. Une majorité de 91 % des répondants utilisant des serveurs Huawei ont indiqué que leurs responsables de la sécurité et leurs administrateurs IT avaient détecté et stoppé les tentatives de violation « immédiatement ou en moins de 10 minutes ». Ils ont en outre précisé que les serveurs KunLun et Fusion de Huawei avaient subi chacun 1,5 cyberattaques au cours des 18 derniers mois. Depuis 2015, Huawei a renforcé ses fonctionnalités avancées, la sécurité inhérente et les performances globales de ses serveurs. Pour pouvoir concurrencer des rivaux tels que Cisco, Fujitsu, HPE, IBM, Inspur, Lenovo et d'autres, la famille de serveurs de Huawei comprend des serveurs lames et en armoire généralistes, ainsi que des serveurs stratégiques pour le calcul hautes performances (HPC). Huawei a également doté ses serveurs de capacités avancées pour pouvoir prendre en charge les applications émergentes nécessitant des ressources de traitement intensives, telles que l'intelligence artificielle, l'analytique du big data, l'apprentissage en profondeur et l'apprentissage automatique. Huawei souligne son intérêt pour la sécurité en publiant des documents sur les bonnes pratiques sur le thème « Comment construire un système de défense proactif ? », via sa solution HiSec qui permet une détection des menaces, une réponse aux menaces, des opérations de sécurité et une maintenance plus intelligentes. Selon Huawei, HiSec améliore les capacités de prévention des menaces dans les réseaux d'entreprise et les infrastructures de télécommunications. Il en résulte une efficacité accrue des opérations et de la maintenance de sécurité, ainsi qu'une réduction de leur coût. En outre, Huawei propose un certain nombre de nouvelles offres de sécurité pour ses diverses solutions de serveur dans le centre de données, le cloud et le réseau.

Conclusions

La sécurité est l'enjeu numéro un qui compromet la fiabilité et la disponibilité des serveurs, de leurs systèmes d'exploitation et des applications stratégiques. Toutes les entreprises doivent faire de la sécurité une priorité et collaborer étroitement avec leurs fournisseurs pour atténuer les risques de sécurité et les ramener à un niveau acceptable.

Chaque seconde et minute supplémentaires d'immobilisation du serveur et d'indisponibilité des applications ont un impact négatif sur les opérations, la productivité des employés et le chiffre d'affaires.

Les résultats de l'enquête internationale 2021 d'ITIC sur la fiabilité des serveurs et de leurs systèmes d'exploitation indiquent que le grand système IBM Z et les serveurs IBM Power, suivis de près par les serveurs ThinkSystem de Lenovo, KunLun de Huawei et Integrity Superdome de HPE, ont consolidé et confirmé leur statut de serveurs les plus fiables du marché. La plateforme d'entreprise IBM Z est la seule à offrir une fiabilité avec une tolérance aux pannes de 99,9999 % et 99,99999 % pour plus de 93 % des entreprises qui l'utilisent. Si l'on exclut les superordinateurs et les matériels à haute disponibilité, aucune plate-forme de serveur n'arrive à s'approcher du niveau de fiabilité, de disponibilité et de sécurité quasiment sans faille de l'IBM Z.

9 répondants sur 10 ont affirmé que les solutions IBM Power Systems et ThinkSystem de Lenovo ont obtenu les chiffres tant convoités de 99,999 % et de 99,9999 % de fiabilité et de disponibilité. Les plates-formes IBM Power Systems et Lenovo ThinkSystem sont jusqu'à 30 fois plus fiables et jusqu'à 36 fois plus abordables et économiques que les serveurs en marque blanche les moins performants.

Autre réalisation notable, IBM et Lenovo ont obtenu la première ou la deuxième place dans toutes les catégories de fiabilité et de disponibilité, ou se sont classés ex-æquo à la première ou la deuxième place pour toutes les mesures de disponibilité, de sécurité ou de facilité de gestion utilisées dans l'enquête.

La fiabilité est fluide et non statique. Aucun serveur, aucun composant - qu'il s'agisse des disques durs, de la mémoire ou de l'unité centrale, du système d'exploitation, des applications, des appareils ou des mécanismes de connectivité - ne sont à l'abri de problèmes ou de défaillances inhérents.

Les serveurs sont le socle sur lequel repose l'ensemble du l'infrastructure du réseau et de son écosystème étendu. Lorsque les serveurs tombent en panne, l'accès aux données est refusé. Toute activité cesse. La productivité se fige. Le chiffre d'affaires est affecté. Environ 88 % de toutes les entreprises exigent désormais une fiabilité minimale de 99,99 % pour les serveurs, les systèmes d'exploitation et leurs principales applications afin de garantir la productivité et un accès ininterrompu aux données. Une fiabilité et une disponibilité élevées protègent également les opérations quotidiennes de l'entreprise, les actifs de données et la propriété intellectuelle, les informations personnelles des employés, les processus métiers et les flux de revenus.

En 2021 et au-delà, la sécurité, les erreurs humaines et les utilisateurs finaux constituent les plus grandes menaces susceptibles de compromettre la fiabilité et la disponibilité des serveurs, des systèmes d'exploitation et des applications.

Personne ne sait combien de temps durera la pandémie mondiale de COVID-19. Et même lorsque la pandémie sera officiellement terminée, ses effets négatifs et son impact persisteront probablement pendant des années, notamment en ce qui concerne les menaces de sécurité et les violations de données.

Telle est la nouvelle norme : les cyberattaquants organisés sont appelés à durer. Ils continueront à utiliser la pandémie pour exploiter les vulnérabilités. Ils continueront à s'emparer de toutes les occasions d'exfiltrer les actifs de données des entreprises et des employés à des fins lucratives.

La fiabilité des serveurs, l'accès ininterrompu aux données et aux applications, la sécurité sont toujours des impératifs, mais plus particulièrement à l'ère du COVID-19, du télétravail et de l'apprentissage à distance. Chaque seconde et minute supplémentaires d'immobilisation du serveur et d'indisponibilité des applications ont un impact négatif sur les opérations, la productivité des employés et le chiffre d'affaires.

Une part importante des serveurs et des applications d'entreprise réside désormais dans des environnements virtualisés sur le cloud et en périphérie du réseau. Depuis le début de la pandémie il y a plus de 18 mois, de nombreuses entreprises ont fait passer leurs employés au télétravail ; les écoles et les universités ont également adopté l'enseignement à distance. Les entreprises, ainsi que les responsables de la sécurité et les administrateurs IT surchargés de travail se retrouvent face à une pression accrue pour garantir la disponibilité de tous les actifs de données.

La sécurité est extrêmement importante. Les vendeurs doivent continuer à renforcer la sécurité intégrée des serveurs, à fournir rapidement des correctifs lorsque des défauts sont constatés et à collaborer avec les clients pour les conseiller de façon prescriptive. Il incombe également aux entreprises d'assurer la fiabilité et la sécurité de toute l'infrastructure de serveur et de réseau, ainsi que celle des applications métier clés dans les centres de données et le cloud. Il est essentiel que les entreprises mettent en œuvre et fassent appliquer des politiques et des procédures de sécurité solides pour **tous les employés**, en particulier les télétravailleurs et les étudiants. La fiabilité et la sécurité sont des éléments fondamentaux de l'infrastructure du réseau. Ces deux éléments sont nécessaires pour assurer un fonctionnement quotidien ininterrompu, sécuriser l'accès aux données et protéger le flux de revenus.

L'Enquête internationale 2021 d'ITIC sur la sécurité des serveurs et de leurs systèmes d'exploitation montre clairement que **toutes** les entreprises, indépendamment de leur taille et de leur secteur vertical, doivent s'efforcer d'identifier et de déjouer de façon proactive et continue des cyberattaques de plus en plus variées, sophistiquées et ciblées.

Pour ce faire, elles doivent mettre en œuvre toutes les mesures de sécurité appropriées. Il est notamment impératif de promulguer et de faire appliquer des politiques et des procédures strictes en matière de sécurité des ordinateurs pour **tous les employés de la société**, depuis les cadres dirigeants jusqu'aux intérimaires et aux stagiaires. Les entreprises doivent allouer des budgets adéquats à l'achat de produits de sécurité et consacrer le temps nécessaire et les ressources internes et externes appropriées pour fournir aux utilisateurs finaux, aux responsables de la sécurité et aux administrateurs IT des outils et une formation.

Il n'existe pas de sécurité infaillible à 100 %. Toutefois, des défenses de sécurité multicouches, renforcées par des tests de vulnérabilité et une sensibilisation à la sécurité, peuvent réduire le nombre de violations de données et d'attaques par rançongiciels, et ainsi ramener le risque à un niveau acceptable.

Les systèmes stratégiques de Cisco, de HPE et de Huawei se sont également avérés extrêmement performants et n'ont pas connu de baisse de la fiabilité au cours des 18 derniers mois, depuis le début de la pandémie mondiale de COVID-19. Les serveurs de Cisco, de HPE et de Huawei ont atteint une fiabilité quasi-équivalente à celle d'IBM et de Lenovo grâce à la robustesse inhérente à leurs matériels de base.

Les serveurs UCS de Cisco ont conservé leurs gains en termes de fiabilité (voir la mise à jour semestrielle de l'enquête internationale 2021 d'ITIC sur la sécurité des serveurs et de leurs systèmes d'exploitation). Depuis 2019, la durée d'immobilisation signalée pour les serveurs Cisco UCS a diminué, passant d'un peu plus de quatre minutes (4,1) dans l'enquête précédente d'ITIC sur la fiabilité, à un peu plus de deux minutes (2,3) par serveur et par an, en raison de défauts du matériel. C'est un chiffre crucial. Une part importante des serveurs UCS de Cisco est déployée en périphérie du réseau, depuis longtemps considérée comme l'un des points les plus vulnérables de l'écosystème.

Aucun vendeur ne peut se reposer sur ses lauriers. La concurrence sur le marché mondial des serveurs est intense. C'est un marché acheteurs, et il le restera. Pour de nombreuses entreprises, en particulier les PME, le prix est le facteur qui détermine la décision d'achat. En revanche, un nombre important d'entreprises choisissent d'acheter du matériel plus robuste, doté d'une sécurité intégrée, d'une gestion avancée, de l'IA et d'une fonctionnalité d'analytique du big data.

Les données de l'enquête montrent que les grandes entreprises accordent une très grande importance au support technique après-ventes et au service clientèle. Les entreprises ont besoin que les fournisseurs agissent rapidement en cas de problèmes. Les vendeurs doivent fournir aux clients des recommandations réalistes et des conseils prescriptifs sur la configuration des systèmes et le cycle de vie des produits, afin d'obtenir et de préserver des performances et une disponibilité optimales.

Comme toujours, ITIC maintient que la distribution des correctifs et des mises à jour en temps opportun incombe aux fournisseurs. De même, ils doivent faire tout leur possible pour informer les clients de tout problème d'incompatibilité connu pouvant avoir un impact potentiel sur les performances. Les fournisseurs doivent également être honnêtes avec les clients et les avertir des problèmes ou des retards dans la livraison des pièces de rechange.

Recommandations

Aucune plateforme de serveur, aucun système d'exploitation de serveur et aucune d'application métier n'offre une sécurité à toute épreuve. Toutefois, IBM, Lenovo, Huawei, HPE et Cisco, qui comptent parmi les plateformes de serveurs les plus fiables, offrent également les plus hauts niveaux de sécurité intrinsèque. Ils permettent ainsi aux clients de réaliser des économies d'échelle très importantes et de protéger leurs actifs sensibles (propriété intellectuelle et données). La sécurité est un projet dont les responsabilités doivent être partagées à parts égales entre les parties prenantes. S'il incombe aux

fournisseurs de garantir une sécurité robuste, les entreprises doivent quant à elles préserver la fiabilité de leur serveur et de l'infrastructure réseau globale. ITIC a défini plusieurs recommandations importantes à l'attention des entreprises :

- **Faites un inventaire.** Vous devez savoir ce qui compose votre réseau. Il est donc nécessaire de cataloguer ***tous les*** serveurs, les applications métier cruciales, les dispositifs réseau (pare-feu, routeurs) dans tout l'écosystème du réseau, y compris le centre de données, les bureaux distants, les clouds publics, privés et hybrides, les appareils IoT et la périphérie du réseau.
- **Dimensionnez correctement vos serveurs**. Les serveurs doivent être suffisamment robustes pour s'adapter aux charges de travail en cours, ainsi qu'aux hausses prévues des charges de travail et aux applications de grande taille.
- **Remplacez, mettez à niveau et actualisez régulièrement vos serveurs.** Vous devez appliquer des correctifs, des mises à jour et des correctifs de sécurité à jour ***chaque fois que nécessaire*** pour préserver le bon état de santé du système et obtenir des performances système maximales.
- **Mettez à jour les logiciels.** Dans la mesure du possible, les systèmes d'exploitation des serveurs et les applications clés s'exécutant sur le serveur ne doivent jamais avoir plus de deux révisions de retard.
- **Mettez en œuvre des politiques et des procédures de sécurité solides.** Les entreprises toutes tailles confondues, dans tous les segments verticaux du marché, doivent impérativement élaborer des politiques et des procédures de sécurité à l'échelle de toute l'entreprise. Diffusez-les à tous les employés (copie papier, e-mail). Les politiques de sécurité appliquées aux ordinateurs doivent faire partie intégrante des directives générales de l'entreprise et comporter des dispositions et des sanctions spécifiques pour la première, la deuxième et la troisième infraction. Il est également conseillé aux entreprises de faire suivre à tous les employés une formation obligatoire à la sécurité informatique, tout comme c'est le cas pour la formation sur le harcèlement sexuel.
- **Surveillez de près les accords de niveau de service (SLA).** Apportez une attention particulière aux contrats d'accord sur les niveaux de service afin de vous assurer que vos fournisseurs de matériels, de logiciels et de solutions cloud sont conformes aux conditions des SLA, voire vont au-delà, afin de pouvoir respecter les niveaux de fiabilité convenus.
- **Réalisez un test des failles de sécurité.** Compte tenu de l'augmentation constante de tous les types de cyberattaques et de violations de données (attaques par rançongiciels, hameçonnages, arnaque au président, pour ne citer que quelques exemples), toutes les entreprises doivent effectuer des tests de vulnérabilité au moins une fois par an et selon les besoins. ITIC recommande aux entreprises de travailler avec des spécialistes indépendants.
- **Créez un plan de gouvernance et de résolution.** Prévoyez un plan de résolution et de gouvernance eu cas de réussite d'une cyberattaque. Définissez la hiérarchie des responsables en cas d'une violation de données ou d'une panne du réseau. Le plan de gouvernance et de résolution doit également affecter et définir des tâches spécifiques pour des groupes et des individus précis. Vérifiez que le plan contient également les coordonnées pertinentes de tous les fournisseurs et prestataires de services tiers.

- **Formez et certifiez les responsables de la sécurité et les administrateurs IT.** Veillez à ce que les responsables de la sécurité et les administrateurs IT reçoivent une formation adéquate et détiennent les certifications de sécurité nécessaires.
- **Formez les utilisateurs finaux.** Veillez à ce que les utilisateurs finaux, ainsi que les intérimaires et les personnels temporaires reçoivent une formation adéquate à la sécurité, englobant notamment les techniques d'escroqueries récentes par email et par hameçonnage, et les attaques par rançongiciels.

Méthodologie

L'Enquête internationale ITIC 2021 sur la sécurité des serveurs et de leurs systèmes d'exploitation a permis d'interroger des cadres supérieurs et des responsables IT dans plus de mille entreprises du monde entier, de janvier 2021 à la mi-juin 2021. Cette enquête indépendante sur le Web comprenait des questions à choix multiples et une question à développement. Pour garantir l'objectivité, ITIC n'a accepté aucune sponsorisation par un fournisseur. Aucun participant au sondage n'a reçu de rémunération. Les analystes d'ITIC ont également mené deux douzaines d'entretiens individuels en face à face avec des clients. Le but était d'obtenir des données anecdotiques précieuses. Il consistait également à comprendre plus en profondeur et en contexte l'impact et les implications des failles de sécurité et des violations de données sur la fiabilité des serveurs d'entreprise et de l'infrastructure du réseau. Les répondants étaient des cadres supérieurs, des responsables de la sécurité, des administrateurs IT et des utilisateurs finaux. ITIC a utilisé des mécanismes d'authentification et de suivi pour éviter les falsifications et empêcher les mêmes participants de répondre plusieurs fois.

Démographie de l'enquête

ITIC a interrogé 1 100 entreprises de toutes tailles dans 28 marchés verticaux. Des entreprises de toutes tailles étaient représentées. Les répondants ont été choisis dans des entreprises allant de petites et moyennes entreprises (PME) de moins de 50 employés jusqu'aux multinationales de plus de 100 000 employés.

Tous les secteurs du marché étaient également représentés : les PME de 1 à 100 employés représentaient 24 % des répondants. Les PME de 101 à 1 000 employés représentaient 28 % des participants. Les 43 % de répondants restants provenaient de grandes entreprises comptant de 1 001 à plus de 100 000 employés. Les répondants à l'enquête provenaient de 49 marchés verticaux différents. Environ 61 % des répondants étaient originaires d'Amérique du Nord, 39 % étaient des clients internationaux originaires de 22 pays d'Europe, d'Asie, d'Australie, de Nouvelle-Zélande, d'Amérique centrale et du Sud et d'Afrique.

Annexes

Cette section fournit des liens vers les diverses statistiques et enquêtes d'ITIC citées dans ce rapport.

Site Web d'ITIC et liens vers des données de l'enquête et les articles de blog :

https://itic-corp.com/blog/2019/11/ibm-lenovo-hpe-and-huawei-servers-maintain-top-reliability-rankings-cisco-makes-big-gains-ibm-lenovo-hardware-up-to-24x-more-reliable-28x-more-economical-vs-least-reliable-white-box-servers/

https://itic-corp.com/blog/2019/11/1678/

https://itic-corp.com/blog/2019/08/itic-poll-human-error-and-security-are-top-issues-negatively-impacting-reliability/

https://itic-corp.com/blog/2019/08/itic-2019-server-reliability-mid-year-update-ibm-z-ibm-power-lenovo-system-x-hpe-integrity-superdome-huawei-kunlun-deliver-highest-uptime/

http://itic-corp.com/blog/2017/07/ibm-z14-mainframe-advances-security-reliability-processing-power/

http://itic-corp.com/blog/2017/06/ibm-lenovo-servers-deliver-top-reliability-cisco-ucs-hpe-integrity-gain/