WHITE PAPER DA VERTIV

Como as Equipes de TI e de Cibersegurança podem trabalhar lado a lado para fortalecer a segurança do gerenciamento de servidores

O Ecossistema Vertiv™ Avocent® ADX traz clareza e controle para reduzir os riscos de segurança dos servidores

Se Adaptando às Mudanças

Os últimos dois anos colocaram sob extremo estresse as equipes de TI em corporações e em pequenas e médias empresas (PMEs) ao redor do mundo. Entretanto, elas se mobilizaram para viabilizar uma força de trabalho híbrida e desenvolver uma plataforma digital para dar suporte ao crescimento no longo prazo. Da mesma forma, as equipes de segurança combateram uma avalanche de ataques à medida que os cibercriminosos migraram sua atenção das redes para os endpoints, que são muito mais fáceis de penetrar.

Entretanto, manter a estabilidade dos negócios no meio de turbulências no mercado e constantes adversidades teve um preço. Tanto as equipes de TI como as de segurança estão passando por uma redução na visibilidade das condições e da performance da rede, ao mesmo tempo em que enfrentam uma disparada na demanda por serviços. Essas equipes são responsáveis por manter a performance e a segurança das redes distribuídas, enquanto redesenham os processos para um mundo de confiança zero. Como resultado, as equipes de redes de TI e de cibersegurança precisam colaborar mais intensamente para melhorar a segurança do gerenciamento de servidores ao longo das redes corporativas. A boa notícia é que 89% dos gerentes de rede dizem que estão fazendo exatamente isto. Ao redor de 37% das organizações agregaram completamente as equipes de gerenciamento de rede e de segurança, enquanto 26% mantêm equipes separadas, mas integraram ferramentas ou processos.[1]

Os servidores são a força motriz da indústria, proporcionando inestimável capacidade de processamento para a enxurrada dados que empresas, usuários e clientes produzem. Junto com outros dispositivos de rede, os servidores viabilizam os serviços digitais e possibilitam as experiências digitais que os clientes desejam. Portanto, manter o uptime (tempo de atividade) e a performance contínua é claramente crítico para TI e para segurança. Além disso, agressores que obtêm acesso aos servidores podem manipular, controlar e roubar ou congelar o acesso aos dados, paralisando a operação comercial de uma empresa e impactando seus clientes. O ataque de ransomware na Colonial Pipeline Co., que levou à escassez de gasolina na Costa Leste dos Estados Unidos, é um exemplo de como esses ataques podem ser incapacitantes e de longo alcance.[2]

Desafios e Oportunidades no Gerenciamento de Servidores pelas equipes de TI e de Segurança

Então, quais são os problemas que as equipes de TI e de segurança enfrentam quando tentam proteger os servidores localizados em data centers empresariais, instalações de colocation e sites de edge, entre outros locais?

Negócios digitais dão origem à dispersão digital: Atualmente, quase tudo é digital: processos de trabalho de colaboradores, interações com clientes, desenvolvimento de produtos e operações da cadeia de suprimentos. Uma pesquisa com profissionais de TI constatou que 47% espera mudanças permanentes, enquanto 13% diz que suas empresas se transformaram completamente por causa dos eventos recentes.[3]

As empresas aumentaram os investimentos em cloud e em edge para acompanhar, criando um alastramento dos dispositivos de TI. Servidores colocados em sites de edge remotos podem não ser gerenciados tão proativamente quanto os servidores em sites centrais, mais ainda apresentam importantes riscos de segurança. O que as equipes de TI e de segurança precisam fazer, mais do que nunca, é ganhar uma visualização centralizada na performance de sua rede. Elas também precisam explorar o acesso remoto seguro e o gerenciamento dentro e fora de banda para manter as redes funcionando e sem problemas de performance.

Quando mais tecnologia significa mais ferramentas: Como resultado do crescimento digital, as equipes de TI e de segurança estão agora gerenciando uma maior quantidade de servidores e dispositivos de rede vindos de uma variedade de fornecedores. Isso significa mais ferramentas, mais políticas e mais complexidade, a não ser que a equipe de TI consolide as tarefas de gerenciamento de rede em uma única ferramenta – e compartilhe dados holísticos com a equipe de segurança. Embora TI tenha dado importantes passos para reduzir a complexidade do gerenciamento, 64% das empresas ainda usam entre quatro e dez ferramentas para gerenciar suas redes[4]. Muitas querem consolidar ainda mais. A boa notícia é que TI pode gerenciar mais dispositivos do que nunca em uma plataforma centralizada. A equipe de segurança também se beneficia por ser capaz de integrar monitoramento físico, ambiental e de dispositivos em uma única visualização.

Centralizando o Gerenciamento dos Dispositivos de TI com Uma Plataforma

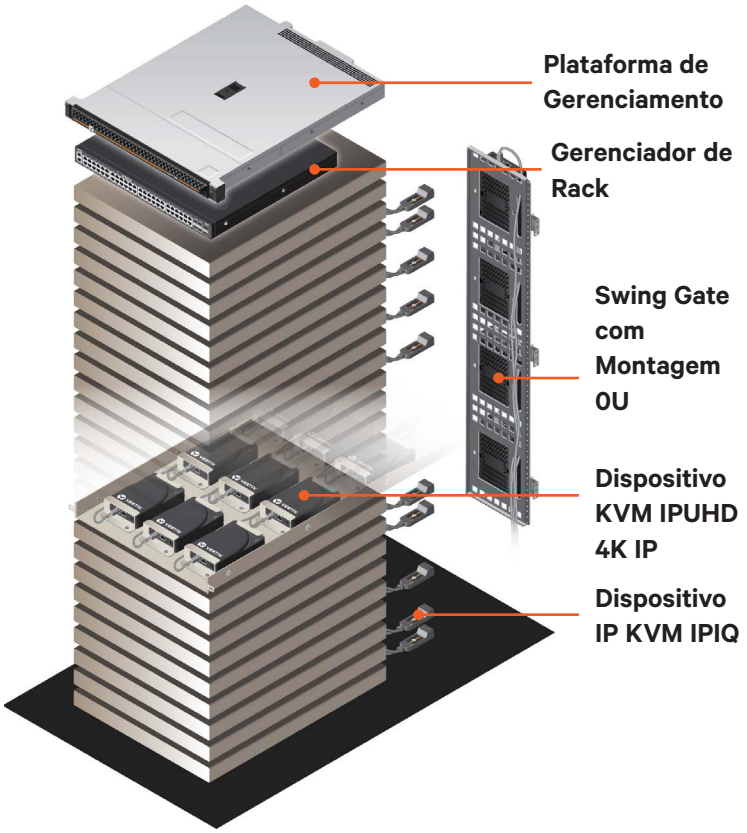
O Ecossistema Vertiv™ Avocent® ADX ajuda às equipes de TI e de cibersegurança centralizar o monitoramento e o gerenciamento, melhorando a segurança dos servidores e de outros dispositivos de rede.

Servidores - Servidores de produção, de desenvolvimento e de testes; servidores não essenciais.

Outros dispositivos de TI - Desktops administrativos, dispositivos de armazenamento, equipamentos de rede, unidades de distribuição de energia para racks (rPDUs), fontes remotas de alimentação de energia ininterrupta (UPSs), sensores remotos, travas de portas de racks, câmeras e outros.

A segurança não tem visibilidade às políticas:
As equipes de TI e de segurança querem gerenciar as condições de todos os servidores, onde quer que eles estejam localizados. Entretanto, porque essas equipes estão usando diversos fornecedores e diversas ferramentas, os dispositivos provavelmente têm políticas de segurança inconsistentes e algumas podem não proporcionar visibilidade e controle granular. Isso é destinado ao fracasso em um mundo com riscos e ameaças constantes. A segurança irá querer fazer uma parceria com TI na definição e no gerenciamento granular dos privilégios de acesso com base nos cargos dos usuários e nas funções a serem por eles desempenhadas. Exemplos incluem controlar quem pode fazer updates de firmwares, anexar mídia virtual à dispositivos e reinicializar servidores. Ao fazer isso, as equipes podem reduzir os privilégios de acesso excessivos que podem ser explorados por cibercriminosos para iniciar ataques devastadores.

IT precisa simplificar a gestão de firmwares:
Automatizar os upgrades de firmwares está tendo uma maior importância à medida que cibercriminosos visam o kernel, a memória e outras vulnerabilidades em servidores e outros dispositivos. Por exemplo, invasores podem usar um malware como o Trickbot para escanear dispositivos buscando vulnerabilidades e, então, ler, escrever ou apagar o firmware UEFI BIOS[5]. Outra ameaça, o novo rootkit iLOBleed, mira em Servidores Empresariais HP, manipulando o firmware e limpando dados dos sistemas.[6] Além disso, equipes de segurança reportam que ainda ocupam 41% do seu tempo com patches de firmware manuais que poderiam ser automatizados[7]. Automatizar esses upgrades elimina os riscos criados por firmware desatualizado e devolve às equipes de TI e de segurança tempo para o trabalho estratégico.



"Mais de 80% das empresas passaram por pelo menos um ataque a firmware nos últimos dois anos, constata estudo da Microsoft. Entretanto, apenas 29% dos orçamentos de segurança dessas empresas estão focados na proteção de firmwares."[8]

Proporcionando maior funcionalidade: TI e segurança podem usar plataformas separadas de monitoramento de rede e automação. Entretanto, por que não agregar esses recursos? Tanto a área de TI quanto a de segurança se beneficiariam ao obter uma visão holística da performance da rede, compartilhando e agindo a partir de dados em tempo real. Isso inclui a capacidade de em conjunto determinar os privilégios de acesso, rever anomalias, planejas respostas a incidentes e implementar as melhores práticas, como a automatização.

Ecossistema Vertiv™ Avocent® ADX – Uma Plataforma Centralizada que TI e Segurança Podem Usar para Colaborar

Então, os desafios de gerenciamento e segurança dos servidores estão aumentando. Mas, a boa notícia é que TI e Segurança podem trabalhar juntos, cooperativamente, para lidar com esses problemas e fortalecer a segurança, contribuído para as metas de suas empresas de criar arquiteturas de confiança zero. E podem fazer isto implementando e compartilhando um roadmap simples de quatro passos.

O Ecossistema Vertiv™ Avocent® ADX proporciona às áreas de TI e de Segurança a plataforma centralizada que elas precisam para melhorar a segurança e o gerenciamento dos servidores. Ele oferece a visualização única, as ferramentas de gerenciamento e os recursos de automatização que ambas as equipes precisam para trazer clareza e controle à rede e à segurança. O Ecossistema Avocent ADX inclui:

- Uma plataforma de gerenciamento para acesso remoto seguro e automatização.
- Um Gerenciador de rack que se conecta fisicamente a módulos de interface ou diretamente aos processadores de serviços, rack PDUs ou equipamentos de rede.
- Módulos de interface que se conectam à dispositivos de agregação e ao alvo final.

O Ecossistema Avocent ADX, baseado em uma arquitetura digital comum com uma plataforma aberta e APIs, permite que até 100 usuários simultâneos monitorem e gerenciem dispositivos. A segurança multinível garante que usuários autorizados apenas tenham acesso aos dispositivos e privilégios de que precisam para realizar o seu trabalho.

Esses usuários têm opções sobre como acessam e gerenciam dispositivos. Administradores de TI e de Segurança podem usar consoles seriais e dispositivos KVM 4K Vertiv™ Avocent® ADX IPIQ para gerenciar dispositivos empresariais fisicamente conectados ao gerenciados de racks. Como alternativa, eles podem usar os dispositivos KVM IP Vertiv™ Avocent® ADX IPIQ como uma solução rápida, de baixo custo e zero U para gerenciar dispositivos sem a necessidade do gerenciador de racks.

Vertiv™ Avocent® Core Insight –Padronize o gerenciamento de TI com firmware de código aberto. As equipes de TI querem padronizar o gerenciamento de dispositivos, eliminando os furos na segurança e aumentando a qualidade do cógido e o speed to market. O Vertiv™ Avoncent® Core Insight (ACI) proporciona uma implementação pronta para ser comercializada do projeto OpenBMC para controladores de gerenciamento de placas de sistema (BMCs). Engenheiros podem usar o firmware ACI para construir sistemas de gerenciamento embutidos seguros, escaláveis e com tecnologia de ponta para qualquer dispositivo.

Desenvolvedores têm opções flexíveis e podem escolher entre:

- Firmware de código aberto pronto a ser desenvolvido.
- Módulos de aplicação ACI avançados que podem ser adicionados à stacks existentes.
- Um serviço por assinatura que proporciona um pacote de ACI pronto para empresas, incluindo acesso ao código fonte integral, ferramentas e suporte premium.

O Vertiv ACI proporciona segurança premium para o tempo de execução, eliminando todo um vetor de vulnerabilidades baseadas na memória.

Implemente Este Roadmap para Fortalecer a Segurança dos Servidores Hoje

Agora que as equipes de TI e de Segurança podem ver e compartilhar dados e executar processos juntas, como elas devem proceder? Aqui está um roadmap simples para melhorar a segurança dos servidores, começando agora.

- **Conecte os dispositivos fisicamente para maior segurança:**
  TI pode conectar os dispositivos ao Gerenciador de Racks Avocent ADX – e escondê-los da visualização e acesso à rede, colocando-os em uma rede privada. A rede privada é então acessível apenas através de uma interface de gerenciamento de racks para indivíduos autorizados, reduzindo o risco de erro humano ou sabotagem interna.
- **Use protocolos seguros para se comunicar com os dispositivos:**
  As equipes de TI e de Segurança nem sempre podem controlar a segurança dos dispositivos. Elas podem precisar usar dispositivos legados ou de novos fornecedores que não tenham os protocolos e as cifras mais modernos. Entretanto, essas equipes podem colocar esses dispositivos menos seguros através do Gerenciador de Racks Avocent ADX para maior proteção. Ao fazê-lo, as equipes de TI e de segurança podem auferir mais valor dos dispositivos mais antigos ou novas inovações em teste (trial) sem comprometer a segurança da rede ou do site.

- **Mantenha atualizado o firmware nos processadores de serviço:** Administradores do sistema podem usar a Plataforma de Gerenciamento Avocent ADX para automatizar os upgrades de firmware dos servidores usando APIs RESTful e kits de desenvolvimento de software (SDKs), trazendo consistência e padronização para essa tarefa tão necessária. Por fim, a Plataforma de Gerenciamento Avocent ADX simplifica os upgrades, evitando o downtime de dispositivos e reduzindo os riscos de segurança.

- **Fortaleça a segurança dos dispositivos com controle granular:**
  Com a Plataforma de Gerenciamento Avocent ADX, é fácil alocar, gerenciar e controlar privilégios, evitando os riscos que privilégios de administrador em excesso criam. Quem faz a instalação dos servidores pode ter um conjunto de privilégios, como instalar imagens e softwares do sistema operacional e reinicializar servidores. A equipe de TI que identifica/resolve problemas nos servidores pode ser autorizada a iniciar sessões de KVM ou seriais e completar importantes ações, como instalar firmware.

Além disso, TI pode padronizar essas ações entre os diferentes tipos de dispositivos. Por exemplo, administradores do sistema podem ser autorizados a reinicializar diversos tipos de dispositivos. A plataforma também oferece recursos de auditoria, permitindo que as equipes de TI e de Segurança revisem esses privilégios continuamente para ter certeza de que não há indivíduos realizando ações não autorizadas.

Conclusão

Melhorar a segurança do gerenciamento de servidores é uma das principais prioridades para corporações e PMEs atualmente. Os servidores nutrem os processos críticos que fazem os negócios digitais funcionarem. Entretanto, eles estão progressivamente em risco, devido à dispersão das redes, do excesso de privilégios administrativos, firmware ultrapassado, vulnerabilidades de memória e outras questões.

As equipes de TI e de segurança podem proativamente identificar e eliminar furos na segurança dos servidores trabalhando juntas, usando uma plataforma centralizada de gerenciamento e monitoramento e processos automatizados. A Plataforma de Gerenciamento Vertiv Avocent ADX proporciona esses recursos essenciais, permitindo que TI e Segurança trabalhem lado a lado para proteger esses dispositivos de missão crítica tanto agora como no futuro.

[1] Shamus McGillicuddy, The Convergence of Network and Security Operations, EMA White Paper, Abril 2021, página 1, https://www.enterprisemanagement.com/research/asset.php/4037/The-Convergence-of-Network-and-Security-Operations

[2] "Hackers Breached Colonial Pipeline Using Compromised Password," artigo, Bloomberg, Junho 4, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[3] 2022 Tech Trends, Research Report, Info-Tech Research Group, slide 3, https://www.infotech.com/research/ss/2022-tech-trends

[4] EMA: Network Management Megatrends, 2020, Kentik, página 1, https://www.kentik.com/resources/ema-network-management-megatrends-2020-report/

[5] "Assessing Enterprise Firmware Security Risk in 2021," artigo, Janeiro 14, 2021, Eclypsium, https://eclypsium.com/2021/01/14/assessing-enterprise-firmware-security-risk-in-2021/

[6] Ravie Lakshmanan, "New iLOBleed Rootkit Targeting HP Enterprise Servers with Data Wiping Attacks," artigo, The Hacker News, Dezembro 30, 2021, https://thehackernews.com/2021/12/new-ilobleed-rootkit-targeting-hp.html

[7] New Security Signals, ibid.

[8] "New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats," artigo, Microsoft, Março 30, 2021,

https://www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/

Vertiv.com | Sede da Vertiv, 1050 Dearborn Drive, Columbus, OH, 43085, Estados Unidos da América

SL-70977PT (R10/22)