EBOOK DA VERTIV

4 Maneiras de Melhorar a Segurança do Data Center Este Ano

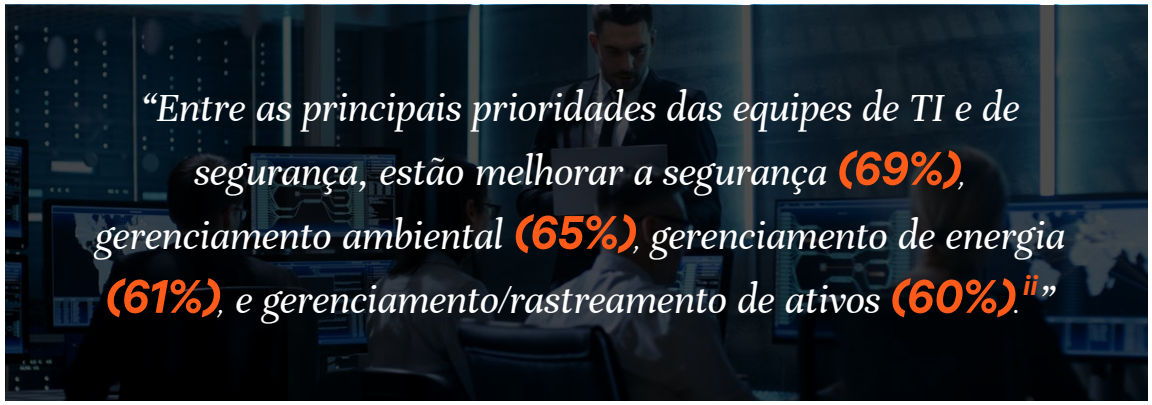
Reduza os Riscos Automatizando Processos e Usando Soluções Seguras da Vertiv

VERTIV

EBOOK DA VERTIV

4 Maneiras de Melhorar a Segurança do Data Center Este Ano

Proprietários e operadores de data centers estão trazendo capacidade nova para atender às vorazes demandas empresariais e possibilitar a transformação digital do negócio. Somente nos Estados Unidos, há 526 megawatts em construção.[i] Como resultado, as equipes de data center e de TI empresariais, de provedores de colocation e de hyperscalers estão gerenciando um footprint maior do que nunca. Muito desse trabalho está sendo feito remotamente, criando novas pressões e desafios a serem ultrapassados.



Como resultado, as equipes de TI e de data centers estão rapidamente evoluindo suas abordagens para o gerenciamento de dispositivos. Elas gostariam de simplificar processos através da adoção de melhores plataformas e ferramentas existentes que:

- Habilitem o acesso remoto seguro para os dispositivos
- Melhorem a visibilidade e o controle da rede
- Centralizem e padronizem o gerenciamento de TI
- Protejam os dados através do uso de ferramentas seguras para o manuseio da informação

A hora de começar é agora. À medida que as estratégias de digitalização das empresas se aceleram, as infraestruturas se tornam mais complexas e introduzem brechas que outros podem explorar. As equipes de data center e de TI podem usar processos automatizados e centralizados para trazer novos níveis de consistência e controle para as práticas de gestão. Ao fazê-lo, elas podem entregar a alta disponibilidade e a resiliência que o seu negócio exige.

VERTIV.

EBOOK DA VERTIV

4 Maneiras de Melhorar a Segurança do Data Center Este Ano

Habilitar o acesso remoto seguro para os dispositivos

Equipes de data center e de TI precisam visualizar, acessar, controlar e gerenciar uma grande variedade de servidores, equipamentos de rede e dispositivos seriais que fazem o seu negócio funcionar.

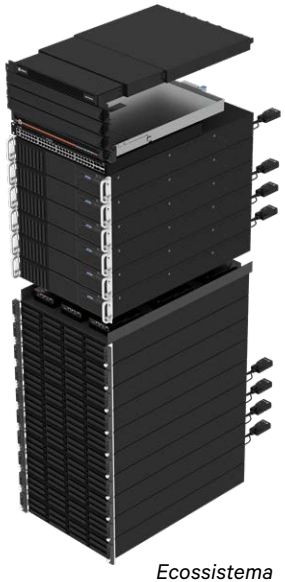
Embora essas equipes trabalhassem antes no site, muitos colaboradores estão agora trabalhando remotamente devido à pandemia – e provavelmente o farão indefinidamente. Esses usuários são os principais alvos de ataques, uma vez que têm privilégios altos que estranhos maliciosos podem usar para ter acesso às redes das organizações. Credenciais comprometidas foram usadas em 20% de todos os ataques em 2021.[iii] Então, não é nenhuma surpresa que as organizações estejam adotando uma abordagem de 'primeiro a identidade' para a segurança.[iv]

"Credenciais utilizadas indevidamente são agora a principal técnica usada nas violações... A infraestrutura de identidades deve ser configurada, mantida e monitorada adequadamente e com muita importância."

- Fonte: Gartner [v]

As equipes podem usar as soluções da Vertiv para:

- **Proporcionar acesso remoto seguro aos dispositivos com base em função e grupo:** Administradores de TI podem usar o Ecossistema Vertiv™ Avocent® ADX para autorizar usuários a realizar as principais tarefas alinhadas às suas funções, tal como monitoramento e gerenciamento de tipos específicos de dispositivos. Administradores de TI podem dar privilégios para diferentes equipes, como TI, segurança, aplicações e testes, que precisem acessar servidores e outros dispositivos de acesso à rede. O Ecossistema Avocent ADX se integra perfeitamente ao Console Serial Vertiv™ Avocent® ACS 8000 para proporcionar acesso seguro similar aos dispositivos seriais, de forma que as equipes possam gerenciar dispositivos, reunir dados e automatizar configurações.
- **Centralizar a autenticação de terceiros:** As equipes de TI podem designar privilégios para terceiros dinamicamente.
- **Garantir consistência na autorização de acesso:** A maioria das organizações usam o conceito de conceder privilégios mínimos enquanto permitem que usuários realizem funções autorizadas. Ao fazer isso, elas podem evitar os problemas que ocorrem quando os direitos de acesso não são proativamente gerenciados, como quando indivíduos perambulam pelas redes e realizam ações não autorizadas em dispositivos.



Ecossistema Avocent® ADX

Avocent® ACS 8000

VERTIV

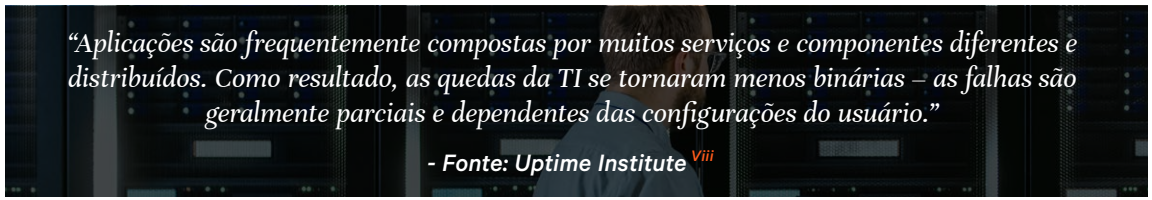
EBOOK DA VERTIV

4 Maneiras de Melhorar a Segurança do Data Center Este Ano

Melhorar a visibilidade e o controle da rede

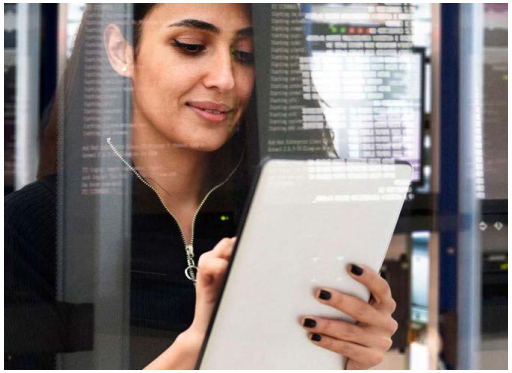
Por data centers empresariais e sites de edge, os milhares de serviços de nuvem dos hyperscales e as infraestruturas de provedores de colocation, o funcionamento de redes está ocorrendo em todos os lugares. Até 2025, 85% das estratégias de infraestrutura integrarão as opções de entrega locais (on-premises), colocation, cloud e edge comparado a 20% em 2020.[vi] E isso ocorrerá porque as equipes de TI estão distribuindo estrategicamente as cargas de trabalho para ter os melhores resultados.[vii]

As equipes de data center e de TI precisam melhorar a visibilidade e o controle, onde quer que trabalhem e seja o que for que gerenciem. Isso é ainda mais importante para fornecedores terceirizados, já que o erro humano ou as brechas de segurança exploradas podem causar impactos críticos aos negócios e prejudicar dezenas de milhares ou milhões de clientes.



As equipes podem usar as soluções da Vertiv para:

- **Usar um único ponto de autenticação:** As equipes podem usar o Ecossistema Avocent® ADX para ter um único ponto de acesso ao servidor e a outros dispositivos de TI, enquanto o Avocent® ACS 8000 também oferece acesso agregado a dispositivos seriais. Ao centralizar a visibilidade e o acesso, os profissionais de data center e de TI podem trabalhar de forma mais eficiente, realizando tarefas de gerenciamento tanto dentro como fora de banda.
- **Controlar o que usuários podem enxergar:** O Ecossistema Avocent ADX possibilita que as equipes controlem os dispositivos que usuários individuais podem enxergar. Isso é especialmente crítico para provedores de colocation e de hyperscale, os quais podem querer segmentar o acesso para que os clientes apenas enxerguem seus próprios dispositivos. Da mesma forma, superusuários podem controlar o que equipes em outras unidades de negócios, terceiros e outras partes autorizadas podem enxergar.



- **Auditar o comportamento de usuários:** Diversas empresas precisam fornecer relatórios sobre acesso de usuários e ações em dispositivos para fins de auditorias e compliance regulatório. O Ecossistema Avocent ADX possibilita aos administradores monitorar quem faz o que, quando e como. Eles podem monitorar cada tecla que os usuários apertam quando estiverem acessando os dispositivos via Avocent ACS 8000. Também é fácil estabelecer alarmes em cadeia para ter avisos imediatos sobre ações muito importantes. Por último, a equipe de TI pode proporcionar acesso on-line e off-line ao log de dados com timestamps do Avocent ACS 8000 para fins de análise e relatórios.

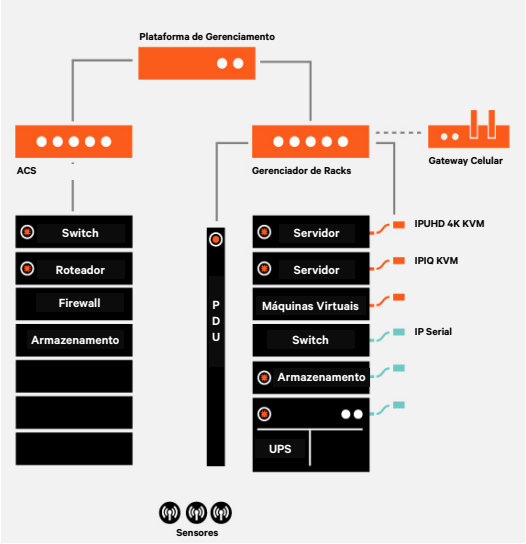
VERTIV

EBOOK DA VERTIV

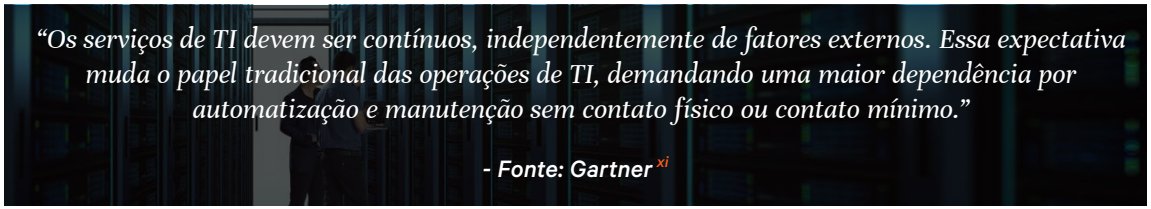
4 Maneiras de Melhorar a Segurança do Data Center Este Ano

Centralizar e padronizar o gerenciamento de TI

A proliferação de dispositivos de rede criou maior complexidade para as equipes de data center e de TI. A maioria dos fornecedores oferecem suas próprias ferramentas para gerenciar seus dispositivos. Como resultado, 64% das empresas usam agora entre 4 e 10 ferramentas para gerenciar redes.[ix] Usar muitas ferramentas pode introduzir brechas de segurança nos processos ou aumentar o risco de erro humano, ambos a partir de ações feitas ou deixadas de ser feitas.



As equipes de data center e de TI querem centralizar e automatizar o gerenciamento dos servidores, dos equipamentos de rede e dos dispositivos seriais.



"Os serviços de TI devem ser contínuos, independentemente de fatores externos. Essa expectativa muda o papel tradicional das operações de TI, demandando uma maior dependência por automatização e manutenção sem contato físico ou contato mínimo."

- Fonte: Gartner [xi]

Equipes que implementam soluções da Vertiv podem:

- **Agregar dispositivos para aumentar a segurança:** Conectar cada dispositivo à internet aumenta drasticamente a superfície de ataque, aumentando os riscos. As equipes podem usar o Gerenciador de Racks Vertiv™ Avocent® ADX para conectar até 48 dispositivos. Elas podem então escondê-los da visualização da rede e do acesso externo ao colocá-los em uma rede privada. Apenas usuários autorizados podem então acessar os dispositivos e executar as ações que sejam autorizados a fazer.
- **Diagnosticar e tratar rapidamente qualquer problema:** Espera-se que as equipes de TI entreguem uma disponibilidade de aplicações e funcionamento contínuo (uptime) para possibilitar os processos digitais do negócio. Como resultando, a pressão é grande para que identifiquem e tratem dos problemas proativamente, bem como para identificar e resolver as quedas da rede. As equipes podem utilizar o Avocent® ACS 8000 para realizar processos de gerenciamento dentro e fora de banda, usando conectividade por celular, Ethernet ou de modem analógico para ter acesso aos dispositivos.
- **Automatizar os upgrades de firmware:** Firmware desatualizado é um dos principais alvos de cibercriminosos, os quais monitoram ativamente as redes procurando por esses problemas. Mesmo assim, apesar dessa realidade, as equipes de segurança dizem que gastam 41% de seu tempo com patches manuais de firmware que poderiam ser atualizados. TI e Segurança podem usar a Plataforma de Gerenciamento Avocent ADX para automatizar os upgrades de firmware dos servidores, fechando essa brecha de segurança para sempre.

VERTIV

EBOOK DA VERTIV

4 Maneiras de Melhorar a Segurança do Data Center Este Ano

Vertiv.Com

Proteger os dados usando ferramentas seguras para manuseio da informação

Os dados são a força vital das indústrias, alimentando as principais operações e impulsionando o crescimento dos negócios. As empresas produzem e gerenciam uma enormidade de dados confidenciais e sensíveis que são normalmente rigidamente governados por regulamentações setoriais.

Empresas biofarmacêuticas querem proteger dados e pesquisas de remédios; vazamentos podem prejudicar sua capacidade de obter e manter aprovações e registros para seus remédios e perder terreno para seus concorrentes. As equipes de serviços financeiros trabalham com dados de clientes e de ações que são protegidos por regulamentações como a GDPR, GLBA, NYDFS e PCI-DSS. Funcionários do governo precisam usar dados sensíveis, confidenciais e não confidenciais que trafegam por redes como JWICS, SIPRNet e NIPRNet. Por último, no setor de saúde, médicos acessam prontuários eletrônicos que contêm informações que permitem identificação pessoal (PII) e informações pessoais sobre a saúde, protegidos pelo HIPAA.

Qualquer que seja o setor, os KVMs Seguros para Desktops Vertiv™ Cybex™ SC podem ajudar aos colaboradores acessar dados sensíveis, dentro dos limites rígidos do controle de segurança:

- **Navegar facilmente entre fontes de informação:** O Cursor Navigation Switching possibilita aos colaboradores visualizar com segurança informações com diversos níveis de confidencialidade na mesma tela. Isso é particularmente bom para operações sensíveis governamentais, como gerenciar infraestrutura crítica ou realizar trabalhos militares ou de inteligência.
- **Evitar a contaminação cruzada de informações:** Informações ficam contaminadas e potencialmente vazadas quando usuários realizam ações não aprovadas. As organizações podem usar os KVMs Seguros para Desktop Cybex™ SC para evitar copiar, recortar ou colar informações entre os níveis de confidencialidade. Enquanto órgãos governamentais precisam desse tipo de proteção rotineiramente, outros setores podem usá-la para tarefas como rever dados confidenciais sobre desenvolvimento de produtos ou informações financeiras de empresas alvo de Fusões e Aquisições.

- **Evitar a manipulação de dispositivos:** Os KVMs Seguros para Desktop Cybex SC oferecem as seguintes proteções para evitar a manipulação. A detecção ativa de manipulação faz com o que o KVM se torne inoperável se os selos forem violados. Além disso, firmware travado evita que os usuários façam ações não autorizadas nas operações KVM.

VERTIV.

EBOOK DA VERTIV

4 Maneiras de Melhorar a Segurança do Data Center Este Ano

Conclusão

A complexidade das redes está crescendo, pressionando as equipes de data center e de TI para simplificar os processos atuais e melhorar a segurança. Esses profissionais podem ajudar a alcançar essas metas ao ativar o acesso remoto seguro para os dispositivos, melhorando a disponibilidade e o controle da rede, centralizando e padronizando o gerenciamento de TI e protegendo os dados ao usar ferramentas seguras de manuseio de informações.

Deixe que este seja o ano em que você se beneficia de maior segurança e maior controle, traga mais consistência aos processos de gerenciamento e simplifique a administração diária com a automatização.

Melhore a segurança por todos os lados com a Vertiv.

Saiba mais sobre:

Ecossistema Vertiv™ Avocent® ADX

Servidor de Console Serial Avocent® ACS 8000

KVM Seguro para Desktop Vertiv™ Cybex™ SC

Recursos

Quer saber mais sobre como melhorar a segurança do data center? Confira estes recursos da Vertiv:

- Possibilitando que os colaboradores manuseiem informações sensíveis e confidenciais de forma segura
- Estabelecer Controles Granulares para Dispositivos de Redes de TI É Agora Mais Fácil do que Nunca
- Como as equipes de TI e de Cibersegurança podem trabalhar lado a lado para fortalecer a segurança do gerenciamento de servidores

[i] "Data Centers," capítulo 8, U.S. Real Estate Market Outlet 2022, relatório CBRE, sem data https://www.cbre.com/insights/books/us-real-estate-market-outlook-2022/data-centers#.
[ii] Ibid.
[iii] "How much does a data breach cost?" webpage, IBM, https://www.ibm.com/security/data-breach
[iv] Kasey Panetta, "The Top 8 Security and Risk Trends We're Watching," artgo, Gartner, Novembro 21, 2021, https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021
[v] Ibid.
[vi] Add reference
[vii] David Cappuccio, Henrique Cecci, Your Data Center May Not Be Dead, but It's Morphing, Gartner, relatório, Setembro 17, 2020, https://www.equinix.com/resources/analyst-reports/data-center-not-dead-morphing-changing?
[viii] Rich Miller, "The Eight Trends That Will Shape the Data Center in 2022," Data Center Frontier, Janeiro 10, 2022, https://datacenterfrontier.com/the-eight-trends-that-will-shape-the-data-center-industry-in-2022/
[ix] EMA: Network Management Megatrends, 2020, Kentik, Página 4, https://www.kentik.com/resources/ema-network-management-megatrends-2020-report/
[x] "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/
[xi] "Gartner Top 6 Trends," ibid.
[xii] "How much does a data breach cost?" IBM, ibid.

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

SL-70939 (R10/22)