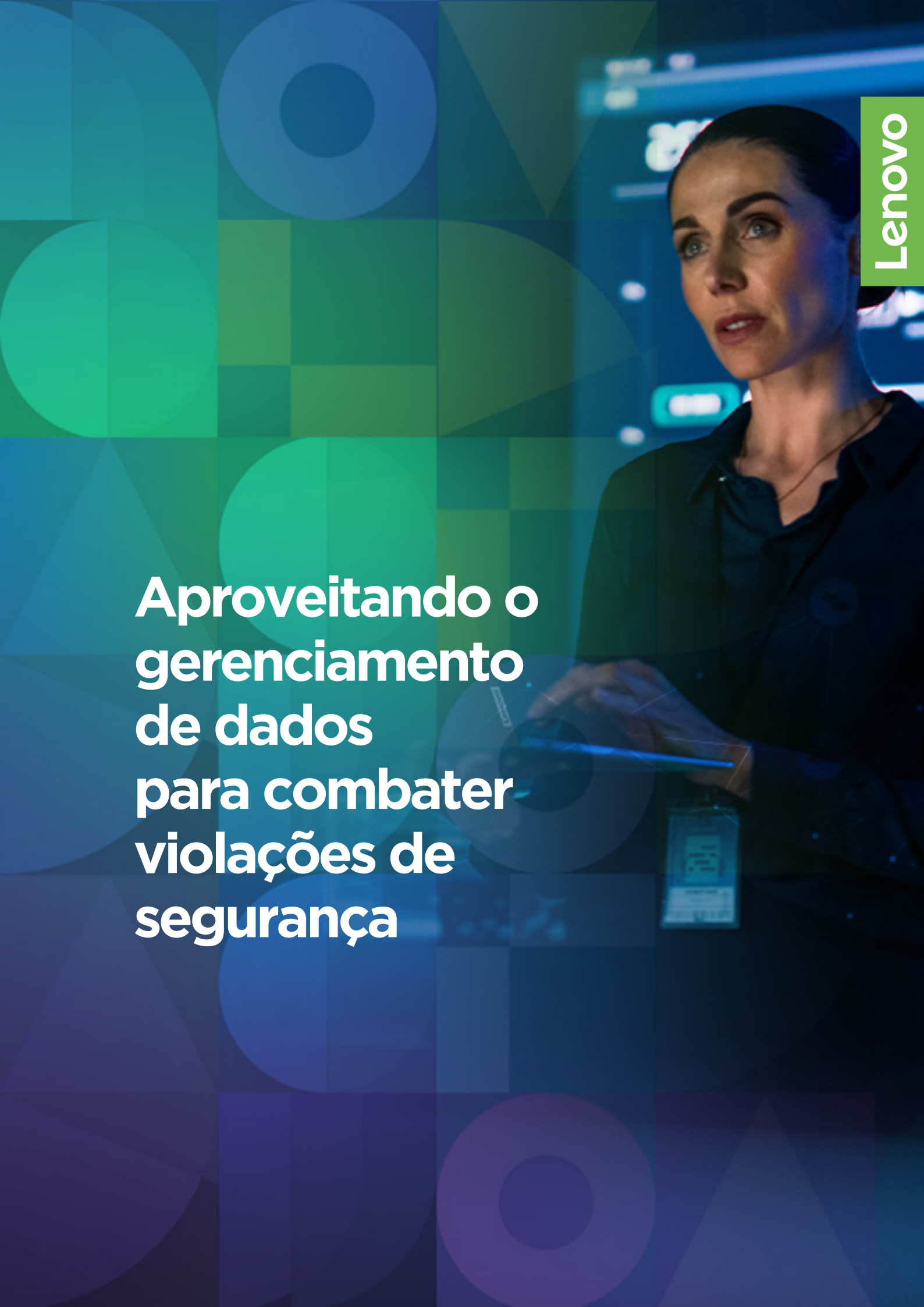
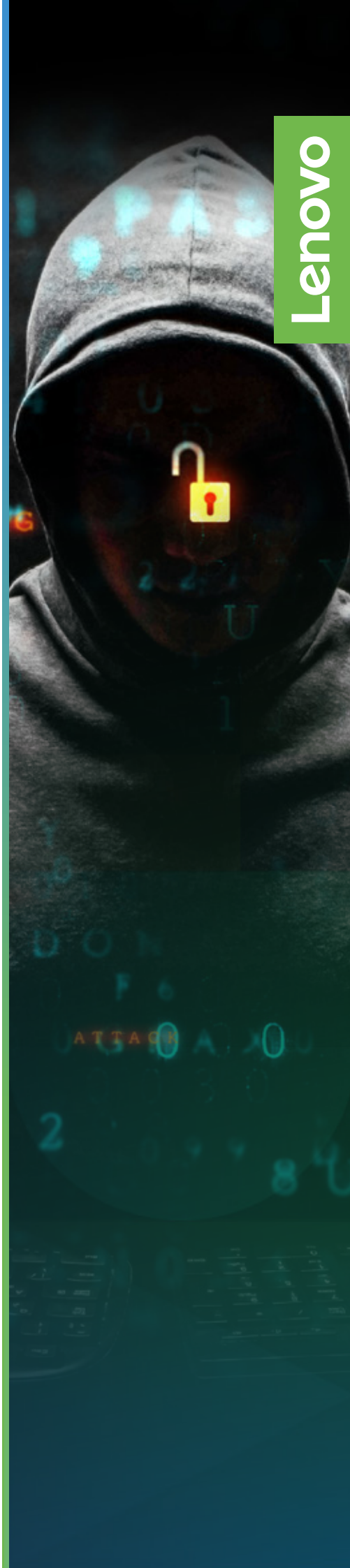


Aproveitando o gerenciamento de dados para combater violações de segurança

As ameaças de segurança cibernética estão aumentando diariamente, criando problemas operacionais, financeiros, regulatórios e de marca incalculáveis para as organizações. Ransomware, malware, roubo de identidade e outros desafios de segurança devem ser identificados, prevenidos e remediados antes que danos extensos possam ser causados e dados essenciais sejam comprometidos.

Este artigo analisa por que e como uma estrutura defensiva baseada em gerenciamento de dados deve ser construída para bloquear ameaças cibernéticas e proteger as empresas contra a perda de dados.

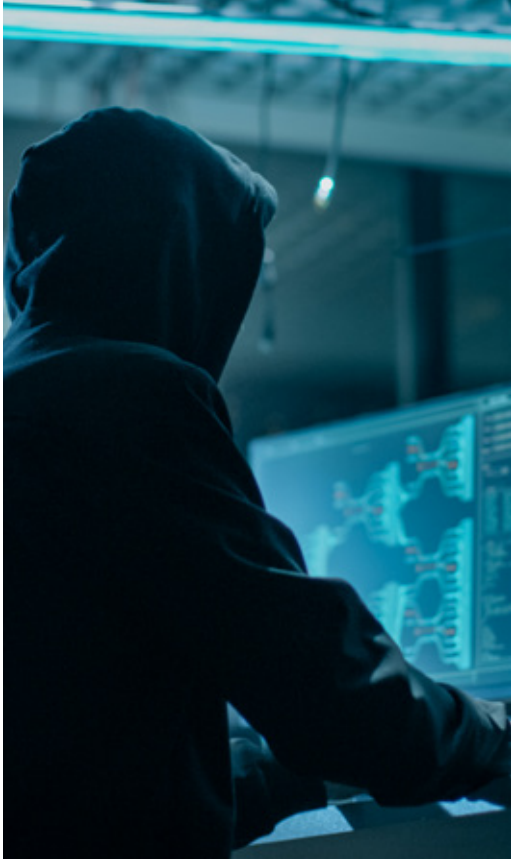


A cada minuto de cada hora de cada dia, as organizações estão sob ataques cibernéticos. Na verdade, os hackers atacam em algum lugar do mundo a cada 39 segundos. [1]A ameaça de ataques cibernéticos, como ransomware, ataques de dia zero e malware móvel, está crescendo a taxas alarmantes conforme os criminosos cibernéticos se tornam mais persistentes e engenhosos, utilizando os recursos coletivos de outros invasores e algoritmos de aprendizado de máquina.

Em 2020, o custo médio de uma violação de dados corporativos excederá US$ 150 milhões. [2]Isso sem falar dos impactos econômicos, operacionais e de reputação igualmente importantes das violações de compliance causadas por aspectos como informações de identificação pessoal comprometidas.

A proteção de dados, identidades e outros ativos digitais exige uma combinação de técnicas de gerenciamento de dados inovadoras, inteligentes e automatizadas. As organizações também devem insistir em armazenamento e infraestrutura de computação resilientes e "seguros de fábrica". Este documento analisa o que as organizações podem e devem fazer para mitigar as ameaças à segurança cibernética e por que o gerenciamento de dados é um elemento fundamental para enfrentar o malware, ameaças persistentes avançadas, ransomware e outros formatos de ataque. Ele também oferece algumas sugestões concretas de parceria com um parceiro de tecnologia confiável e comprovado para soluções de gerenciamento de dados.

1 "15 Alarming Cyber Security Facts and Stats," Cybint Solutions, 23 de setembro de 2019.
2 "Business Losses to Cybercrime Data Breaches to Exceed $5 Trillion by 2024," Juniper Research, 27 de agosto de 2019.



O que as empresas devem fazer hoje

As empresas tornaram-se mais engenhosas na sua luta contra ameaças de segurança, que comprometem centenas de bilhões de dólares anualmente em tudo, de assinaturas de monitoramento de ameaças e serviços de correção de violação de dados a firewalls de última geração e servidores resistentes a malware. No entanto, os ataques continuam se proliferando, aumentando a pressão sobre as organizações para reforçar seus esforços de proteção de dados do núcleo, passando pela borda, até a nuvem.

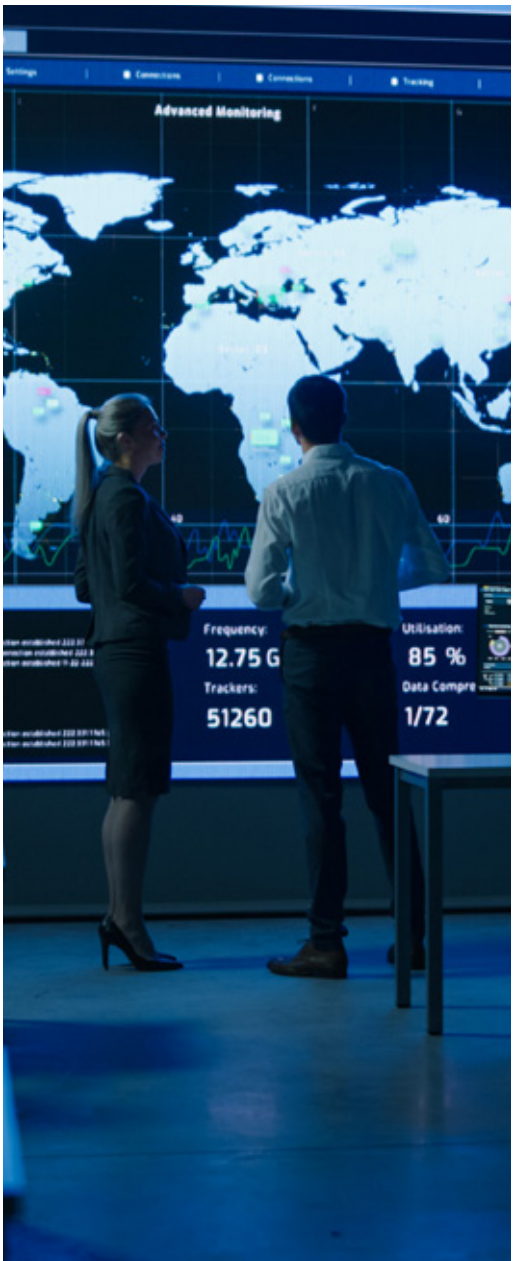
Quando "fazer o que sempre foi feito" não funciona mais, é hora de utilizar novas ideias, novas estratégias e novas ferramentas.

No centro de uma estrutura de segurança cibernética e proteção de dados sólida, eficiente e flexível está o gerenciamento de dados. Há muitos elementos de uma arquitetura de gerenciamento de dados que contribuem para uma postura de segurança cibernética inteligente, automatizada e responsiva. Por exemplo, o backup e arquivamento são essenciais para a proteção de dados e restauração de dados rápida e confiável, enquanto instantâneos (snapshots), deduplicação e compressão melhoram a otimização do armazenamento. O gerenciamento de dados também é fundamental para a continuidade dos negócios, visibilidade de dados e auditabilidade para fins de compliance e governança no caso de um ataque. Isso é particularmente verdadeiro em um ambiente de TI em nuvem e multinuvem cada vez mais híbrido, em que os dados geralmente são migrados do local para a nuvem e de/para diferentes sistemas de armazenamento.

O gerenciamento de dados é uma parte inestimável da detecção e mitigação de ataques de segurança cibernética e deve ser uma parte integrante da infraestrutura de TI, como armazenamento, para assegurar que o gerenciamento seja realizado facilmente, sem muito monitoramento e intervenção manuais.

Um líder comprovado do setor com especialização demonstrável em gerenciamento de dados é a Lenovo, líder global em infraestrutura, software e serviços de TI. A ampla linha de recursos de armazenamento, computação, software e serviço/suporte da Lenovo ajuda as organizações a criar uma estrutura de segurança abrangente com base no gerenciamento de dados de última geração.

A estratégia de defesa de segurança cibernética da Lenovo é construída com base em vários princípios fundamentais, incluindo a primazia do gerenciamento de dados para detectar e prevenir ataques potencialmente prejudiciais automaticamente, sem precisar depender de um exército de analistas de segurança. As soluções de armazenamento e software da Lenovo também são construídas com base na “segurança por design”, onde os produtos e serviços são criados desde o início com a segurança como função principal, em vez da sua inclusão após a implementação da infraestrutura e o surgimento de ameaças.



Como o gerenciamento de dados, a infraestrutura e o software da Lenovo fortalecem suas defesas

Na última década e meia, a Lenovo construiu uma reputação de liderança em infraestrutura de TI do terminal ao data center. Seus desktops, notebooks, servidores e armazenamento são amplamente reconhecidos por requisitos empresariais, como desempenho, escalabilidade, resiliência e segurança.

As soluções de armazenamento e computação da Lenovo são partes fundamentais da estrutura de defesa de segurança cibernética de uma organização. Suas séries DM e DE de armazenamento totalmente em flash e flash híbrido, combinadas com a linha de servidores ThinkSystem, ajudam a detectar e mitigar o impacto de violações de segurança em vários níveis, incluindo:

- Autenticação multifator
- Access points leves
- Monitoramento de contas e grupos privilegiados
- Segmentação de rede
- Acesso baseado na função
- Criptografia de volume
- Criptografia agregada
- Limpeza segura
- Criptografia de armazenamento
- Inicialização segura do Onboard Key Manager

O hardware e software de armazenamento da Lenovo detectam e mitigam o impacto das ameaças cibernéticas em vários níveis, incluindo:

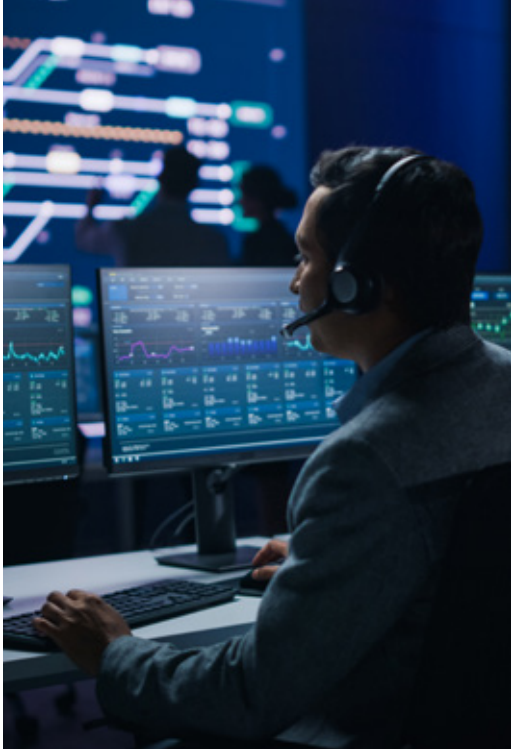
- Geração de instantâneos (snapshots) para garantir que nenhum dado seja perdido nas principais cargas de trabalho.
- Restaurações de dados rápidas, simples e confiáveis.
- Replicação para mover os dados para fora do local para reiniciar cargas de trabalho em caso de violação de dados ou interrupção de serviço.
- Arquitetura segura por design, que começa no nível dos componentes na fábrica.

As organizações estão gastando grandes somas de dinheiro em ferramentas de backup, serviços de detecção de ameaças, proteção contra malware e firewalls de última geração. No entanto, se – ou quando – essas etapas falharem, as organizações ainda devem ter a capacidade de fazer o backup de dados de produção de maneira completa, confiável e segura, independentemente da sua movimentação ou localização. Além disso, os dados das cópias de segurança devem ser validados para garantir que os administradores de TI e de armazenamento não estejam inicializando dados ruins.

Adicionalmente, a segurança da infraestrutura de armazenamento da Lenovo é reforçada pelas sólidas parcerias da empresa com os principais fornecedores de software de armazenamento de backup. As parcerias da Lenovo ajudam as organizações a suportar o impacto das violações de dados com criptografia de implementação simples, mas poderosa, para fornecer recursos de backup básicos, backups validados e testes fáceis de processos de restauração.

Os arrays de armazenamento Lenovo DM aproveitam o software de gerenciamento de armazenamento líder do setor para combater ameaças por meio de uma criptografia poderosa, instantâneos e tecnologia SnapLock para criar dados não graváveis e não apagáveis na mídia de armazenamento visando evitar que os arquivos sejam alterados ou excluídos até uma data de retenção pré-determinada ou padrão.

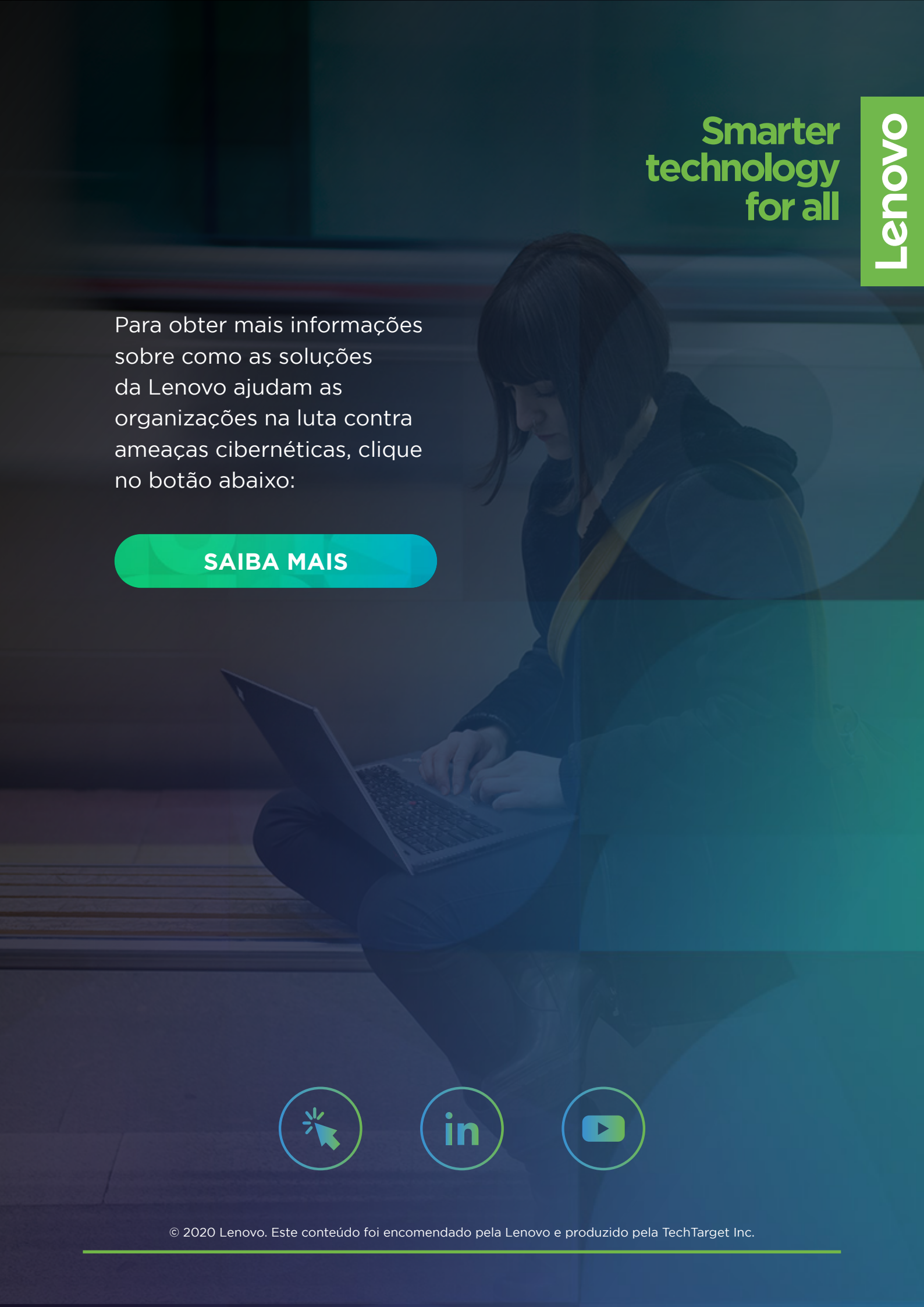
Essas e outras ferramentas de segurança são integradas às soluções de armazenamento da Lenovo desde o início, assegurando que as organizações possam aproveitar as vantagens das defesas comprovadas imediatamente, sem precisar “enfiar” as ferramentas de segurança.



Conclusão

Os ataques cibernéticos estão aumentando e nenhuma organização está imune a eles. Empresas de todos os portes, geografias e setores devem atacar as causas dos riscos de segurança cibernética com uma abordagem de vários níveis e camadas. O elemento fundamental para proteger os dados críticos antes que os hackers possam penetrar nos sistemas e ex-filtrar os dados é uma estratégia de gerenciamento de dados bem planejada e bem executada para garantir que os dados essenciais estejam sempre disponíveis e possam ser restaurados facilmente se os sistemas forem comprometidos.

As soluções de infraestrutura de armazenamento da Lenovo foram projetadas desde o início visando resiliência, escalabilidade e desempenho — e para ajudar as organizações a resistir a ataques cibernéticos e mitigar seu impacto.



Smarter technology for all

Lenovo

Para obter mais informações sobre como as soluções da Lenovo ajudam as organizações na luta contra ameaças cibernéticas, clique no botão abaixo:

SAIBA MAIS