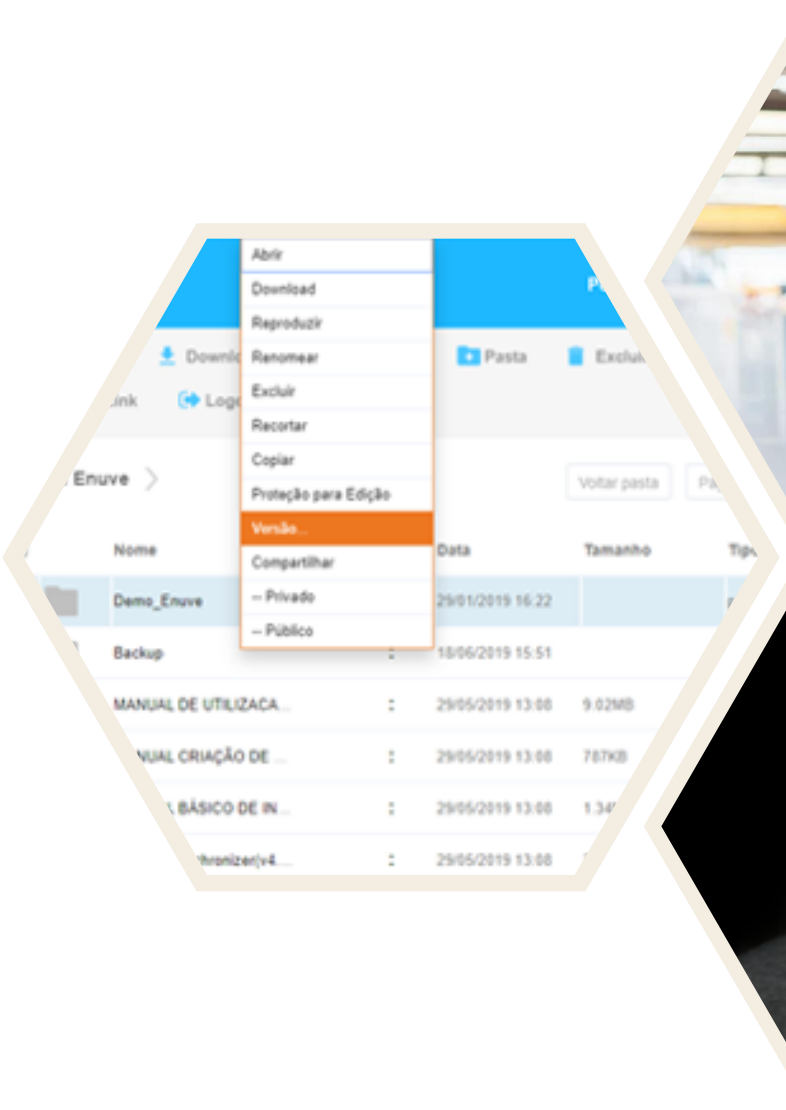
O guia completo para proteção contra perda de dados



enuve

Introdução

À medida que as ferramentas colaborativas e o armazenamento em nuvem aumentam em popularidade, você pode se perguntar como a proteção contra perda de dados se aplica à sua empresa, quais são as melhores práticas de backup de dados ou se você pode confiar em aplicativos em nuvem para armazenar adequadamente suas informações preciosas.

À medida que os aplicativos de backup continuam a se expandir, a Enuve desenvolveu este guia abrangente para ajudá-lo a navegar pelas águas muitas vezes turvas da proteção contra perda de dados corporativos.

Aqui falamos sobre alguns recursos e funcionalidades que oferecem a melhor proteção contra a perda de dados.

1. O que é proteção contra perda de dados?

A proteção contra perda de dados são os processos, ferramentas e medidas preventivas usadas para detectar quaisquer possíveis violações de dados nas informações armazenadas em toda a empresa. Ao detectar e bloquear dados confidenciais, monitorar invasões externas e evitar vazamentos de dados, o software de proteção contra perda de dados pode salvar sua empresa de riscos potencialmente devastadores.

2. O que não é proteção contra perda de dados?

É importante lembrar que a Proteção contra perda de dados é separada e distinta da Prevenção contra perda de dados.

A proteção contra perda de dados está focada em garantir que, quando sua empresa for atingida por perda de dados (seja qual for a forma), você esteja protegido contra a perda desses dados, tendo uma cópia deles armazenada fora do local.

A prevenção contra perda de dados, no entanto, está focada em impedir que os dados saiam de sua empresa por meio de um processo altamente complexo, demorado e que geralmente falha – bloquear todas as maneiras pelas quais os dados podem sair. Um efeito colateral comum da maioria das ferramentas de prevenção contra perda de dados é uma grande diminuição na produtividade dos funcionários porque eles não conseguem mais trabalhar da maneira a que estão acostumados.

3. O que causa a perda de dados empresariais?

A perda de dados pode ser resultado de diversos erros e riscos, como vazamento de dados, falhas tecnológicas, roubo, vírus, erro do usuário ou até mesmo derramar uma xícara de café.

Principais causas de interrupção dos negócios

Falha de hardware: 140.000 discos rígidos falham toda semana.

Erro do usuário: café derramado, erros simples de funcionários - de cliques errôneos a laptops perdidos - foram responsáveis por 1 em 7 incidentes de violação de dados em 2016.3

Desastre natural: Incêndios em prédios, inundações e outros desastres inesperados que podem atingir a empresa e despende tempo e custo para recuperar, além do tempo de inatividade.

Cibercrime: As pequenas empresas são os principais alvos do cibercrime. Metade das pequenas empresas já foi atingida por ransomware e 43% são os principais alvos de ataques de malware.

4. O impacto da perda de dados nos negócios

Perder dados críticos como informações de clientes, informações de contas financeiras ou propriedade intelectual – ou até mesmo perder temporariamente o acesso a esses dados – leva a custos devastadores.

Os custos devastadores da perda de dados:

Tempo de inatividade: a perda de dados ou arquivos essenciais para sua empresa pode fazer com que ela seja totalmente encerrada.

Perda de produtividade: quase 80% dos custos de tempo de inatividade vêm da perda de produtividade dos funcionários. Seus funcionários não podem fazer seu trabalho diário porque não podem acessar seus arquivos.

Recriando o trabalho perdido: Se os arquivos não puderem ser recuperados, você terá que arcar com o custo – em tempo e trabalho – de recriá-los.

Oportunidades de vendas perdidas: é um mundo acelerado e sem desculpas. Se sua equipe de vendas não puder fazer uma apresentação porque o pitch deck foi perdido, essa oportunidade pode ter desaparecido para sempre.

Perda de receita: tempo de inatividade, perda de produtividade, perda de oportunidades de vendas - tudo isso afeta fortemente seus resultados.

5. Armazenamento em nuvem versus proteção contra perda de dados: qual é a diferença?

A perda de dados na computação em nuvem costuma ser uma ameaça negligenciada quando se trata de proteção contra perda de dados. As ferramentas de colaboração são uma maneira moderna e inovadora de armazenar seus dados, mas veja por que você pode precisar de proteção adicional.

Ferramentas de colaboração em nuvem: impulsionando a produtividade moderna

Ferramentas de colaboração na nuvem, como Google Drive, Microsoft OneDrive, Box e Dropbox, impulsionam novas formas poderosas de trabalhar, permitindo o compartilhamento contínuo de ideias e dados que aceleram a velocidade dos negócios, aumentam a eficiência e melhoram as experiências dos clientes.

Cloud Storage = proteção contra perda de dados?

À medida que as empresas procuram novas maneiras de aproveitar as ferramentas de colaboração na nuvem, é tentador vê-las como um substituto potencial para um verdadeiro produto de proteção contra perda de dados. Mas uma ferramenta que armazena arquivos na nuvem não é a mesma coisa que proteção automática contra perda de dados na nuvem. Na verdade, os maiores pontos fortes dessas ferramentas tornam-se pontos fracos perigosos quando usados no lugar do verdadeiro backup automático baseado em nuvem, expondo sua empresa a grandes riscos - desde ajudar a espalhar malware ou ransomware até perder produtividade, receita e até mesmo clientes.

Para ajudar as empresas a maximizar o valor de suas ferramentas de colaboração na nuvem – ao mesmo tempo que protegem seus arquivos, sua propriedade intelectual e sua produtividade – detalhamos como os pontos fortes das ferramentas de colaboração também podem ser seus maiores pontos fracos.

5. Armazenamento em nuvem versus proteção contra perda de dados: qual é a diferença?

Proteção contra perda de dados na nuvem + ferramentas de colaboração:

Colaboração na nuvem

Ferramentas de colaboração na nuvem
Acesse arquivos em qualquer lugar
Escolha facilmente os arquivos para compartilhar
Sincronize as edições mais recentes instantaneamente
Mantenha seu negócio em movimento

Backup automático na nuvem

Arquivos seguros em todos os lugares
Proteja automaticamente todos os arquivos
Restaurar qualquer versão imediatamente
Sempre se recupere

Os riscos de confiar na colaboração na nuvem como proteção contra perda de dados

Um ponto forte: sincroniza as versões mais recentes dos arquivos nos quais seus funcionários estão trabalhando atualmente.

Torna-se um ponto fraco: os funcionários só compartilham arquivos nas fases posteriores de conclusão. Arquivos de trabalho em andamento, notas, ideias e todos os outros trabalhos que vêm antes de um rascunho “compartilhável” ficam completamente desprotegidos contra perda de dados.

5. Armazenamento em nuvem versus proteção contra perda de dados: qual é a diferença?

Totalmente dependente da conformidade do funcionário

Um ponto forte: dá aos usuários controle máximo sobre o acesso e compartilhamento de arquivos.

Torna-se uma fraqueza: mesmo que a política oficial da sua empresa seja salvar todos os arquivos - incluindo arquivos de trabalho em andamento - no aplicativo de compartilhamento na nuvem, você ainda depende completamente de seus funcionários se lembrarem de salvar os arquivos manualmente todas as vezes. Se esquecerem – ou ignorarem – essa política, arquivos valiosos ficarão desprotegidos.

Armazenamento limitado

Um ponto forte: armazenamento em nuvem “gratuito e ilimitado”.

Torna-se um ponto fraco: se você usar uma ferramenta de colaboração em nuvem para proteção verdadeiramente abrangente – todas as versões de todos os arquivos, para sempre – provavelmente atingirá os limites ocultos do armazenamento “ilimitado” e acabará pagando um prêmio pela capacidade de armazenamento adicional.

Faltam ferramentas administrativas essenciais

Um ponto forte: funcionalidade desenvolvida pensando no usuário final.

Torna-se uma fraqueza: os administradores não têm como confirmar quais arquivos estão protegidos.

5. Armazenamento em nuvem versus proteção contra perda de dados: qual é a diferença?

Não foi desenvolvido para proteger e proteger informações valiosas

Ponto forte: acesso contínuo e compartilhamento fácil.

Torna-se um ponto fraco: as soluções de colaboração em nuvem são criadas para facilitar o compartilhamento, mas isso significa que elas também podem compartilhar facilmente malware e vírus. As soluções de proteção contra perda de dados fornecem um “air-gap” para ajudar a garantir que as infecções não sejam compartilhadas.

Propagação de malware e ransomware

Ponto forte: Sincronização em tempo real e compartilhamento contínuo de arquivos.

Torna-se uma fraqueza: os arquivos infectados que começam no dispositivo de um funcionário se espalham rapidamente para outros usuários por meio da sincronização automática. E pior, o malware é projetado especificamente para essa fraqueza, usando ferramentas de colaboração em nuvem para penetrar em todos os arquivos da empresa por meio de um único dispositivo.

5. Armazenamento em nuvem versus proteção contra perda de dados: qual é a diferença?

Preenchendo as lacunas com proteção automática contra perda de dados

As verdadeiras soluções de proteção contra perda de dados oferecem funcionalidade exclusiva projetada especificamente para eliminar lacunas e fornecer proteção abrangente de todos os seus arquivos e dados, para que você sempre possa se recuperar, não importa o que aconteça.

Restaurações mais rápidas: técnicas exclusivas de armazenamento de dados, fluxos de trabalho de restauração simples e recursos de restauração pontual significam que você pode restaurar um laptop inteiro em minutos, com apenas alguns cliques. não diminuindo o trabalho também.

Da fonte: a proteção automática contra perda de dados extrai arquivos diretamente dos laptops e desktops dos funcionários, capturando todos os arquivos de trabalho em andamento para proteger a produtividade.

Abrangente: as soluções automáticas de proteção contra perda de dados na nuvem abrangem todas as versões de todos os arquivos, para que você possa voltar rapidamente ao momento anterior à ocorrência de um incidente.

Seguro: recursos como criptografia sofisticada para dados em trânsito e em repouso e controles de acesso simples protegem suas informações mais valiosas e confidenciais.

Restaurações mais rápidas: técnicas exclusivas de armazenamento de dados, fluxos de trabalho de restauração simples e recursos de restauração pontual significam que você pode restaurar um laptop inteiro em minutos, com apenas alguns cliques.

6. Os erros comuns e as melhores práticas de proteção contra perda de dados

Com 37% das pequenas e médias empresas perdendo dados na nuvem, não é surpresa que especialistas e analistas de segurança de dados concordem: a proteção contra perda de dados é um complemento essencial para aplicativos de compartilhamento na nuvem. Em muitos casos, a prevenção contra perda de dados não pode ser alcançada, portanto, as empresas devem praticar a proteção contra perda de dados. Na verdade, a propriedade intelectual (IP) contida em todos esses arquivos representa cerca de 80% do valor típico do negócio.

As soluções dedicadas de proteção contra perda de dados preenchem as lacunas deixadas pelos aplicativos de compartilhamento na nuvem, garantindo a proteção contínua dos dados de todos os arquivos. As soluções de proteção contra perda de dados também são criadas especificamente para a recuperação de desastres mais rápida, organizando arquivos para restaurações rápidas e oferecendo restauração pontual.

Resumindo: os aplicativos de compartilhamento em nuvem são projetados para impulsionar o trabalho; a proteção contra perda de dados foi desenvolvida especificamente para permitir que você se recupere. Em vez de criar uma estratégia de backup focada apenas em hackers e ameaças cibernéticas, a melhor prática é adotar uma abordagem holística e honesta que leve em consideração as tendências naturais (e humanas) de seus funcionários. Procure ferramentas que os capacitem - não os sobrecarregue.

Crie uma estratégia de proteção contra perda de dados que seja silenciosa, automática, constante e abrangente – e mantenha seu pessoal (e sua empresa) avançando.

6. Os erros comuns e as melhores práticas de proteção contra perda de dados

5 chaves para criar uma melhor estratégia de proteção contra perda de dados de negócios para humanos imperfeitos

I. Tenha um backup

O erro comum

A maioria das empresas pensa que tem seus arquivos e dados protegidos, mas um estudo recente descobriu que 58% das pequenas empresas não estavam preparadas para um incidente de perda de dados. Além disso, mais da metade de todos os backups (60%) acabam falhando na restauração efetiva dos arquivos perdidos, fazendo com que o negócio comece do zero.

Prática recomendada de backup de dados

Vale a pena dizer em voz alta: Qualquer proteção é melhor do que nenhuma proteção. E certifique-se de seguir a estratégia básica de backup “3-2-1”:

6. Os erros comuns e as melhores práticas de proteção contra perda de dados

II. Torne-o automático: não dependente de humanos

O erro comum

A maioria das empresas pensa muito no backup em si: onde está localizado, como é protegido, etc. Mas e como os arquivos e dados são protegidos? Ironicamente, a abordagem tradicional é contar com funcionários para salvar manualmente arquivos importantes em um servidor, uma unidade de rede ou outros locais designados. Mas se o maior motivo para proteger seus arquivos é proteger contra erros humanos, você não pode ter uma política que dependa desses mesmos humanos propensos a erros. Pense nisso: a melhor prática é proteger todos os arquivos a cada 15 minutos. Se seus funcionários realmente parassem para salvar arquivos manualmente 32 vezes ao dia, você veria uma grande queda na produtividade.

Prática recomendada de proteção contra perda de dados

Todas as principais soluções de proteção contra perda de dados corporativos agora fazem backup automático e silencioso de arquivos continuamente. Você não está vulnerável a funcionários que se esquecem de fazer backup - e não está sobrecarregando seus funcionários com a tarefa constante de salvar arquivos manualmente, que drena a produtividade.

6. Os erros comuns e as melhores práticas de proteção contra perda de dados

III. Proteja seus arquivos na fonte: direto do laptop ou desktop

O erro comum

A pesquisa sugere que 60% dos arquivos e dados da sua empresa residem exclusivamente nos desktops e laptops de seus funcionários. Se você estiver fazendo backup apenas de um destino central, como uma unidade de rede, todos esses arquivos de trabalho em andamento – toda essa produtividade e valor – ficarão nos laptops e desktops de seus funcionários, não protegidos. Isso ocorre porque os funcionários normalmente movem os arquivos para o destino central quando terminam - ou pelo menos em um estado "pronto para compartilhar".

Prática recomendada de proteção contra perda de dados

Como a maioria dos arquivos e dados de sua empresa agora residem nos desktops e laptops de seus funcionários (onde eles fazem a maior parte do trabalho), as principais soluções de proteção contra perda de dados são proteger arquivos e dados diretamente desses dispositivos de endpoint. Essa abordagem garante a continuidade dos negócios, capturando e protegendo a produtividade e o valor de todos os seus funcionários.

6. Os erros comuns e as melhores práticas de proteção contra perda de dados

IV. Obtenha a vantagem da proteção automática contra perda de dados: ilimitada, mais segura e mais econômica

O erro comum

Outra ironia do backup tradicional: muitas empresas ainda contam com backup baseado em hardware. O hardware tem duas grandes falhas: falha e é vulnerável a danos físicos. Além disso, o backup local convencional tem todas as deficiências da TI convencional: um grande investimento inicial de capital; um longo período de implementação; e alguém para gerenciar e manter seu espaço finito.

Prática recomendada de proteção contra perda de dados

As múltiplas redundâncias da nuvem significam que você nunca está vulnerável a desastres ou falhas de tecnologia. A proteção automática contra perda de dados é simples – instalada e funcionando instantaneamente, sem nada para gerenciar ou manter. Os especialistas em segurança de dados concordam que a nuvem oferece as ferramentas de segurança mais avançadas, graças às atualizações em tempo real que incluem os patches de segurança mais recentes e novos recursos de segurança.
Por fim, o armazenamento em nuvem oferece uma opção econômica para proteger todos os seus arquivos, para que você não precise escolher quais arquivos proteger. Isso significa que você pode seguir outra prática recomendada de proteção contra perda de dados: proteger todas as versões de todos os arquivos, para que você possa voltar instantaneamente ao momento anterior a um incidente, restaurando uma versão “limpa” e minimizando a perda de produtividade.

6. Os erros comuns e as melhores práticas de proteção contra perda de dados

V. Os aplicativos de compartilhamento em nuvem NÃO são iguais à proteção automática contra perda de dados

O erro comum

Todos os aplicativos de armazenamento em nuvem não são criados iguais. Aplicativos de compartilhamento na nuvem como Dropbox, Google Drive e Microsoft OneDrive estão ajudando empresas de todos os tamanhos a trabalhar de novas maneiras inteligentes. Mas, os mesmos recursos que tornam os aplicativos de compartilhamento em nuvem ótimos para compartilhamento e colaboração os tornam uma responsabilidade perigosa quando usados no lugar de serviços de backup em nuvem automáticos reais:

Depende de ações manuais – Os funcionários precisam selecionar ativamente os arquivos a serem adicionados.

Nem todos os arquivos são protegidos – os funcionários só compartilham arquivos nos estágios posteriores de conclusão. Todo o trabalho que entrou em um rascunho "compartilhável" é vulnerável à perda total.

Os erros de uma pessoa passam a ser de todos - se um funcionário cometer um erro ou excluir um arquivo - e não o detectar imediatamente - esse erro se tornará um problema de todos.

Pode espalhar malware e ransomware – Se um funcionário compartilhar um arquivo infectado, ele pode se espalhar rapidamente para todos.

Não projetado para restaurações de arquivos fáceis e rápidas – Se vários arquivos – ou um laptop inteiro – forem perdidos, o processo de recuperação de desastres geralmente requer uma restauração demorada.

7. Mantenha seus negócios avançando com proteção contra perda de dados da Enuve

Em sua essência, a Enuve protege você, garantindo que sempre haja outra cópia de seus dados, não importa o que aconteça com seu computador. Você pode estar pensando "espere, isso é backup!"

A Enuve fecha as lacunas deixadas pelas soluções de backup antigas, reduz o risco de perda de dados críticos de negócios e torna mais fácil para você continuar atendendo seus clientes, em vez de se preocupar com TI e segurança. Ele faz isso de várias maneiras.

· Backup de servidores de arquivos e estações de trabalho
· Backup de máquinas virtuais
· Armazenamento ilimitado conforme sua necessidade
· Backup automático e ilimitado
· Criptografia AES 256 altamente segura de ponta a ponta
· Guardamos quantas versões você desejar de cada arquivo
· Fácil recuperação em caso de perda ou desastre
· Proteção contra Ransomwares
· Painel de gestão centralizado
· Relatório de logs com todas as ações dos usuários
· Fácil acesso aos arquivos da empresa
· Controle de acessos por parte dos usuários
· Mobilidade através de acesso web e app
· Possibilidade de trabalhar diretamente na nuvem

A Enuve é uma maneira econômica e simples para qualquer empresa se proteger contra a perda de dados. Sua empresa pode reduzir a quantidade total de trabalho que você pode perder no caso de um desastre digital de 24 horas para apenas 30 minutos.

Se você quiser conhecer com mais detalhes, solicite aqui um contato.