10 Etapas para a Resiliência Cibernética do Microsoft 365

Conteúdo

O Aumento dos Ataques Cibernéticos ao Microsoft 365

Proteger os dados do Microsoft 365 é um aspecto essencial de uma estratégia moderna de cibersegurança, já que as aplicações do conjunto permeiam as operações diárias de inúmeros negócios e operações. Com uma grande variedade de ferramentas de produtividade, incluindo o Exchange, o Teams, o SharePoint, o OneDrive e mais, o Microsoft 365 contém uma riqueza de informações confidenciais e dados essenciais de negócios, e é a razão pela qual há cada vez mais empresas investindo em soluções de terceiros ou serviços de backup gerenciados para protegê-los.[1] Na verdade, há evidências de que o ransomware está sendo projetado com o propósito específico de se infiltrar no Microsoft 365 e em outras aplicações SaaS. De acordo com um relatório da Coalition, houve um aumento de 12% nas reivindicações virtuais no primeiro semestre de 2023, impulsionado por ataques de ransomware, com um pedido médio de resgate de US$ 1,62 milhão.[2] Como consequência de seu uso generalizado, e à medida que mais funcionários instalam e usam o Microsoft 365 em máquinas de trabalho em casa, a plataforma tem se tornado particularmente vulnerável para invasores que capitalizam essa infraestrutura diversificada.

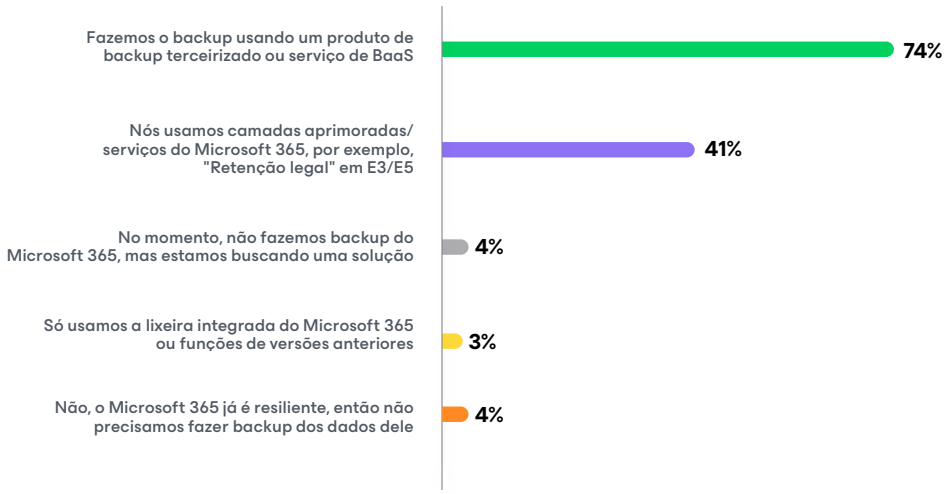
12%

de aumento nas reivindicações cibernéticas no primeiro semestre de 2023

US$ 1,62 milhão

é o pedido médio de resgate

Sua organização faz backup dos dados a partir do Microsoft 365?



[1] Relatório sobre Tendências em Proteção de Dados 2024

[2] Microsoft 365 ransomware: Sua Guia abrangente para compreensão, prevenção e recuperação

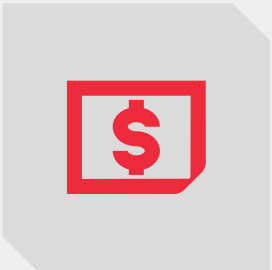
Os riscos associados à perda de dados do Microsoft 365 são, portanto, além de complexos, muito reais. A perda de dados resulta em sérias interrupções operacionais e pode infligir danos financeiros significativos devido ao tempo de inatividade e à perda de produtividade. Em um relatório, líderes de TI estimaram o custo do tempo de inatividade em US$ 1.467 por minuto (US$ 88.000 por hora)[3] — o que, considerando o volume de tempo gasto e de trabalho realizado com o Microsoft 365 em um dia de trabalho comum, não é uma surpresa. Além disso, quando dados confidenciais são expostos, as organizações enfrentam penalidades pesadas de conformidade e danos à reputação — no caso de infrações da GDPR, multas de até US$ 21 milhões.[4] Considerando que os dados do Microsoft 365 são extremamente confidenciais para as organizações e seus funcionários, é mais do que provável que eventos de perda de dados desgastem não apenas a confiança de um cliente, mas também de um funcionário, potencialmente levando a um declínio nos negócios e a danos à reputação de longo prazo dentro e fora da empresa.

As possíveis consequências de dados desprotegidos do Microsoft 365 não podem ser exageradas. Violações que expõem informações pessoais podem levar a roubo de identidade e fraude, causando danos muito tempo depois do comprometimento inicial. Para as empresas, a perda de propriedade intelectual pode corroer as vantagens competitivas e resultar em custosas batalhas legais ou multas, que também podem enfrentar litígios se forem consideradas negligentes na proteção dos dados de seus clientes.

Não há como evitar isso. Uma abordagem proativa para proteger os dados do Microsoft 365 é mais do que uma ideia inovadora — é imperativo garantir que as empresas mantenham a continuidade, respeitem as responsabilidades legais e normativas e mantenham a confiança do cliente.

[3] Relatório sobre Tendências de Proteção de Dados de 2022
[4] Quais são as multas da GDPR?

Custo associado à perda de dados



O custo do tempo de inatividade será US$ 1.467 por minuto (US$ 88.000 por hora)

No caso de infrações GDPR, multas chegam a $21 milhões.

Violações que expõem informações de persona podem levar a roubo de identidade e fraude.

Etapas para se preparar contra ataques

1. Autenticação multifator

Autenticação multifator (MFA) é uma medida de segurança essencial que exige que os usuários forneçam dois ou mais fatores de verificação para obter acesso a recursos digitais, como contas de e-mail, aplicativos de negócios e serviços online. A MFA melhora muito a segurança, adicionando camadas de proteção além de apenas uma senha. Isso significa que, mesmo que um cibercriminoso obtenha a senha de um usuário, ainda precisará ignorar os fatores de autenticação adicionais para obter acesso. Isso não é nada menos que uma barreira formidável contra a entrada não autorizada.

Os benefícios da MFA são muitos, principalmente no contexto do Microsoft 365, em que os dados confidenciais e as comunicações corporativas são perpétuas. A MFA pode se defender contra as consequências de ataques cibernéticos comuns, como phishing, em que os invasores enganam os usuários para que divulguem credenciais.

Essa etapa adicional de autenticação pode ser algo que o usuário sabe (como um PIN ou uma pergunta de segurança) ou algo que o usuário tem (como um smartphone ou hardware da empresa).

Mesmo em cenários onde as senhas são comprometidas devido a senhas fracas ou reutilizadas, uma configuração de MFA continuará protegendo a conta contra acesso não autorizado. Esse nível de segurança é crítico em ambientes do Microsoft 365, onde o acesso remoto é rotineiro e os usuários podem estar se conectando a partir de redes não seguras ou dispositivos pessoais. No geral, como um fato simples e tranquilizador, a MFA cria um mecanismo de defesa dinâmico que se adapta ao cenário de ameaças em evolução.

Benefícios do MFA

Defende contra as consequências de ataques cibernéticos comuns

Continua protegendo a conta contra acesso não autorizado

Cria um mecanismo de defesa dinâmico que se adapta ao cenário de ameaças

2. Acesso de privilégio mínimo

O princípio do menor privilégio é um dos pilares de práticas eficazes de cibersegurança, integralmente relacionado ao conceito de arquitetura Zero Trust, e é fundamental para fortalecer uma organização contra possíveis ataques cibernéticos. Uma arquitetura Zero Trust opera sob a premissa de que há ameaças dentro e fora da rede, de modo que nenhum usuário ou sistema seja automaticamente confiável.[5] Isso se alinha ao princípio do privilégio mínimo, o qual determina que os usuários devem receber níveis mínimos de acesso (ou permissões) necessários para desempenhar suas funções de trabalho, e nada além disso. Para o Microsoft 365, implementar esses princípios pode significar restringir o acesso a determinados documentos, pastas, sites, configurações administrativas e aplicativos com base na função do usuário na organização.

Adotar um modelo de acesso de privilégio mínimo pode aumentar significativamente a postura de segurança do seu ambiente do Microsoft 365. Em primeiro lugar, esse modelo minimiza a possível superfície de ataque do pacote de software para cibercriminosos. Se a conta de um usuário for comprometida, o invasor estará limitado aos direitos de acesso dessa conta, que idealmente devem ser os mais restritivos possíveis. Por exemplo, se as credenciais de um usuário forem roubadas, o invasor não conseguirá acessar informações confidenciais ou executar tarefas administrativas se esses direitos não estiverem associados à conta do usuário. Essa limitação de danos cria uma zona de quarentena para qualquer violação de segurança e é fundamental para controlar a propagação de um ataque em uma organização.

[5] https://www.veeam.com/news/new-zero-trust-data-resilience-model-introduced-by-it-security-and-data-protection-experts.html

3. Backups Regulares

Sendo um alvo preferencial para os cibercriminosos, os backups são extremamente importantes para o Microsoft 365, principalmente quando você considera o Modelo de responsabilidade compartilhada da Microsoft[6], o qual afirma que as empresas são responsáveis pela segurança de seus dados. O ransomware representa uma ameaça significativa para a integridade de dados, uma vez que os invasores têm como objetivo criptografar os arquivos de uma organização e exigir pagamento para liberá-los. No entanto, as ameaças aos dados não se limitam a ataques maliciosos. Os dados também podem ser comprometidos por exclusões acidentais ou vários outros percalços. Manter os backups atualizados permite que a organização recupere rapidamente o acesso aos seus dados, independentemente da perda ser resultado de ransomware, erro humano ou muitos outros motivos críticos para manter backups do Microsoft 365.[7] Isso não apenas minimiza o tempo de inatividade, mas também envia uma mensagem forte de que a organização não é um alvo fácil para ataques futuros.

Implementar uma rotina de backup regular significa estabelecer um cronograma que encontre um equilíbrio entre o volume de dados tratados e os recursos disponíveis para operações de backup. Isso deve incluir o backup de e-mails, documentos, contatos, calendários e quaisquer outros dados armazenados no pacote Microsoft 365.

Pense nisso como ter uma apólice de seguro. Pode não ser necessário todos os dias, mas quando o desastre acontece, pode ser a diferença entre uma recuperação rápida e uma catástrofe letal.

[6] Responsabilidade Compartilhada na Nuvem

[7] Os 7 Motivos Críticos para Fazer Backup do Microsoft 365

4. Backups imutáveis

A imutabilidade desempenha um papel fundamental na proteção dos ativos digitais de uma organização contra alteração ou exclusão, seja por ameaças virtuais ou erro humano. Para o Microsoft 365, onde grandes quantidades de dados são rotineiramente geradas, compartilhadas e armazenadas, garantir que cópias de backup sejam impermeáveis a mudanças é um elemento crítico de uma estratégia robusta de mitigação de ameaças.
A imutabilidade garante que, uma vez feito o backup, a informação permaneça em um estado puro e inalterável por um determinado período de tempo.

Para as organizações que usam o Microsoft 365, os backups imutáveis servem de escudo contra ataques de ransomware, que visam não só dados operacionais ativos, mas também repositórios de backup. Na verdade, de acordo com uma pesquisa, quase todos os ataques de ransomware (93%) têm como alvo específico os backups.[8] Para outras medidas de segurança, uma cópia de backup imutável dos dados é importante. Ao criar e aplicar políticas de retenção que protegem dados de backup contra sobrescrita ou adulteração, as empresas podem efender suas práticas de continuidade contra criptografia ou destruição indesejada dos dados. A imutabilidade garante que, apesar de qualquer violação de segurança que afete os armazenamentos de dados atuais, a organização pode restaurar as operações a partir de um backup limpo e inalterado.

93%

dos ataques de ransomware visam especificamente os backups.

[8] Relatório sobre Tendências de Ransomware 2023

5. Plano de resposta a incidentes

Um plano de resposta a incidentes é um plano bem estruturado. Ele detalha os processos que uma organização deve seguir quando confrontada com vários incidentes de segurança cibernética, servindo como roteiros para identificar, conter, erradicar e se recuperar de ameaças de segurança, além de garantir que todas as partes interessadas estejam informadas e preparadas para agir.

Para as organizações que usam o Microsoft 365, a base de um plano sólido de resposta a incidentes inclui a identificação de ativos críticos dentro do ecossistema do Microsoft 365. Isso significa identificar onde os dados confidenciais são armazenados, seja no OneDrive, SharePoint, Exchange Online ou em outro lugar. Uma vez identificados esses ativos, o plano deve definir potenciais ameaças e criar uma lista priorizada de riscos, ao lado de estratégias para mitigá-los. Isso inclui o uso de ferramentas integradas de monitoramento e detecção, estratégias de contenção imediata, erradicação de ameaças, comunicação robusta entre as partes e a identificação e recuperação de quaisquer dados perdidos ou comprometidos.

A cola que une um plano de resposta a incidentes é uma preparação minuciosa. Isso vai além de ferramentas técnicas, treinamento e colaboração das equipes de TI e segurança. Isso vale para todos os funcionários. Para aqueles que usam o Microsoft 365, as organizações devem realizar sessões regulares de educação adaptadas ao seu intrincado ecossistema. Os funcionários que usam aplicações do Microsoft 365, como o Outlook e o Teams, devem ter o conhecimento necessário para discernir e reagir a atividades suspeitas, que podem vir na forma de mensagens aparentemente legítimas, convites falsos para reuniões de colegas de trabalho ou e-mails que parecem ser autênticos de líderes da empresa. As pessoas podem ser um ponto fraco da cibersegurança de qualquer organização, mas funcionários bem treinados têm o potencial de formar uma barreira formidável contra ameaças.

Um plano de resposta a incidentes começa com

estrutura abrangente de resposta a incidentes

Identificando ativos críticos

Importância da Preparação dos Funcionários

6. Auditorias regulares e testes de penetração

Auditorias regulares e testes de penetração são componentes essenciais para manter um ambiente do Microsoft 365 resiliente. Na verdade, o próprio Microsoft 365 fornece uma gama de ferramentas integradas para auditoria e detecção de ameaças[9], servindo como uma linha de base para fortalecer seu ambiente contra várias ameaças de segurança. Essas práticas servem como medidas proativas, permitindo que as empresas identifiquem e corrijam problemas antes que eles possam ser explorados por invasores.

As auditorias do ecossistema do Microsoft 365 envolvem a revisão sistemática de vários aspectos, como permissões de usuário, controles de acesso a dados e configurações de segurança. Embora às vezes sejam complicadas, as auditorias regulares ajudam a garantir que as configurações do sistema permaneçam alinhadas com as melhores práticas e as políticas de segurança organizacional; é um hábito saudável para se criar e manter. Como o Microsoft 365 engloba uma variedade de serviços, essas auditorias devem ser abrangentes e abranger cada serviço para evitar vulnerabilidades negligenciadas.[10]

Muitas vezes referido como "hacking ético", o teste de penetração complementa as auditorias regulares, permitindo que as organizações avaliem a eficácia de suas medidas de segurança. Isso envolve simular ataques cibernéticos na infraestrutura do Microsoft 365 para identificar pontos fracos que os invasores do mundo real podem explorar. Para organizações aplicáveis, os testes de penetração devem investigar todas as camadas de seu ecossistema Microsoft 365, desde a resistência dos funcionários ao phishing até a resiliência de ferramentas técnicas, como firewalls, sistemas de detecção de ameaças e planos de resposta a incidentes. Os insights coletados nesses testes direcionam as organizações no ajuste de seus programas de treinamento e estratégias de segurança, permitindo que desenvolvam defesas mais abrangentes e eficazes quando uma ameaça cibernética inevitavelmente surgir.

[9] Microsoft 365 Orientações para segurança e conformidade

[10] Microsoft 365 segurança nativa: Desbloqueando recursos de conformidade e monitoramento

7. Políticas de restrição de software

Uma política de restrição de software (SRP) é um recurso de segurança que as organizações podem usar para identificar e controlar a execução de software em hardware especifico. Para as organizações corporativas que usam o Microsoft 365, a implementação dessa política pode atuar como um importante mecanismo de defesa para a proteção de muitos dispositivos pelos quais elas são responsáveis. Como Microsoft 365 contém uma série de ferramentas distintas, ele também convida a uma variedade de vetores de ameaças distintos e exploráveis. Ao ditar qual software pode ou nãoser executado em um sistema, os SRPs reduzem efetivamente a superfície de ataque disponível a agentes mal-intencionados.

Ao construir um SRP para um ambiente Microsoft 365, o objetivo é garantir que apenas aplicativos, scripts e processos confiáveis tenham permissão para executar, incluindo vetores de ameaças na lista branca e na lista negra, conforme necessário. Para máxima eficácia, as SRPs devem ser configuradas tendo em mente o acesso de privilégio mínimo e devem ser regularmente atualizadas para refletir as alterações no software usado por uma organização. Isso inclui atualizações para as ferramentas do Microsoft 365, a adição de novo software ou a descontinuação de aplicações legadas.

Ao impedir que o malware aproveite técnicas comuns de exploração, os SRPs são altamente eficazes para interromper a cadeia de infecção e manter uma zona de quarentena. A integração de SRPs em uma estratégia de segurança cibernética é uma abordagem inovadora que ajuda a proteger a infraestrutura de uma organização contra a execução de software não confiável — algo que, à medida que as corporações crescem e contratam novos funcionários, é uma possibilidade cada vez maior.

8. Monitoramento e registro em log

Monitoramento e o registro em log constituem um passo vital para garantir a segurança e a integridade de qualquer ambiente Microsoft 365. Ao manter um olhar vigilante sobre as atividades do sistema e manter registros abrangentes de eventos, as organizações podem detectar possíveis incidentes de segurança em tempo real, diagnosticar problemas do sistema, entender o escopo das violações e melhorar a postura geral da segurança.

Para administradores do Microsoft 65, a importação de logs para um sistema SIEM (Informação de Segurança e Gerenciamento de Eventos) compatível pode simplificar muito esse processo. O Azure Sentinel, por exemplo, é um SIEM nativo da Microsoft que usa uma matriz de conectores de dados predefinidos para streaming dos dados de log de uma organização diretamente na aplicação SIEM. Em seguida, esses dados são normalizados para obter conjuntos de dados consistentes e monitorados por meio de ferramentas de análise integradas.

Um monitoramento eficaz deve abranger uma rede ampla para detectar uma gama de possíveis anomalias indicativas de uma ameaça de segurança, que vão desde tentativas de login fracassadas (sugerindo um ataque de força bruta) até padrões de download incomuns (sugerindo exfiltração de dados indesejados) a muitos outros. O registro abrangente é igualmente importante, servindo como a documentação de todas as atividades monitoradas. Esses registros devem capturar detalhes suficientes para permitir a reconstrução de eventos em um incidente inteiro — antes, durante e depois. Isso se torna inestimável na análise forense pós-incidente, mas também auxilia nas auditorias de conformidade e no refinamento de medidas de segurança com o passar do tempo.
O registro em log deve ser cuidadosamente configurado para garantir que os dados coletados sejam acionáveis, fornecendo informações claras e relevantes sem o ruído que pode ser gerado por um escopo excessivamente ambicioso.

Com o tempo, os insights coletados do monitoramento e dos registros fornecem às organizações os dados necessários para fazer alterações proativas de políticas e simplificar as atualizações de segurança.

9. Separação de dados

A separação de privilégios é uma estratégia amplamente aplicável e eficaz usada por organizações para aprimorar sua infraestrutura de segurança e é altamente aplicável ao integrar serviços orientados por dados, como o Microsoft 365. Estratégias, como arquiteturas de multilocatários, limites administrativos e restrição de conta condicional, têm como foco a estruturação de dados e seus privilégios para reduzir o acesso não autorizado e limitar os possíveis danos das violações de segurança. Ao manter diferentes conjuntos de dados separados e dividir as redes em segmentos discretos, as organizações reduzem significativamente o risco inicial de violações de segurança e efetivamente colocam em quarentena surtos caso ocorram.

O uso de políticas de separação de privilégios no Microsoft 365 permite que as organizações mantenham regras rígidas de acesso. Como falamos em nossa seção anterior, a melhor dessas regras garante que usuários, administradores e serviços recebam apenas as permissões necessárias para executar tarefas necessárias e não mais — por exemplo, o princípio do menor privilégio e controle de acesso baseado em função (RBAC).

Para organizações que operam em várias jurisdições ou têm unidades de negócios distintas, separar os locatários do Microsoft 365 por meio de uma arquitetura de multilocatários pode ajudar a isolar os dados e controlar o acesso. Trata-se da criação de fronteiras administrativas distintas por locatário. Isso isola os ambientes de seus próprios dados, contas de usuários e controles de acesso e garante que os requisitos de conformidade e segurança sejam atendidos individualmente e que uma violação ou um problema de segurança em um locatário não comprometa a integridade dos outros.

Dentro desses limites administrativos, as políticas de acesso condicional e as restrições de conta adicionam outra camada de defesa e podem ser implementadas diretamente no Microsoft 365. Essas políticas permitem que as organizações definam e implementem regras baseadas em contexto para qualquer conta, permitindo que as regras de segurança de uma organização sejam otimizadas para o nível de risco, a localização geográfica ou as irregularidades dinâmicas de uma conta, como logins ou downloads suspeitos.

Como tal, a separação metódica pode ser aplicada a todos os níveis da hierarquia de uma organização e fornece uma base sólida para proteger os dados do Microsoft 365 e outros ativos digitais. Como a compartimentalização estratégica não apenas mitiga o risco de acesso não autorizado, mas também oferece proteções e fallbacks em camadas contra violações de segurança, a separação de dados e privilégios conquistou justamente seu status de abordagem confiável para as organizações fortalecerem suas defesas cibernéticas, manterem continuidade dos negócios e, finalmente, darem passos em direção à resiliência cibernética em seu ambiente do Microsoft 365.

10. Criptografia

Criptografia é uma medida de segurança fundamental que serve como uma linha principal de defesa na proteção de informações confidenciais, garantindo que apenas partes autorizadas com a chave de descriptografia correta possam acessar as informações originais, e se aplique aos dados, independentemente de seu uso, movimento ou localização. Em relação ao Microsoft 365, a criptografia oferece uma camada de segurança que ajuda as empresas a proteger suas comunicações, documentos e outros dados, não importa onde eles residam em sua infraestrutura de nuvem.

E-mails de phishing e sites infectados são frequentemente os precursores sutis de ataques ransomware graves. Nos últimos anos, o ransomware RobbinHood devastou organizações de forma infame, custando-lhes milhões de dólares em resgate, tempo de inatividade e esforços de recuperação, tudo por causa de um e-mail infectado que foi baixado involuntariamente e o malware foi introduzido no sistema.

Ferramentas integradas, como os rótulos de confiabilidade do Microsoft 365, ajudam a evitar isso, aderindo a protocolos rígidos que podem criptografar automaticamente documentos e e-mails, evitando assim a infecção inicial, desconfiando de e-mails suspeitos e alertando o usuário sobre remetentes potencialmente perigosos. Esses rótulos podem ser configurados com políticas de gerenciamento de direitos, permitindo que os administradores determinem quem pode acessar os dados ecomo eles podem ser usados. É um nível de classificaçãoe proteção de conteúdogovernado centralmente pelas organizações, permitindo que os administradores de TI arbitrem o manuseio, o compartilhamento ea manipulação de dados. Dessa forma, os usuários bem-intencionados têm várias proteções em vigor para evitar a introdução ou disseminação de malware (e não prejudicar os fluxos de trabalho no processo).

A criptografia eficaz forma, em última análise, a base sobre a qual a privacidade e a conformidade normativa são construídas. As organizações que utilizam efetivamente os recursos de criptografia do Microsoft 365 em paralelo às suas políticas de segurança já existentes são muito mais resilientes cibernéticos do que aquelas que não os utilizam. Práticas sólidas de criptografia são fundamentais para a proteção de dados valiosos contra ransomware e ameaças cibernéticas, sustentando assim a privacidade, garantindo conformidade normativa e apoiando um espaço de trabalho seguro e colaborativo.

A Resiliência Cibernética do Microsoft 365 Começa com o Backup

Ao considerarmos o cenário futuro do gerenciamento e da segurança de dados, o Backup como Serviço (BaaS) surgiu como um método preferido para proteger Aplicações de SaaS, como o Microsoft 365. O BaaS é uma abordagem baseada na nuvem que fornece às organizações um sistema remoto online para fazer backup e armazenar seus dados. A integração do BaaS com uma estratégia do Microsoft 365 se alinha com a necessidade de soluções de proteção de dados robustas, escaláveis e flexíveis, sendo todas elas componentes críticos para garantir a resiliência organizacional.

Os serviços de backup permitem que as empresas terceirizem suas necessidades de backup para provedores especializados, que oferecem soluções ponta a ponta que podem automatizar processos de backup, reduzir a quantidade de infraestrutura local necessária e fornecer medidas de segurança de alto nível — tudo isso fornecendo-lhes acesso e controle diretos sobre seus dados. Para os usuários do Microsoft 365, o BaaS significa maior segurança de dados, eficiência operacional e tranquilidade.

Proteger um ecossistema Microsoft 365 é um esforço multifacetadoque exige que as organizações se envolvam tanto em medidas preventivas estratégicas quanto em planos eficazes de resposta a incidentes. A jornada para a resiliência cibernética do Microsoft 365 é contínua e requer um compromisso com o uso eficaz dos avanços tecnológicos. Felizmente, existem fornecedores de backup dedicados, personalizados para dados do Microsoft 365.

Veeam Data Cloud *for Microsoft 365*

O **Veeam Data Cloud *for Microsoft 365*** permite resiliência radical para os dados do Microsoft 365, com um toque moderno. A principal solução de backup do Microsoft 365 do setor — Veeam Backup *for Microsoft 365* — agora é fornecida como um serviço.

Simplifique sua estratégia de backup com software, infraestrutura de backup e storage ilimitado em um serviço de nuvem completo que permite aproveitar a proteção avançada de dados e a tecnologia de segurança dentro de uma experiência de usuário simples e contínua.

O Veeam Data Cloud *for Microsoft 365* é um serviço de backup que fornece proteção de dados e recuperação de dados abrangentes para **Microsoft Exchange, SharePoint, OneDrive for Business and Teams**, proporcionando o controle completo de seu ambiente do Microsoft 365.

→ Solicite uma demonstração de Veeam Data Cloud for Microsoft 365

Com o **Veeam Data Cloud *for Microsoft 365***, você recebe:

- **Tecnologia líder do setor confiável:** A solução de proteção de dados mais abrangente, com mais de uma década de inovação contínua desenvolvida em escala.
- **Plataforma moderna, segura e intuitiva:** Crie facilmente jobs de backup, complete restaurações e obtenha insights do Microsoft 365 em uma interface Web moderna.
- **Serviço com tudo incluído:** Software, infraestrutura de backup e storage ilimitado contínuos, juntamente com a manutenção coberta pelos especialistas.

Esteja preparado, mantenha-se informado

Sua jornada em direção à resiliência cibernética do Microsoft 365 não termina aqui, está apenas começando. Expanda seu entendimento, refine suas estratégias e fique à frente em 2024. Deixe-nos ajudar você a transformar desafios em oportunidades conferindo nossa coleção expandida de recursos:

- 8 Benefícios de um Serviço de Backup para Microsoft 365
- Microsoft 365 backup para Leigos
- Melhores Práticas de Recuperação do Microsoft 365

Sobre a Veeam Software

A Veeam®, líder Nº 1 do mercado global em proteção de dados e recuperação de ransomware, tem a missão de ajudar todas as organizações não só a se recuperar de uma paralização ou perda de dados, mas também a avançar. Com a Veeam, as organizações alcançam a resiliência radical por meio da segurança, recuperação e liberdade de dados para a sua nuvem híbrida. A Veeam Data Platform fornece uma solução única para ambientes físicos, virtuais, na nuvem, SaaS e Kubernetes que oferece tranquilidade aos líderes de TI e segurança, mantendo suas aplicações e dados protegidos e sempre disponíveis. Com sede em Seattle e escritórios em mais de 30 países, a Veeam protege mais de 450.000 clientes no mundo inteiro, incluindo 74% do Global 2000, que confiam na Veeam para manter seus negócios em operação. Resiliência radical começa com a Veeam. SAIBA MAIS em www.veeam.com ou siga a Veeam no LinkedIn @veeam-software e X @veeam.

