Microsoft

Guia de Segurança do Microsoft 365

scansource

Microsoft

Guia de Segurança M365

Para darem continuidade em seus negócios quando a pandemia começou, empresas ao redor do mundo investiram em ferramentas em nuvem que possibilitaram o trabalho remoto. O Microsoft 365 se destacou no cenário corporativo como uma ferramenta de colaboração e comunicação segura, sendo adotada como uma ferramenta central nas organizações.

Permitir que funcionários trabalharem de qualquer lugar e ainda serem capazes de se comunicar e colaborar de forma segura, com o passar dos dias, tem sido o principal desafio de empresas ao redor do mundo. A pandemia mudou o cenário das organizações e essas estão permitindo cada vez mais que os funcionários trabalhem acessando dados e informações corporativas de casa, cafeterias, coworks e outros locais. A capacidade de manter identidades, dispositivos, aplicativos e dados seguros se tornam uma prioridade para essas organizações.

A complexidade da TI aumentou, os ciberataques estão cada vez mais sofisticados e as empresas já estão procurando soluções para esses desafios.

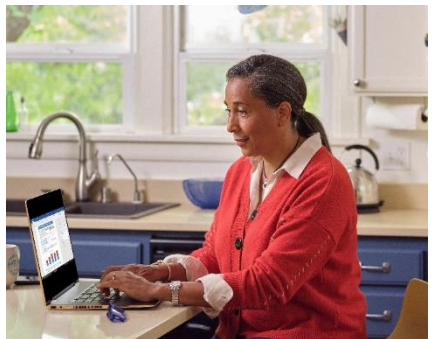
Pensando no contexto atual, elaboramos este guia para que empresas e administradores saibam como promover e melhorar a segurança da TI utilizando as ferramentas do Microsoft 365. Confira a seguir.

Microsoft 365

Microsoft 365 é uma **solução em nuvem segura, econômica e confiável para colaboração em tempo real e trabalho seguro de praticamente qualquer lugar.**

Ele inclui Microsoft Teams, armazenamento em nuvem e aplicativos conhecidos do Office com opções avançadas de segurança. Você pode usá-lo para conversar, ligar, hospedar reuniões online e colaborar em tempo real.



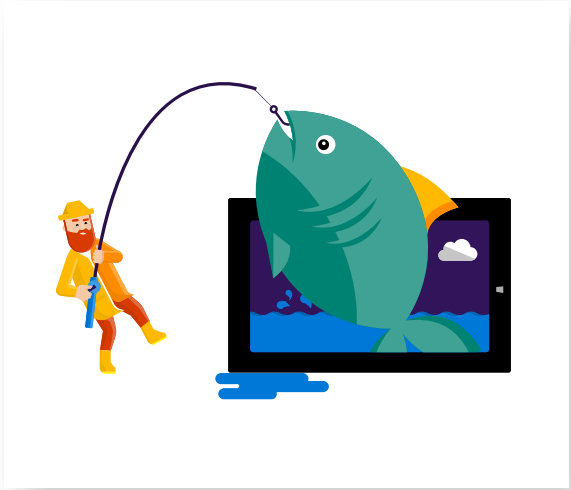
Segurança nas empresas

A responsabilidade da cibersegurança é coletiva

- Para criar um escudo efetivo contra ciberataques, é necessário difundir uma cultura baseada em mitigação de riscos. O sucesso em aumentar a segurança das empresas não pode estar baseada apenas na implantação de tecnologias, mas também na educação e concientização dos funcionários de como os ataques funcionam e como podem ser evitados.

  Ao terem visibilidade do seu papel na segurança da organização, os funcionários coloboram para melhorar a posição de segurança da empresa.

Ameaças Comuns e como agir frente a elas



Ataques de Phishing

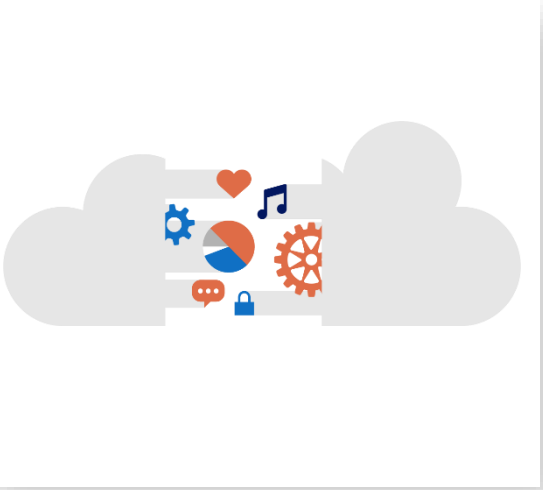
O golpista envia um texto direcionado, como um e-mail, com o objetivo de convencer a vítima a clicar em um link, baixar um anexo, enviar as informações solicitadas ou até mesmo concluir um pagamento real.

Evite clicar em links suspeitos e certifique-se de que a mensagem foi enviada por uma fonte confiável. Configure uma ferramenta anti-phishing automatizada, e evite a contaminação em massa.

Ransomware

Através de um software malicioso, os dados críticos de um usuário ou organização são criptografados para que não possam ser acessados. Arquivos, bancos de dados ou aplicativos. Então, o atacante exige um pagamento para que os dados sejam devolvidos.

Evite clicar em links desconhecidos e baixar arquivos de sites não confiáveis. Em caso de infecção, garanta que uma ferramenta anti-Ransomware esteja configurada.



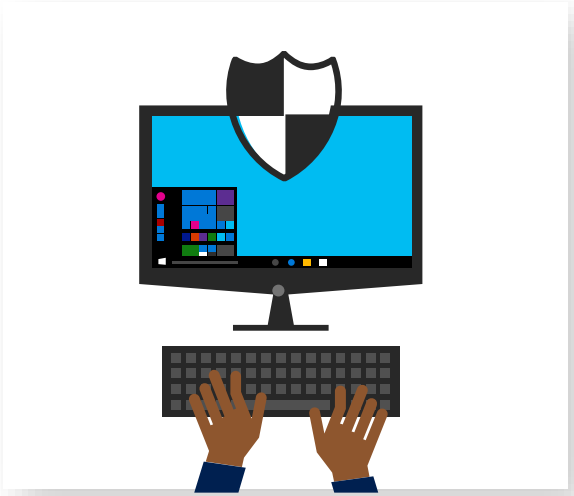
Ataque de dicionário

O objetivo do ataque é que através do método de tentativa e erro (força bruta) o atacante consiga as credenciais de identidade de um usuário. Posteriormente essa identidade é utilizada para acessar dados sensíveis, segredos industriais, etc.

Utilize ferramentas de autenticação Multifator que, além da senha, solicitam um código de verificação (SMS, ligação, token). Muitos transtornos são evitados com essa ação.

Segurança no Microsoft 365

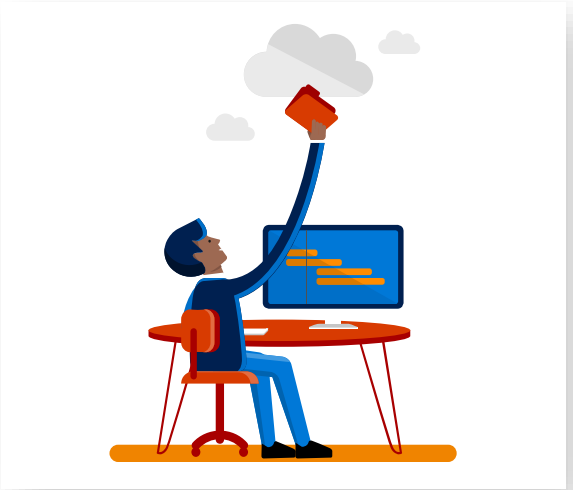
Por fornecer gerenciamento centralizado, simplicidade de configuração e ferramentas de produtividade, o Microsoft 365 se destaca por ser uma ferramenta eficiente e econômica.
Mas para que você aproveite todos os benefícios de forma segura, é necessário conhecer e aplicar os recursos disponíveis para proteger os dados da sua empresa e dos seus clientes:



Proteção contra ameaças cibernéticas

Acesso Seguro a aplicativos

Torna os dados de clientes mais seguros



Gerenciamento de usuários e dispositivos em qualquer lugar

Recursos para melhorar a segurança com o Microsoft 365

Autenticação multifator (MFA)

O MFA é um processo em que um é solicitado uma forma adicional de identificação. É exigido um dos seguintes fatores a mais para que o usuário seja autenticado: Algo que você sabe (senha), algo que você tem (um dispositivo confiável como token, ou código via sms) ou algo que você é (biometria). Evita acesso em caso de roubo de senhas.

Acesso controlado a pastas

Ajuda você a proteger dados valiosos contra aplicativos mal-intencionados, como Ransomwares, que criptografam e sequestram dados e documentos.

Anti-phishing

Através de inteligência artificial, identifica e Analisa mensagens envolvidas em ataques de phishing coordenados. Também é possível simular ataques e acompanhar as ações de seus funcionários e administradores para posterior capacitação e criação de políticas de prevenção.

Data Loss Prevention

Para proteger dados confidenciais e evitar que seus usuários os compatilhem de forma inadequada. Essa pratica é chamada de prevenção contra perda de dados (DLP). No Microsoft 365 é possível rotular esses dados e criar políticas de restrição de compartilhamento.

Microsoft Defender Application Control

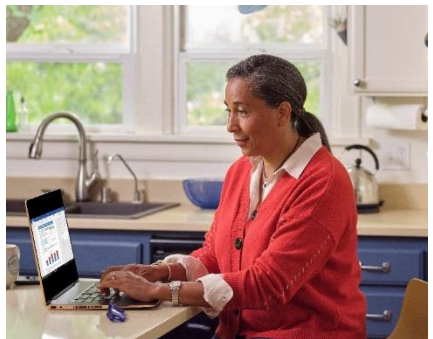
Camada de segurança baseada em software que impõe uma lista explicita de softwares que podem ser executados em um computador.

Microsoft 365 Defender

Microsoft 365 Defender é um **pacote de defesa empresarial pré e pós-violação** unificado que coordena de forma nativa a detecção, a prevenção, a investigação e a resposta entre pontos de extremidade, identidades, e-mail e aplicativos para fornecer proteção integrada contra ataques sofisticados.

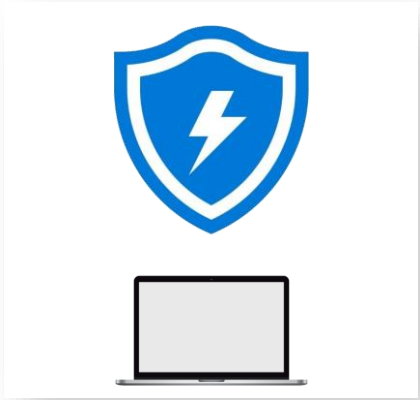
A seguir, você aprenderá a proteger sua organização com Microsoft 365 Defender



Serviços do Microsoft 365 Defender

Pacote de defesa empresarial



Microsoft Defender for Endpoint

Proteção preventiva, detecção pós-violação, investigação automatizada e resposta para dispositivos endpoint: Notebooks, Desktops e dispositivos móveis.

Microsoft Defender for O365

Protege sua organização contra ameaças recebidas através de canais de comunicação como: mensagens de email, links (URLs) e ferramentas de colaboração.

Microsoft Defender for Identity

Identifica, detecta e investiga ameaças avançadas, identidades comprometidas e ações internas mal-intencionadas direcionadas à sua organização.

Microsoft Defender Cloud Apps

Fornece visibilidade avançada, controle sobre a viagem de dados e análises sofisticadas para identificar e combater ameaças cibernéticas em todos os seus serviços de nuvem da Microsoft e de terceiros.

Microsoft Defender for Endpoint

Proteção para dispositivos que previne, detecta, investiga responde a ameças avançadas.

Gerenciamento de ameaças e vulnerabilidades

Essa funcionalidade interna usa uma abordagem baseada em risco que muda o jogo para a descoberta, priorização e correção de vulnerabilidades de ponto de extremidade e configurações incorretas.

Redução de superficie de ataque

Conjunto de recursos que inclui proteção de rede e proteção na Web, que regulam o acesso a endereços IP, domínios e URLs mal-intencionados. Mitiga exploração de vulnerabilidades em sem ambiente.

Proteção de última seração

Para reforçar ainda mais o perímetro de segurança da sua rede, o Microsoft Defender for Endpoint usa a proteção de última geração projetada para capturar todos os tipos de ameaças emergentes.

Detecção e resposta

Os recursos de detecção e resposta de ponto de extremidade são colocados em vigor para detectar, investigar e responder a ameaças avançadas que podem ter passado dos dois primeiros pilares de segurança. Utilize a ferramenta de busca para detectar violações.

Investigação e correção automatizadas

Em conjunto com a capacidade de responder rapidamente a ataques avançados, o Microsoft Defender for Endpoint oferece recursos automáticos de investigação e correção que ajudam a reduzir o volume de alertas em minutos em escala.

Especialistas em Ameaças da Microsoft

serviço de busca de ameaças gerenciadas fornece busca proativa, priorização, contexto e informações adicionais que capacitam ainda mais o SOCs (Centros de operações de segurança) para identificar e responder a ameaças de maneira rápida e precisa.

Microsoft Defender for O365

Proteção dos canais de comunicação.

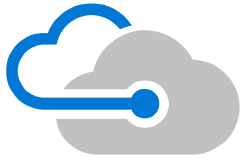
Previnir e Detectar

Proteção contra Phishing, SPAM e Malwares através de analise de links e anexos de e-mail, OneDrive, SharePoint e mensageria.

Utiliza de inteligência artificial e analise de comportamento para mitigar ameaças.

Investigar

Pesquise logs para auditorias e rastreamento de mensagens. Ferramenta completa de analise.



Responda

Limpeza automática e retroativa de mensagens mal-intencionadas de phishing, spam ou malware que já foram entregues para o usuário. Refina as listas de permissão e bloqueio para um nível de segurança elevado.

Microsoft Defender for Identity

Defenda-se contra ameaças de roubo e violação de identidade

Monitorar e traçar o perfil do comportamento e atividades do usuário

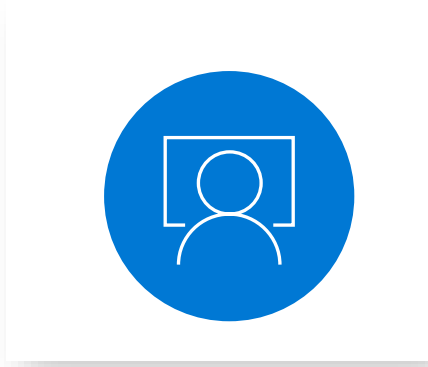
O defender for Identity monitora e analisa as atividades e informações do usuário em sua rede, incluindo permissões e membros do grupo, criando uma linha de base comportamental para cada usuário

Proteger as identidades dos usuários e reduzir a superficie de ataque

O Defender for Identity fornece insights sobre configurações de identidades e práticas recomendadas de segurança. Através de ´relatórios de securança e análise de perfil do usuário.

Identifique atividades suspeitas e ataques cibernéticos avançados

Melhora a detecção de ataques sofisticados. Tenha uma visão sobre credenciais comprometidas, movimentos de ataques laterais e ataques mais sofisticados que podem estar ocorrendo.

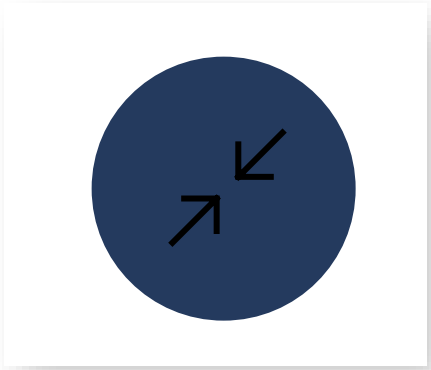


Investigue alertas e atividades do usuário

O Defender for Identity foi projetado para reduzir o ruído geral de alerta, fornecendo apenas alertas de segurança relevantes e em tempo real.

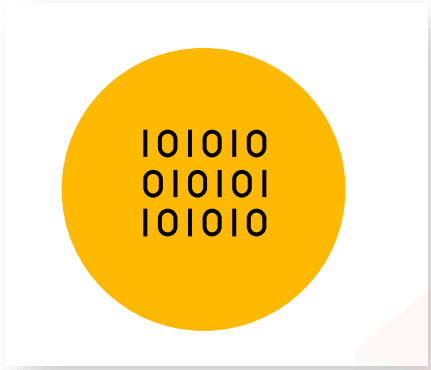
Microsoft Defender Cloud Apps

Visibilidade avançada e controle de viagem de dados de aplicativos em nuvem.



Descubra e controle o uso de Shadow IT

Identifique os aplicativos de nuvem, IaaS e PaaS usados por sua organização. Investigue os padrões de uso, avalie os níveis de risco e a preparação dos negócios de mais de 25.000 aplicativos SaaS em relação a mais de 80 riscos. Comece a gerenciá-los para garantir a segurança e a conformidade.

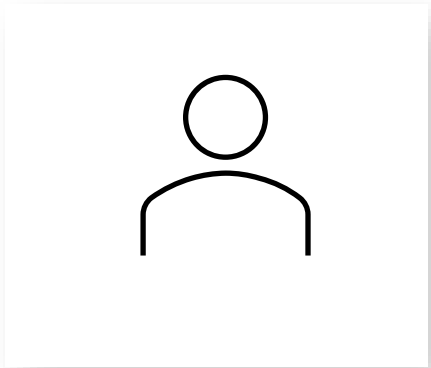


Proteja suas informações confidenciais em qualquer lugar na nuvem

Reconheça, classifique e proteja a exposição de informações confidenciais em repouso. Aproveite as políticas prontas para uso e os processos automatizados para aplicar controles em tempo real em todos os seus aplicativos na nuvem.

Proteja contra ameaças cibernéticas e anomalias

Detecte comportamento incomum em aplicativos de nuvem para identificar ransomware, usuários comprometidos ou aplicativos não autorizados, analise o uso de alto risco e faça correções automaticamente para limitar o risco à sua organização.



Avalie a conformidade de seus aplicativos na nuvem

Avalie se os seus aplicativos na nuvem atendem aos requisitos de conformidade relevantes, incluindo conformidade regulamentar e padrões do setor. Evite vazamentos de dados para aplicativos não compatíveis e limite o acesso a dados regulamentados.

Dicas de segurança

1

Segurança como cultura organizacional

Quando os funcionários entendem seu papel nas estratégias de segurança, os riscos são minimizados.

Trabalhe a capacitação dos usuários, para que possam identificar e mitigar ameaças.

2

Seja proativo, não reativo

Aplique hoje as medidas de segurança para elevar a segurança da organização.

Recursos como o MFA estão incluídos em todas as ofertas do Microsoft 365. Acesse o Microsoft Secure Score e tenha recomendações de melhorias de segurança conforme seu licenciamento atual do Microsoft 365.

3

Proteja os e-mails

E-mails de phishing estão cada vez mais comuns e sofisticados. Utilize o Microsoft Defender para Office 365 para proteger a organização de ataques sofisticados por anexo e links.

Aplique fluxo de mensagens, bloqueando o encaminhamento automático de mensagens, e consequentemente a evasão de dados.

4

Proteja-se contra softwares maliciosos

Ataques Ransomware costumam causar grande impacto financeiro e operacional nas empresas.

Habilite o Microsoft Defender para Endpoint para acesso controlado a pastas, e acrescente uma cama extra de proteção para softwares maliciosos como Ransomwares.

5

Investigue

Utilize as ferramentas de auditoria e logs do Microsoft 365 e tenha uma visão 360° do seu ambiente e como os dados são tratados.

Essa ação garante a melhoria continua e minimiza riscos.

Microsoft Security

Obrigado.

scansource

Solicite apoio a um especialista de segurança Microsoft

microsoftcsp@scansource.com