



**Revenda Autorizada e
Paceiro de Serviços Esy e
Safetica**

safetica ONE

Enterprise DLP e Proteção contra ameaças internas

Protege seus dados e oferece suporte à eficiência operacional, evitando erros humanos e atos maliciosos.

- ✓ **All-in-one** contra perda de dados e proteção contra ameaças internas
- ✓ **O mais fácil de implementar e integrar** Enterprise DLP
- ✓ **Controle avançado do espaço de trabalho** e análise de comportamento
- ✓ **Requisitos de hardware muito baixos** para servidores e dispositivos

Protegendo seus dados enquanto dá suporte à eficiência operacional

Safetica ONE é uma solução de segurança de dados All-in-One projetada para escalabilidade e necessidades de pequenas e médias empresas. Tenha seus dados valiosos sob controle com ótimo tempo de retorno. Vá além da prevenção de perda de dados com uma análise holística do comportamento para detectar ameaças internas e responder antes mesmo que se transformem em incidentes. Aproveite os insights sobre o espaço de trabalho da empresa, ativos digitais e operações para otimizar custos.



Pessoas e dados são o combustível para as empresas modernas.

Quando dados confidenciais são perdidos ou roubados, a reputação, a vantagem competitiva e a lucratividade de uma empresa sofrem.

O custo médio de uma violação de dados é **\$4.24 milhões**.*

60% das pequenas empresas **fecham em até 6 meses** após uma grande violação de dados.**

*2021 Cost of Data Breach Report, Ponemon Institute; ** National Cyber Security Alliance, October 2012

Toda organização **pode proteger seus dados**

A segurança interna nunca foi tão fácil. Ajudamos você a proteger seus dados, orientar seu pessoal e apoiar a conformidade comercial. O Safetica ONE evita violações de dados e facilita o cumprimento das regulamentações de proteção de dados, protegendo sua empresa contra erros humanos ou comportamentos maliciosos.

DLP empresarial fácil de implementar e integrar

De acordo com o Relatório do Quadrante de Dados DLP de 2021 da SoftwareReviews, o Safetica ONE se destaca e lidera em facilidade de implementação e integração.

Controle avançado do espaço de trabalho e análise de comportamento

Obtenha controle sobre o hardware e o software para otimizar os custos. Com um módulo extra, você também pode obter informações detalhadas sobre o comportamento arriscado do usuário e alterações no espaço de trabalho.

Requisitos de hardware muito baixos

O Safetica ONE pode ser implantado em servidores disponíveis sem comprar hardware adicional. O Safetica Client tem um impacto abaixo de 3% no desempenho dos dispositivos.

Principais cenários de casos de uso

Classificação de dados e auditoria de fluxo de dados

Safetica ONE ajuda você a descobrir e classificar os dados valiosos de uma empresa com base na inspeção de conteúdo, contexto e propriedades do arquivo. Ele audita todas as atividades de dados confidenciais, independentemente de onde os dados são armazenados ou movidos, para que você possa relatar e investigar onde há risco de vazamento ou roubo. Essas descobertas são fundamentais para a proteção de dados.

Propriedade intelectual e proteção de dados confidenciais

Com Safetica ONE, você pode proteger dados confidenciais relacionados a negócios, clientes, códigos-fonte ou projetos contra vazamentos acidentais ou intencionais. As notificações sobre como tratar dados confidenciais podem ajudar a aumentar a conscientização sobre segurança de dados e educar os funcionários.

Detecção e resposta as ameaças internas

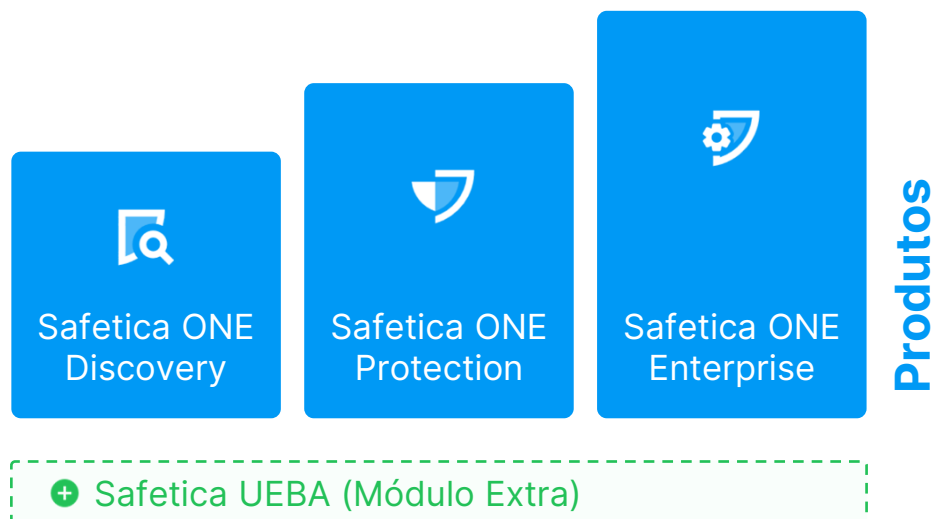
Qualquer um pode cometer um erro que pode colocar seu negócio em risco. Com Safetica ONE, você pode analisar riscos internos, detectar ameaças e mitigá-las rapidamente. Controle seu espaço de trabalho digital híbrido, descubra software e hardware indesejados, analise o comportamento para detectar e auditar funcionários de alto risco.

Detecção e mitigação de violação de conformidade regulatória

Safetica ONE ajuda você a detectar, prevenir e mitigar violações regulatórias. Seus recursos de auditoria suportam a investigação de incidentes para cumprir os regulamentos e padrões de proteção de dados como GDPR, LGPD, HIPAA, SOX, PCI-DSS, GLBA, ISO/IEC 27001 ou CCPA.

Safetica ONE protege:

- Dados pessoais
- Documentos estratégicos da empresa
- Bancos de dados de clientes
- Dados relacionados ao pagamento, como números de cartão de crédito
- Propriedade intelectual – desenhos industriais, segredos comerciais e know-how
- Contratos



Referência de Arquitetura



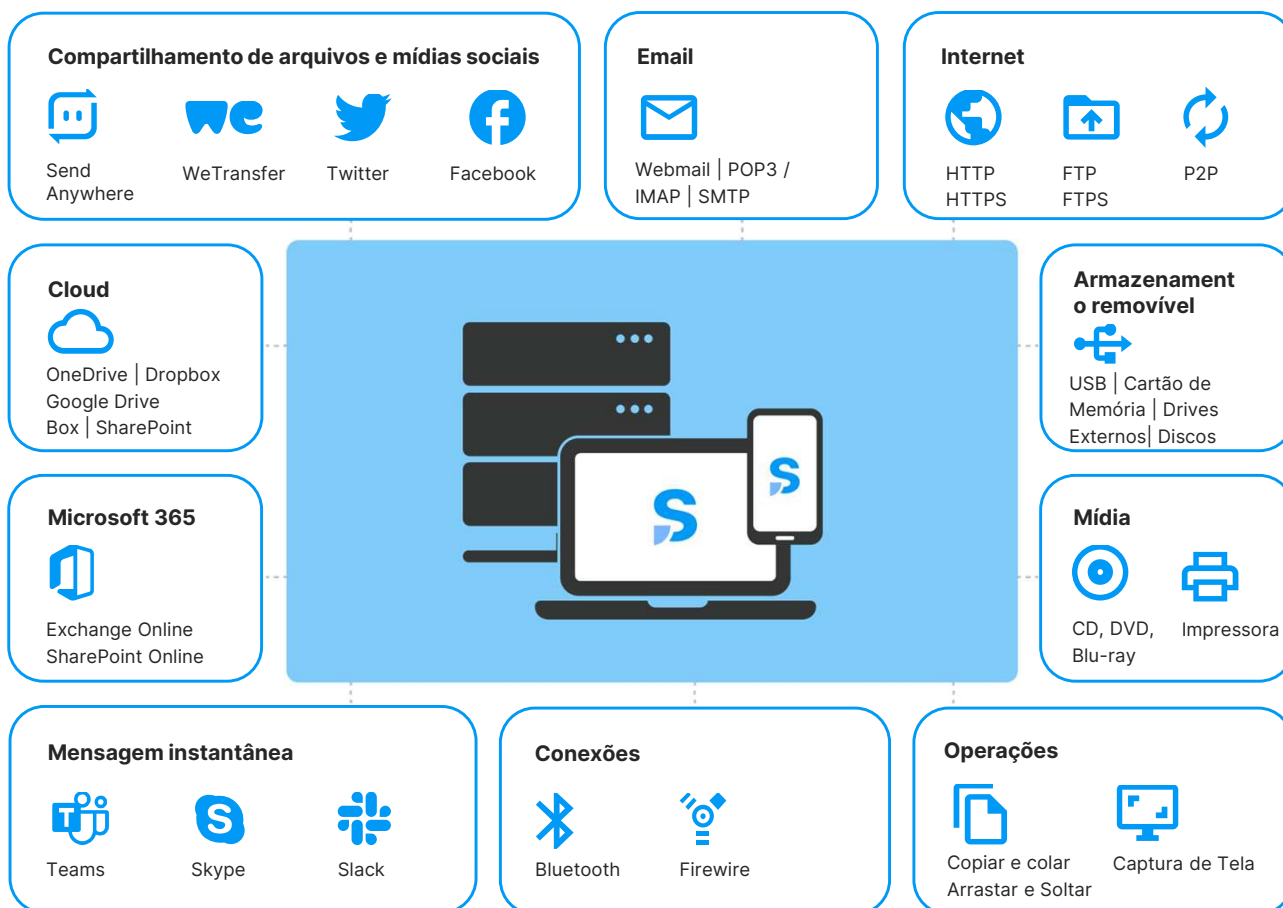
O servidor físico ou virtual executa um banco de dados com atividades do endpoint e registros de segurança. O Safetica Management Console permite que os administradores gerenciem políticas de segurança e exibam as informações coletadas.

Todas as ações são registradas e as políticas de segurança são aplicadas em desktops, laptops e outros dispositivos remotos ou mesmo offline com um Safetica Client.

Os dados confidenciais são protegidos em todos os canais.

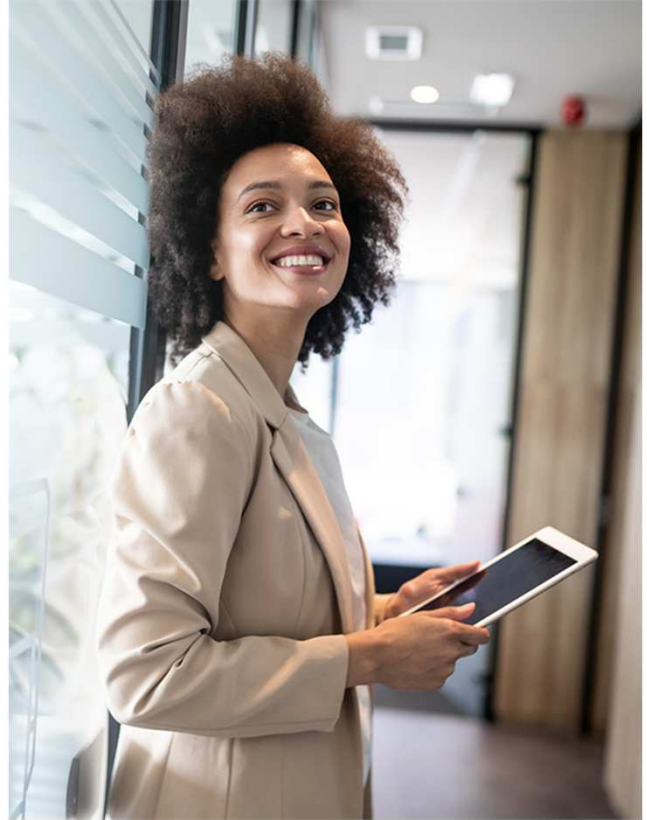
Plataforma de dados cobertos

A Safetica mantém os dados protegidos em vários canais e plataformas, garantindo que seus dados estejam seguros onde quer que residam ou passem.



Benefícios do Discovery

Safetica ONE Discovery audita e classifica todos os fluxos de dados em sua organização. Ele identifica informações confidenciais e riscos de segurança usando inspeção de conteúdo com OCR. Obtenha uma visão geral rápida do que está acontecendo em seu espaço de trabalho em tempo real. Compreenda melhor todas as atividades internas, processos e riscos de dados para melhorar a segurança de seus dados e eficiência interna.



Obtenha insights sobre incidentes de segurança de dados e [violações de conformidade regulatória](#) para poder responder e mitigar seus impactos



[Audite e classifique](#) seus fluxos de dados confidenciais em qualquer canal ou atividade para descobrir onde seus dados estão em risco de perda



Obtenha [notificações instantâneas](#) e [relatórios de gerenciamento](#) com avaliação de nível de risco de fácil leitura e visão geral de incidentes



[Descubra e remova](#) softwares indesejados ou desnecessários, serviços em nuvem ou hardware / periféricos



[Solução fácil de implantar](#) com integração de um clique com o [Microsoft 365](#) que respeita os processos estabelecidos e fornece os relatórios dentro de alguns dias

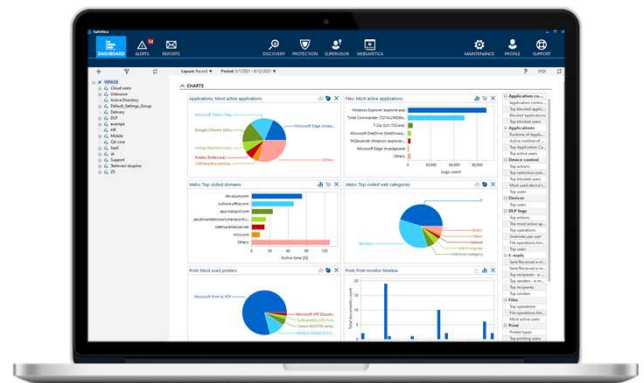


Analise objetivamente as [atividades do usuário](#) em seu ambiente e determine se o [equipamento e a rede da empresa](#) são usados de maneira adequada

Principais destaques

Identifique como os dados da empresa são usados e para onde são armazenados e enviados, independentemente de onde residam.

- ✔ Suporte para Windows e macOS
- ✔ Integração com Microsoft 365 em Um Clique
- ✔ Classificação e Inspeção de Conteúdo de Arquivos
- ✔ Fácil de atualizar para a plataforma com recursos completos
- ✔ É executado em bare metal ou Ambiente Virtualizado e em VM hospedado na nuvem



Console do Safetica Management para Safetica ONE Discovery fornece uma visão profunda de todas as operações de arquivos gravados com diferentes visualizações para fácil interpretação.

Benefícios do Protection

Safetica ONE Protection identifica riscos, educa seus funcionários e evita erros e atos maliciosos das pessoas para proteger seus dados. A combinação de análise de dados, classificação de dados e prevenção contra perda de dados (DLP) com proteção contra ameaças internas cria um ambiente seguro enquanto mantém operações de negócios eficientes.



Tenha **controle sobre os fluxos de dados** **confidenciais** e **riscos internos** com base na análise de comportamento e inspeção de conteúdo



Obtenha **relatórios de segurança** regulares e **notificações de incidentes** em tempo real



Use **Safetica Zones** para simplificar a segurança de dados de alto nível



Crie uma **cópia** dos dados que vazam para manter as evidências forenses para uma investigação mais aprofundada

Defina políticas claras para todos os usuários e canais de dados

Configure políticas de segurança para grupos ou indivíduos específicos. Selecione o fluxo de trabalho desejado com ações configuráveis de auditoria silenciosa, por meio de notificações de usuário para bloqueio estrito.

Detecte ameaças potenciais e análise os riscos

Responda às ameaças antes mesmo que um grande incidente aconteça, graças à descoberta precoce de anomalias de comportamento e riscos de fluxo de dados em sua organização. Safetica ONE usa classificação avançada de conteúdo e OCR para detecção de dados confidenciais em arquivos de imagem e documentos PDF digitalizados

Principais destaques

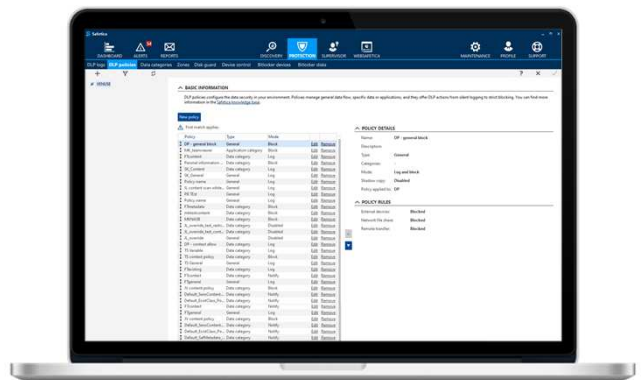
Com base na inspeção de conteúdo, análise de risco interno e políticas claras definidas para todos os canais de dados, Safetica ONE Protection pode reconhecer quando alguém comete um erro ou se arrisca com seus dados confidenciais. Dependendo do modo em que o Safetica ONE está operando, ele pode bloquear a atividade de risco, notificar o administrador ou lembrar o funcionário sobre as diretrizes de segurança da organização.

Capacite os funcionários a trabalhar com dados confidenciais

Exiba notificações educacionais para os funcionários quando houver risco de violação da política para que eles saibam ou decidam. Aplique processos específicos para proteger os dados mais valiosos.

Tenha todos os dispositivos sob controle, online e offline

Restrinja o uso de periféricos portáteis ou mídia não autorizada. Controle os dispositivos corporativos e controle os dados que saem do Microsoft 365. O Safetica permanece totalmente ativo, independentemente da conexão de rede. Todos os registros coletados são sincronizados quando a conexão é restaurada.



Safetica Management Console permite a configuração detalhada de políticas DLP, categorias de dados ou relatórios.

Benefícios do Enterprise

Safetica ONE Enterprise estende a prevenção contra perda de dados e proteção contra ameaças internas por meio de controle de fluxo de trabalho adicional, automação e integração perfeita com soluções de segurança de rede de terceiros, SIEMs e ferramentas de análise de dados.



Integração automatizada de terceiros e recursos para casos de uso avançados.



Políticas para controle de fluxo de trabalho em terminais da empresa



Suporte para Active Directory em ambientes de multi-domínios



Marca personalizada de notificações de segurança no End Point

Integrações perfeitas

A automação de políticas de segurança e a integração com sua equipe de TI ajudam a proteger seus ativos, mesmo em ambientes complexos.

A integração nativa com dispositivos de rede [Microsoft 365](#) ou [Fortinet](#) oferece controle estendido sobre dispositivos desconhecidos e cria uma solução robusta de segurança de end point para rede.

Todos os incidentes e logs auditados podem ser enviados automaticamente para soluções SIEM, por exemplo, [Splunk](#), [IBM QRadar](#), [LogRhythm](#) ou [ArcSight](#) para investigação posterior. A API REST fornece dados coletados para ferramentas como [Power BI](#) ou [Tableau](#) para análise avançada.

Controle poderoso de fluxo de trabalho

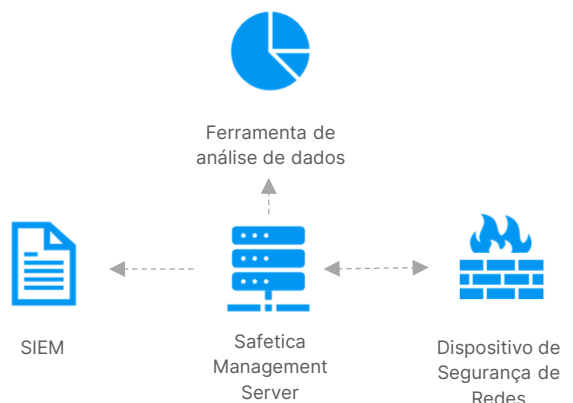
O conjunto de recursos de controle permite definir como os usuários podem trabalhar, independentemente dos dados envolvidos.

Com o controle do fluxo de trabalho, você pode impor um processo seguro específico e bloquear todas as outras formas de executar uma ação.

O controle de fluxo de trabalho inclui [políticas de DLP](#) de aplicativos para gerenciar o comportamento de vários tipos de aplicativos como CRM ou IM e regras de [política de DLP](#) com configurações personalizadas aplicadas a diferentes redes, caminhos locais ou acesso exclusivo para usuários com privilégios.

Principais destaques

- ✓ Suporte para Windows e macOS
- ✓ Integração de um clique com Microsoft 365
- ✓ Integração de dispositivos de rede Fortinet
- ✓ Integração de API com Power BI ou Tableau
- ✓ Notificações imediatas entregues em seu e-mail
- ✓ Inspeção de conteúdo de arquivo com modelos pré-definidos
- ✓ Classificação de conteúdo com base em várias abordagens



Benefícios do Módulo UEBA

Conhecimento é a primeira e mais importante etapa para entender o fluxo de trabalho da sua empresa, os hábitos de trabalho dos funcionários e a produtividade. Enriqueça qualquer produto Safetica ONE com o módulo User and Entity Behavior Analytics para ver as atividades do usuário em detalhes e descobrir suas anomalias de comportamento.



Reconhecer atividades indesejáveis do usuário

Com auditoria de atividades de trabalho e rotulagem e categorização automatizadas de aplicativos usados e sites visitados por usuários específicos



Obtenha informações mais detalhadas sobre a comunicação por e-mail

Com registros de todos os e-mails recebidos e enviados em relação à privacidade do funcionário



Rastreie as mudanças no comportamento do usuário

Com visão geral e visualização de tendências e mudanças no comportamento do usuário em sua rede ao longo do tempo



Audite o uso de recursos

Para obter uma visão geral e precisa se as licenças de hardware e software adquiridas são distribuídas e usadas de forma eficiente



Obtenha relatórios abrangentes e alertas em tempo real

Sobre as atividades individuais do usuário, mesmo quando estiver trabalhando remotamente



Auditoria de pesquisas de emprego

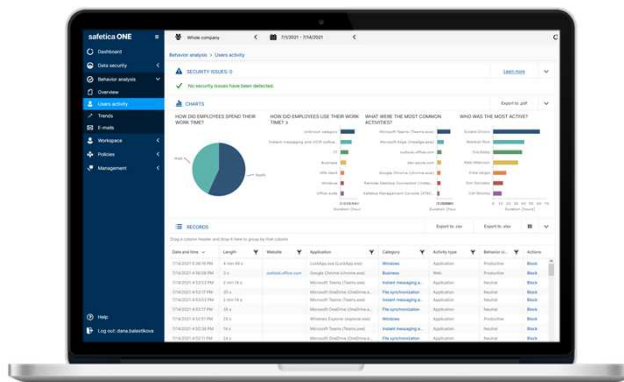
Para identificar portais de empregos visitados por usuários específicos, que podem representar um risco futuro de segurança de dados

Identificação de anomalias raiz dos problemas

Aprofunde-se e identifique os elementos problemáticos em seu ambiente para tratar de questões de segurança ou eficiência empresarial. Análise objetivamente as atividades relacionadas ao trabalho de funcionários individuais com informações detalhadas. Descubra se alguém visita sites perigosos ou usa aplicativos indesejáveis.

Transparência no trabalho

Permita que a alta administração e os líderes de departamento vejam como funcionam seus relatórios individuais. Fique por dentro de tudo, mesmo quando seus funcionários trabalham em casa ou precisem de mobilidade. Evite riscos de segurança e gerencie a eficiência dos funcionários, identificando trabalhadores ociosos, procura de emprego e padrões de comportamento suspeitos.



WebSafetica fornece uma visão geral e fácil de entender todas as ameaças possíveis. Obtenha estatísticas importantes no painel, configure visualizações personalizadas.

Lista de Recursos I

| Compatible com Windows, macOS, Microsoft 365 | Safetica ONE Discovery | Safetica ONE Protection | Safetica ONE Enterprise |
|---|---------------------------|----------------------------|----------------------------|
| Auditoria de Segurança | ✓ | ✓ | ✓ |
| Auditoria de segurança de fluxo de dados Auditoria de segurança do fluxo de dados em todos os canais, incluindo dispositivos externos, upload da web, e-mail, mensagens instantâneas, impressão e unidades de nuvem. | ✓ | ✓ | ✓ |
| Arquivo do Office 365 e auditoria de e-mail Auditoria de operações de arquivo e comunicação de e-mail de saída no Office 365. | ✓ | ✓ | ✓ |
| Auditoria de conformidade regulatória Descubra violações dos regulamentos mais comuns, como PCI-DSS, GDPR ou HIPAA em todas as variações regionais. | ✓ | ✓ | ✓ |
| Auditoria de segurança do espaço de trabalho Auditar o uso de dispositivos, aplicativos, redes e impressão da empresa. Descubra recursos não utilizados ou mal utilizados para manter o espaço de trabalho, garantir a retenção e reduzir custos. | ✓ | ✓ | ✓ |
| Inspeção de conteúdo Classifique arquivos e e-mails confidenciais por meio de inspeção de conteúdo poderosa com modelos pré-definidos ou regras e dicionários personalizados. | ✓ | ✓ | ✓ |
| Deteção de atividades suspeitas Reaja rapidamente graças à deteção em tempo real de atividades suspeitas e alertas imediatos por e-mail. | ✓ | ✓ | ✓ |
| Endpoint Data Protection | ✗ | ✓ | ✓ |
| Proteção de e-mail e rede Proteção de dados para e-mail, upload da web, mensagens instantâneas e compartilhamentos de rede. | ✗ | ✓ | ✓ |
| Dispositivos e proteção de impressão Gerencie o fluxo de dados para dispositivos externos e proteja dados confidenciais contra impressão proibida em impressoras locais, de rede ou virtuais. | ✗ | ✓ | ✓ |
| Proteção de trabalho remoto Evite vazamentos de dados em terminais remotos ou conexões de área de trabalho remota. Oferece suporte a uma ampla variedade de soluções de acesso remoto. | ✗ | ✓ | ✓ |
| Classificação de dados avançada Use tecnologias avançadas para detectar e rotular dados confidenciais com base na origem, contexto do fluxo de trabalho ou tipo de arquivo. Aproveite a deteção de metadados para usar classificações de terceiros. Permitir que os próprios usuários classifiquem os arquivos. | ✗ | ✓ | ✓ |
| Diferentes políticas de remediação Reaja com flexibilidade aos incidentes detectados para capacitar e educar seus funcionários. Os incidentes podem ser registrados, bloqueados ou justificados / bloqueados com substituição. | ✗ | ✓ | ✓ |
| Cópia da evidência do incidente Mantenha evidências forenses de incidentes criando cópias de evidências dos dados que vazam. As cópias das evidências são totalmente criptografadas e podem ser mantidas em computadores locais com uma política de retenção. | ✗ | ✓ | ✓ |

Lista de Recursos II

| Compatível com Windows, macOS, Microsoft 365 | Safetica ONE Discovery | Safetica ONE Protection | Safetica ONE Enterprise |
|--|---------------------------|----------------------------|----------------------------|
| Endpoint Data Protection | × | ✓ | ✓ |
| Controle do espaço de trabalho Defina seu espaço de trabalho seguro e reduza o perímetro por aplicativo e controle do site. Evite comportamentos indesejáveis em sua empresa e reduza os custos de gerenciamento de segurança. | × | ✓ | ✓ |
| Safetica Zones Fácil gerenciamento do perímetro de dados seguro com Safetica Zones exclusivas, que reduzem significativamente o número de políticas de proteção de dados. | × | ✓ | ✓ |
| Gerenciamento de criptografia BitLocker Gerenciamento centralizado de unidades locais e dispositivos externos com criptografia BitLocker. | × | ✓ | ✓ |
| Proteção de dados na nuvem | × | ✓ | ✓ |
| Proteção de sincronização de nuvem de end point Proteção de dados para unidades de nuvem em end points, por exemplo, OneDrive, Google Drive, Dropbox, Box, etc. | × | ✓ | ✓ |
| Proteção do End point Microsoft 365 Proteção de dados para Microsoft 365 e SharePoint de terminais. Evite compartilhar ou enviar dados que você deseja manter longe da nuvem. | × | ✓ | ✓ |
| Proteção de informações do Azure Detecção de classificações de dados do Microsoft Azure Information Protection, mesmo em formato criptografado. | × | ✓ | ✓ |
| Proteção Exchange Online Unifique as políticas de e-mail entre end points e e-mail na nuvem. Gerenciar e filtrar dados de saída de pontos de extremidade e do Exchange Online. | × | ✓ | ✓ |
| Recursos da empresa | × | × | ✓ |
| Branding de notificações Marca personalizada de notificação do usuário final (logotipo). | × | × | ✓ |
| Controle de fluxo de trabalho Políticas de aplicativos e configurações de políticas de especialistas para alinhar o fluxo de trabalho do terminal com os processos da empresa. | × | × | ✓ |
| Suporte multi-domínio Suporte corporativo de vários domínios para Active Directory. | × | × | ✓ |
| Automação de Segurança | × | × | ✓ |
| Integração SIEM Relatório automatizado de incidentes para soluções SIEM (Splunk, QRadar, LogRhythm, ArcSight, etc.). | × | × | ✓ |
| Integração FortiGate Integração de segurança automatizada com dispositivos de rede FortiGate para criar uma solução de segurança end point-to-network robusta. | × | × | ✓ |
| API de relatórios API para relatar dados Safetica para serviços de análise e visualização. | × | × | ✓ |

Especificações Técnicas

Servidor

- Processador quad-core de 2,4 GHz
- 8 GB de RAM e mais
- 100 GB de espaço disponível em disco
- Um servidor compartilhado ou dedicado, suporte de máquinas virtuais e hospedagem em nuvem
- Requer conexão ao servidor com MS SQL 2012 e superior ou Azure SQL
- MS Windows Server 2012 e superior (64 bits)

Base de dados

- MS SQL Server 2012 e superior, ou MS SQL Express 2016 e superior, ou Azure SQL.
- MS SQL Express é parte de um instalador universal e recomendado para até 200 end points protegidos.
- 200 GB de espaço em disco disponível (idealmente 500 GB ou mais, dependendo da faixa de dados coletados).
- Um servidor compartilhado ou dedicado, suporte de máquinas virtuais e hospedagem em nuvem. Ele pode ser hospedado junto com o servidor Safetica.

Cliente Windows

- Processador dual-core de 2,4 GHz, 2 GB de RAM e mais
- 10 GB de espaço disponível em disco
- MS Windows 7, 8.1, 10, 11 (32 bits [x86] ou 64 bits [x64])
- Pacote de instalação MSI
- .NET 4.7.2 e superior

cliente macOS

- Processador quad-core de 2,4 GHz, 2 GB de RAM e mais
- 10 GB de espaço disponível em disco
- macOS 10.10 e superior (para conjunto completo de recursos DLP, recomendo 10.15 e superior).

Provedores de nuvem com suporte

- Microsoft Azure, Microsoft 365

Certificações Selecionadas

- ISO 9001 e ISO / IEC 27001
- Membro do Cybersecurity Tech Accord
- Microsoft Gold Partner
- Membro da ESET Technology Alliance
- Membro da Fortinet Technology Alliance
- Parceiro Tecnológico Netwrix



500 000⁺
dispositivos protegidos

120⁺
países

90⁺
Embaixadores de
segurança

Quem somos nós

Safetica é uma empresa de software Tcheca que fornece soluções de prevenção contra perda de dados e proteção contra ameaças internas para organizações de todas as formas e tamanhos. Aqui na Safetica, acreditamos que todos merecem saber que seus dados estão seguros.

Alianças de tecnologia



Prêmios e conquistas



THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

FORRESTER

Gartner



Excelente
Proteção de Dados,
Fácil de Usar



@safetica

Experimente a demonstração da Safetica!
www.safetica.com/demo

safetica

Contato

Phone: +55 11 5461-1374

Email: contato@osait.com.br

Website: <https://osait.com.br>

Rua Flórida, 1703 – CJ. 62 - Cidade Monções – São Paulo – SP.



Excelente
Proteção de Dados,
Fácil de Usar



Experimente a demonstração da Safetica!
www.safetica.com/demo

safetica