

# Kaspersky Endpoint Security Cloud

kaspersky

---

Proteção direta, aonde  
quer que você vá

---

## Ilusão perigosa

### Gestores de PMEs acreditam:

"Somos muito pequenos para sermos um alvo para cibercriminosos"



### A realidade:

**57%**

das violações foram realizadas por atores externos<sup>1</sup>

**US\$ 105 mil**

O custo das violações de dados para PMEs<sup>2</sup>

**60%**

das pequenas e médias empresas hackeadas encerram as atividades em até seis meses<sup>3</sup>

### Estou sobrecarregado com tanto trabalho

**44%**

das empresas afirmam que gerenciar ambientes complexos é uma de suas principais preocupações de cibersegurança<sup>1</sup>

### Meus recursos e orçamento são apertados

Organizações de menor porte podem não ter orçamento para bancar defesas adicionais de malware para além de AV de desktop.



### Nossa força de trabalho remota representa alto risco à segurança

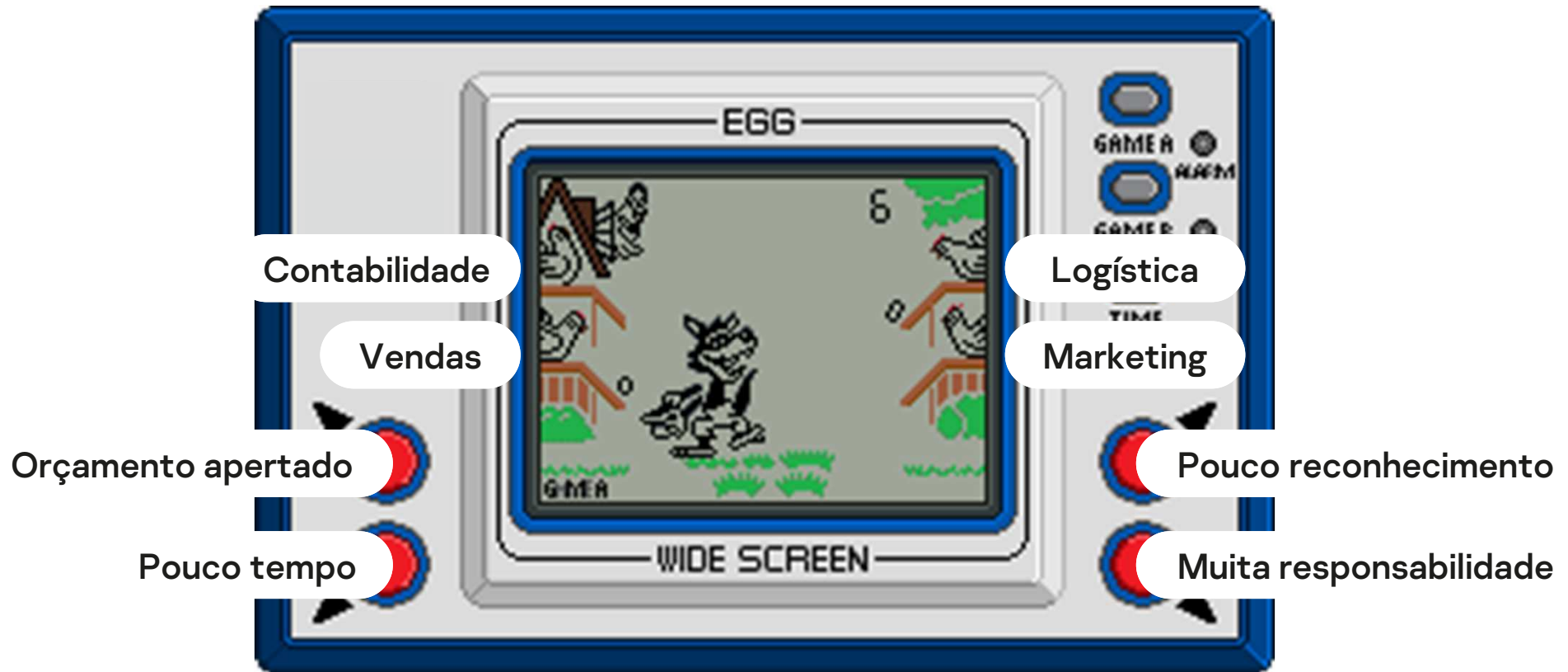
**64%**

das PMEs permitem que seus funcionários trabalhem de locais fora do escritório regularmente<sup>2</sup>

**40%**

das organizações afirmam que a falta de mão de obra técnica capacitada é um dos 3 principais desafios para a proteção contra incidentes complexos<sup>3</sup>

Um dia típico na administração de TI é assim...



# Permitiremos que você:

## Proteger dispositivos

De forma rápida e de qualquer lugar

## Tenha mais tempo para as tarefas de negócios

Graças à automação de tarefas de rotina

## Habilite uma força de trabalho móvel segura

Com proteção para dispositivos móveis incluída

## Agregue valor ao negócio digital ágil

Controlando e protegendo seus serviços na nuvem

## Desfrute de tranquilidade

À medida que você combate ameaças evasivas e constroi suas habilidades de cibersegurança.

## Proteção direta para sua empresa - aonde quer que você vá



### Uma única solução de segurança para todas as necessidades de TI

- Desktops e laptops Windows e Mac
- Servidores de arquivos Windows
- Smartphones e tablets Android e iOS
- Microsoft Office 365



### Protegendo a força de trabalho remota, onde quer que eles estejam

- Esteja em todos os lugares e proteja qualquer pessoa usando [cloud.kaspersky.com](https://cloud.kaspersky.com)
- Corrija e criptografe dispositivos remotamente

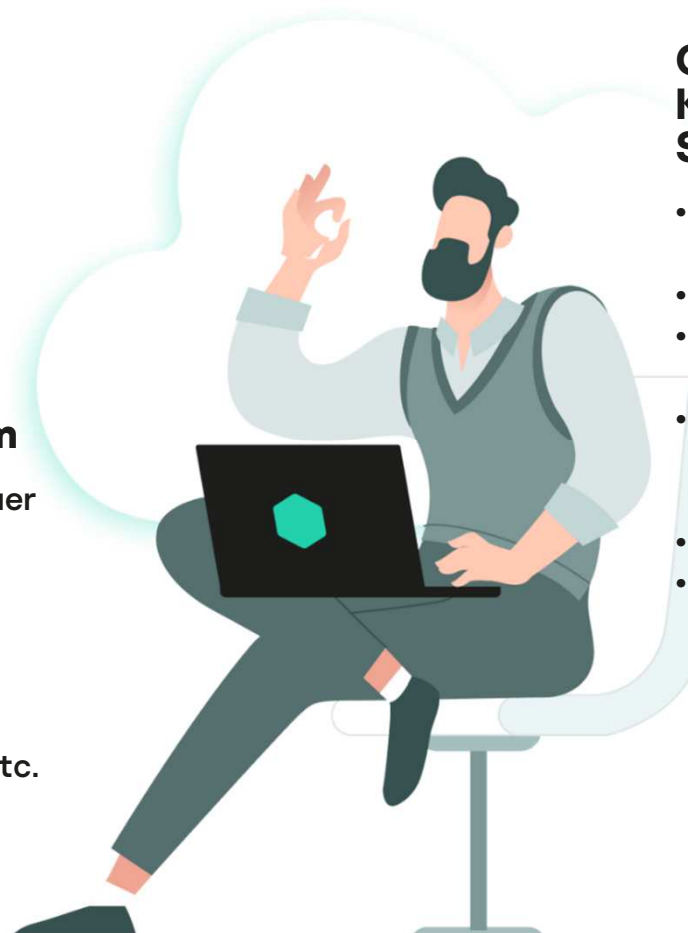


### Assuma o controle da nuvem

- Bloqueie a Shadow IT: SaaS, redes sociais etc.
- Proteja o ambiente de colaboração do MS Office 365

### Compromissos do Kaspersky Endpoint Security Cloud:

- Tempo mais rápido para proteção
- Sem investimento de capital
- Sem 'remendar sextas-feiras'
- Nenhum conjunto de habilidades avançado necessário
- Recursos reimplementados
- Mais tempo para tarefas vitais para os negócios



Solução pronta para usar

7

Tudo o que você precisa é de um navegador e uma conexão com a internet

Inscreva-se em  
[cloud.kaspersky.com](https://cloud.kaspersky.com)

Adicione dispositivos  
a serem protegidos

Gerencie gastando só  
15 minutos (aprox.) semanalmente



Crie uma  
conta no  
[cloud.kaspersky.com](https://cloud.kaspersky.com)

Crie um espaço de trabalho\* e  
implemente software de  
endpoint.

Uma política padrão é aplicada  
automaticamente a todos os  
dispositivos conectados.

**E pronto!**  
**Os usuários**  
**estão**  
**protegidos**

Gerencie  
gastando só  
15 minutos  
(aprox.)  
semanalmente

## Recursos avançados para proteção e gerenciamento de endpoints

8



### Proteção

- Proteção contra ameaças de arquivo, e-mail e web, malware conhecidos, desconhecidos e avançados
- Prevenção contra ransomware e exploits
- Detecção de comportamento e mecanismo de neutralização
- Controle adaptativo de anomalias **novo**
- Firewall e bloqueador de ataques de rede
- Avaliação de vulnerabilidades
- Prevenção de ataques Bad USB **novo**
- Detecção e Resposta de Endpoints **novo**



### Gerenciamento de segurança e controle

- Cloud Discovery
- Proteção para o Microsoft Office 365
- Data Discovery
- Controle da Web
- Controle de dispositivos
- Controle de Aplicativos **novo**
- Gerenciamento de patches
- Gerenciamento de criptografia (Windows BitLocker, macOS FileVault)



### Segurança móvel

- Antivírus móvel
- Gerenciamento de senhas
- Controle de recursos e da Web
- Recursos antirroubo



---

## Economize tempo em operações de rotina

### Gerenciamento de patches

- Visão geral dos aplicativos instalados em dispositivos
- Lista das correções disponíveis para atualizar os aplicativos para as versões mais recentes
- Atualizações remotas e agendamento: saiba que está usando apenas os produtos mais atuais e seguros.



### Gerenciamento da criptografia

- Recursos nativos do sistema operacional para proteger dispositivos remotos e ativos confidenciais
- Protege os dispositivos mesmo em caso de perda ou roubo



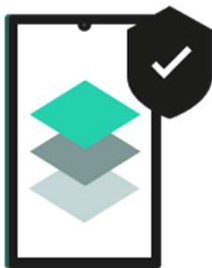
### Resposta a ameaças sem esforço

- Prevenção automática contra ameaças
- Reversão de atividades mal-intencionadas
- EDR automatizado



## Adquira o controle sobre dispositivos móveis não gerenciados

### Proteção antivírus e da Web para dispositivos móveis



- Proteção em tempo real contra ameaças, vírus e aplicativos maliciosos
- Bloqueia phishing e sites maliciosos

### Gerenciamento de senhas



- Aplicação de senha de desbloqueio de tela
- Suporta Face ID e Touch ID

### Mobilidade para o trabalho, não para a distração

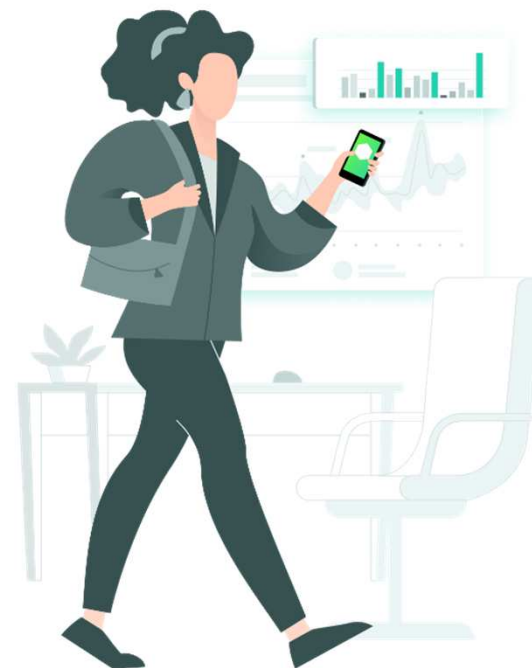


- Controle de aplicativos para Android
- Controle de recursos

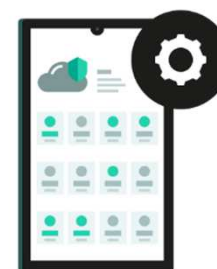
### Respostas automáticas contra roubo



- Bloqueie/desbloqueie dispositivos
- Ative um alarme sonoro
- Limpe dados



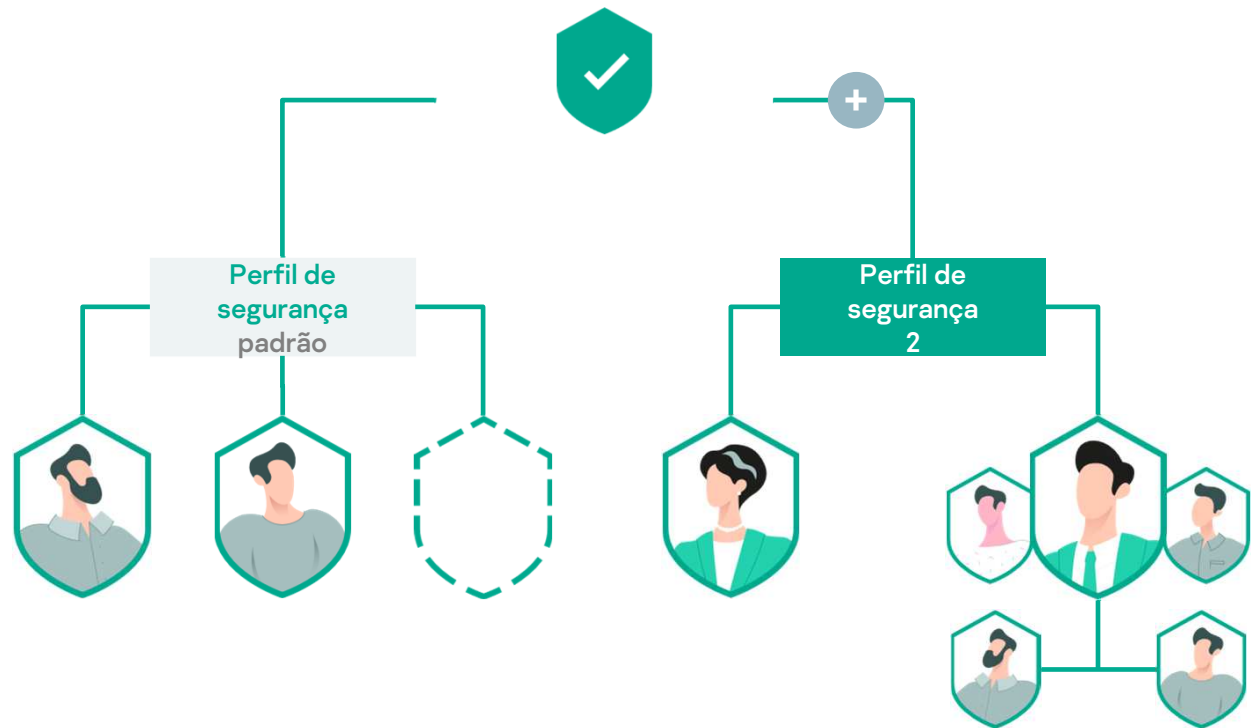
### Recursos poderosos para dispositivos iOS supervisionados



- Controle da Web
- Configurações de proxy
- Restrições de recursos (até 40 recursos)

## Perfis de segurança baseados em usuários


- Um único perfil de segurança é aplicado a todos os dispositivos em que o usuário trabalha
- Pronto para ser usado desde o início
- Perfis separados e personalizados para diferentes dispositivos e grupos de funcionários





# Relatórios rápidos



Companies Administrators Licenses

 **0**  
No devices with vulnerabilities

 **248**  
Devices safe (status OK)

 **48**  
Disinfected threats

## ^ Protection statistics about devices managed by Kaspersky Endpoint Security Cloud

Click a link to filter your workspaces.

### Devices by severity level of vulnerabilities

<a href="#">Critical</a>	0
<a href="#">High</a>	0
<a href="#">Warning</a>	0

### Protection status of devices

<a href="#">Critical</a>	0
<a href="#">Warning</a>	0
<a href="#">OK</a>	248

### Status of anti-virus database updates

<a href="#">More than a week ago</a>	0
<a href="#">1 to 7 days ago</a>	48
<a href="#">During last 24 hours</a>	200



# **Lidando com os desafios atuais**

---

## Shadow IT

14

---

É fácil para os funcionários usarem ferramentas de colaboração "não sancionadas"

---

O que pode criar problemas de compatibilidade e riscos de segurança, além de impactar a produtividade

---

TI deve conhecer o panorama global para determinar um plano de ação



---

O Cloud Discovery revela o panorama real para que você possa agir

15

### **Analise o uso do SaaS:**

- Painel – exibição estatística
- Relatório em PDF para CEO/HR



### **Entenda a situação:**

- Os funcionários não sabem quais são as ferramentas legítimas
- As ferramentas corporativas são inconvenientes e cheias de falhas
- Os usuários podem ignorar intencionalmente as políticas de segurança



### **Planeje e reaja:**

- Eduque os funcionários
- Bloqueie usuários/grupos
- Restrinja serviços/categorias particulares



☰

Kaspersky Endpoint Security Cloud  
**Cloud Plus GmbH**

---

① Information panel

👤 Users

📱 Devices

🔒 Security management ▼

🧪 Quarantine

📦 Distribution packages

⚙️ Settings

---

Privacy Policy
Legal Notice
Help
Support

© 2021 AO Kaspersky Lab

👤 Alexander.Korobko
▼

Admin

- Getting started
- Monitoring
- Reports
- Event log
- License

## Widgets

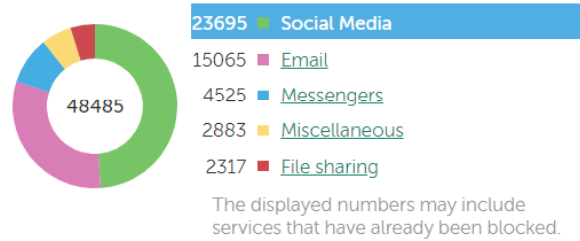
Each widget contains information about all managed devices. Unless otherwise specified, widgets show information for a period of not more than the last 30 days.

## Cloud Discovery

Monitor cloud services that are used most often on Windows devices and block access to cloud services that you consider unwanted.

Cannot find a cloud service that your company uses? [Let us know](#)

### Cloud Discovery information



### TOP 5 services

Usage	Service name	Risk level	Access
13375	<a href="#">Instagram</a>	Low	Allowed
6984	<a href="#">Facebook</a>	Low	Allowed
892	<a href="#">VKontakte</a>	Low	Allowed
726	<a href="#">Twitter</a>	Low	Allowed
502	<a href="#">Pinterest</a>	Low	Allowed

### TOP 10 service users

[Go to reports](#)

Access attempts	User alias	Device name	Service name	Security profile	Access
5234	<a href="#">Diana.Kanivets</a>	<a href="#">DESKTOP-KRK2C0C</a>	Facebook	<a href="#">Default profile</a>	✔ Allowed ▼
1742	<a href="#">Andrey</a>	<a href="#">AKOR-ΠΚ</a>	Facebook	<a href="#">Servers</a>	✔ Allowed ▼
3	<a href="#">Eric.Payne</a>	<a href="#">WIN-APPPQVJK7UG</a>	Facebook	<a href="#">Default profile</a>	✔ Allowed ▼
3	<a href="#">John Connor</a>	<a href="#">DESKTOP-6I4S961</a>	Facebook	<a href="#">Servers</a>	✔ Allowed ▼
2	<a href="#">Soeren.Kohls</a>	<a href="#">DESKTOP-JMOIO5I</a>	Facebook	<a href="#">Default profile</a>	✔ Allowed ▼





## Como se manter em conformidade ao armazenar dados confidenciais na nuvem?

- Você precisa de visibilidade contínua e controle dos dados sensíveis
- Relatórios sobre o armazenamento externo de dados possibilitam analisar a exposição e remediar rapidamente

## Kit de ferramentas DLP já integrado

18

### Dados em uso

Impeça o uso não autorizado

Controle de dispositivos



### Dados em movimento

Impeça a transmissão não autorizada

Cloud Discovery



Dropbox



facebook



Microsoft 365

### Dados em repouso

Impeça o armazenamento não autorizado



Data Discovery atualizado



Gerenciamento da criptografia completa de disco

# Aplicativos auditados



OneDrive



SharePoint  
Online



Teams

- Office comum: doc, docx, ppt, pptx, xls,xlsx
- Código aberto: odt, odp, ods
- Formatos mistos: PDF, RTF
- Imagens: jpeg, tiff, png, jp2

## Tipos de PII compatíveis

**QUALQUER** número de  
cartão de crédito

PII específicas de país

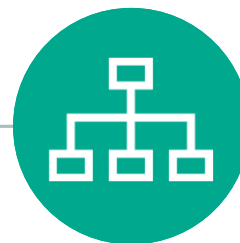
- Alemão
- Italiano
- EUA



Identifique e detecte o que pode ser um risco de perda de dados



Confira o link compartilhado para identificar o autor do documento



ou



Altere você mesmo a opção de compartilhamento no armazenamento

Entre em contato com o autor do arquivo para evitar a perda de dados

## A escolha é sua. No entanto:

160  
arquivos

A organização PME média tem cerca de 160 arquivos com dados confidenciais em seu armazenamento em nuvem



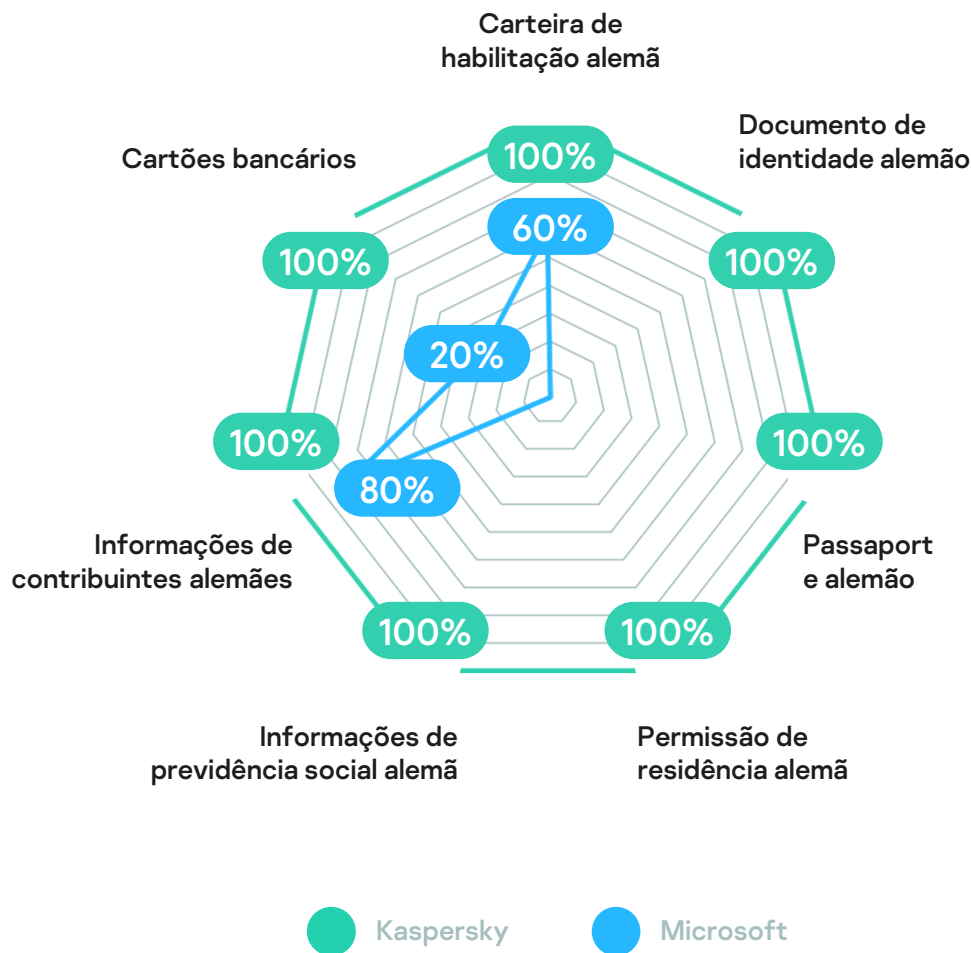
24  
arquivos

15%

Apenas 15% deles, cerca de 24 arquivos, são compartilhados fora da empresa

Dessa forma, a geração contínua de relatórios do Kaspersky Endpoint Security Cloud e uma correção manual pontual de um compartilhamento arriscado pode ser suficiente para **manter sua empresa totalmente em conformidade.**

## Você confia nos recursos do Microsoft 365 DLP?



# Você pode. Mas confira também o desempenho da descoberta de dados de outras soluções



A Kaspersky atingiu uma taxa de descoberta de 100% sem falsos positivos

[Saiba mais](#)

**Kaspersky Endpoint Security Cloud  
Cloud Plus GmbH**

- Information panel
- Users
- Devices
- Security management
- Quarantine
- Distribution packages
- Settings
- Privacy Policy
- Legal Notice
- Help
- Support
- © 2021 AG Kaspersky Lab
- Alexander Korobko  
Admin

## Data Discovery detections (83)

The list below shows a maximum of 1000 detected documents and images that are located in Office 365 cl

Show detections by services: Any | [OneDrive](#) | [SharePoint](#)

[Export detections](#)

LAST EDITED ON	Data categories	Access type	File name
1:42 pm 02/22/2021	<a href="#">IDs</a>	Private	<a href="#">PPTX_residencepermit.pptx</a>
1:42 pm 02/22/2021	<a href="#">IDs</a>	Private	<a href="#">ODP_residencepermit.odp</a>
1:41 pm 02/22/2021	<a href="#">Cards</a>	Private	<a href="#">XLSX_creditcard.xlsx</a>
1:41 pm 02/22/2021	<a href="#">Cards</a>	Private	<a href="#">RTF_creditcard.rtf</a>
1:41 pm 02/22/2021	<a href="#">Cards_IDs</a>	<b>Public</b>	<a href="#">XLS_creditcard.xls</a>
1:41 pm 02/22/2021	<a href="#">Cards</a>	Private	<a href="#">PPTX_creditcard.pptx</a>
1:41 pm 02/22/2021	<a href="#">Cards</a>	Private	<a href="#">PPT_creditcard.ppt</a>
1:41 pm 02/22/2021	<a href="#">Cards</a>	Private	<a href="#">ODS_creditcard.ods</a>
1:41 pm 02/22/2021	<a href="#">Cards</a>	Private	<a href="#">ODT_creditcard.odt</a>
1:41 pm			

### Data Discovery detection details

[Tell us what you think about Data Discovery](#)

Last edit date and time  
02/22/2021 1:41 pm

**Detected data**  
Credit/Debit Card Number, German Residence Permit

**Access to the file**  
**Public**

**Full path to the file**  
OneDrive:  
Ivan Pupkin /  
CreditCard /  
**XLS\_creditcard.xls**

[Link to the file in Office 365](#)  
Share this link with the file owner.  
To gain access to the file, you may need Office 365 credentials.

Last edited by  
Ivan Pupkin

[View the Online Help article about Data Discovery detections](#)

[OK](#)

---

Proteja a colaboração corporativa

24

# Mantenha a segurança com Kaspersky Security for Microsoft Office 365



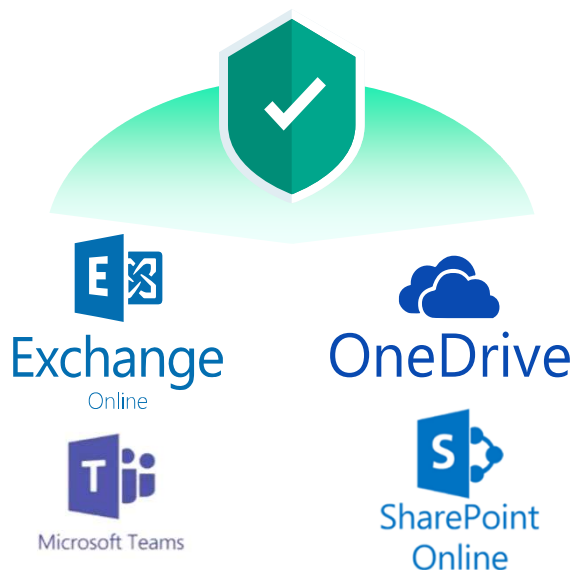


---

## Kaspersky Security for Microsoft Office 365

25

Tendo combatido Shadow IT com o Cloud Discovery, você pode implementar com segurança o Microsoft Office 365 com proteção que já está incluída no Kaspersky Endpoint Security Cloud Plus and Pro



Sem software ou servidores adicionais:

Gerenciamento  
[@ Kaspersky Business Hub](#)

Proteção completa para todos os principais serviços de comunicação e colaboração do pacote O365.

- Impede o phishing e o comprometimento de e-mail corporativo (BEC), evitando o roubo de contas
- Impede a propagação de malware por comunicações de e-mail e armazenamento corporativo em nuvem
- Bloqueia os métodos de spam mais sofisticados
- Remove anexos indesejados antes que os usuários possam cometer um erro

Sem atrasos, sem latência.

Integração perfeita com o Microsoft Office 365 via API e uso de workloads do Microsoft Azure.



**Aumente sua  
proteção**



---

Alertas de proteção de endpoints podem deixar muitas **perguntas sem resposta**

---

Eu não **vejo nem entendo** que aconteceu

---

**Ameaças evasivas:**  
ransomware, malware, spyware financeiro...

- Fácil para os atacantes obterem
- Difícil de detectar
- Mais perigosas

## Análise de causa-raiz e visibilidade

### ● Onde?

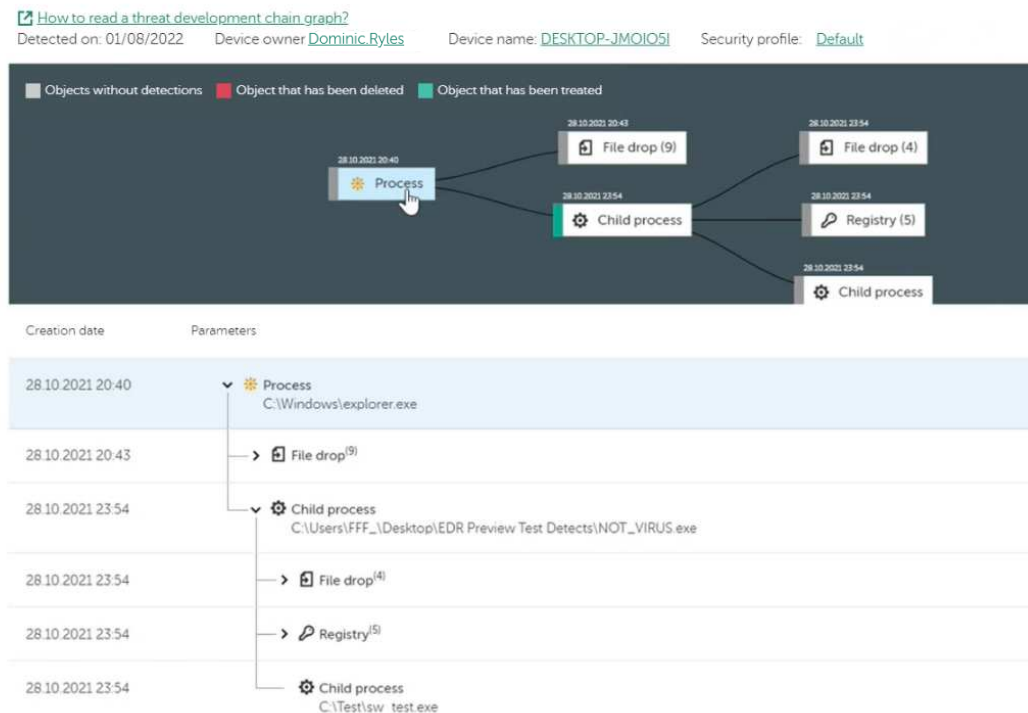
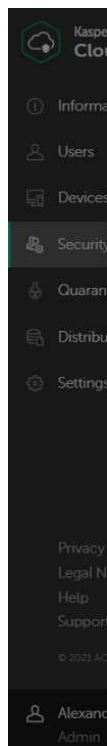
Mostra exatamente o que ocorreu, em qual host e com qual usuário

### ● Como?

A visualização do caminho de propagação do ataque ajuda você a ver e analisar rapidamente como a ameaça se desenvolveu no host

### ● O quê?

Usando todos os dados avançados e ferramentas de visualização, você pode entender a causa-raiz da ameaça e determinar se ações de resposta adicionais precisam ser adotadas





## Reação imediata

Responda a uma ameaça com apenas alguns cliques no cartão de alerta e reaja às ameaças analisadas instantaneamente

## Opções de resposta automatizada

- Verificação de IoC
- Isolar o host
- Impedir a execução de arquivos
- Colocar o arquivo em quarentena
- Verificar áreas críticas

## Reduzir a superfície de ataque

30



Novo

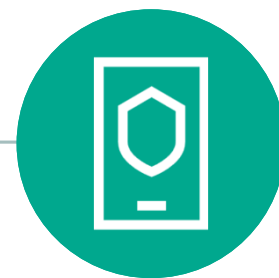
### Controle de aplicativos

Gerencia a inicialização de aplicativos nos computadores dos usuários. Reduz o risco de contaminação restringindo o acesso a aplicativos



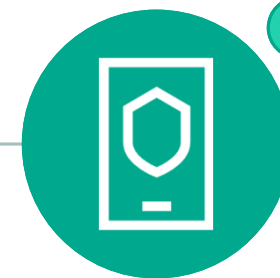
### Controle da Web

Controle centralizado sobre o acesso a recursos da Web suspeitos ou não relacionados ao trabalho



### Controle de dispositivos

Restringe o acesso do usuário a vários dispositivos para proteger os dados contra armazenamento, transferência ou conversão ilegal



Novo

### Controle adaptativo de anomalias

Técnicas de Machine Learning aplicadas para estudar o comportamento dos usuários e aprender a bloquear cenários incomuns.



## Upgrade de habilidades

Generalistas de TI e administradores de sistemas precisam lidar com muitos desafios – a cibersegurança é apenas um deles, mas exige habilidades específicas.



## Torne-se um profissional em cibersegurança

O administrador de TI não precisa ser um especialista em segurança – ajudaremos com treinamento online disponível no console da Web do administrador de segurança



## Fácil e divertido

Usamos uma combinação de teoria e instrução prática em ambientes simulados

Mantenha-se em dia com as mais recentes ameaças evasivas e técnicas de mitigação à medida que sua segurança de TI amadurece

---

Em conformidade com as melhores práticas

32



## Cyber Security Small Business Guide

O Kaspersky Endpoint Security Cloud abrange essas recomendações do "Guia de Cibersegurança para Pequenas Empresas" do National Cyber Security Centre, Reino Unido

- ✓ Instale e ative o software antivírus
- ✓ Ative o firewall
- ✓ Ative a proteção por senha
- ✓ Mantenha sua proteção atualizada
- ✓ Mantenha os dispositivos em dia
- ✓ Mantenha todos os seus equipamentos de TI atualizados (patching)
- ✓ Controle o uso de unidades USB
- ✓ Aplique restrições para evitar que usuários baixem aplicativos de terceiros
- ✓ Instale e ative aplicativos de rastreamento para todos os dispositivos disponíveis, por exemplo, Buscar meu iPhone.



A Kaspersky alcançou mais primeiros lugares em testes independentes do que qualquer outro fornecedor de segurança.

E fazemos isso de forma consistente, ano após ano.



**MOST TESTED\***  
**MOST AWARDED\***  
**KASPERSKY PROTECTION**

[\\*kaspersky.com/top3](https://kaspersky.com/top3)

---

**62**

Testes/avaliações

---

**81%**

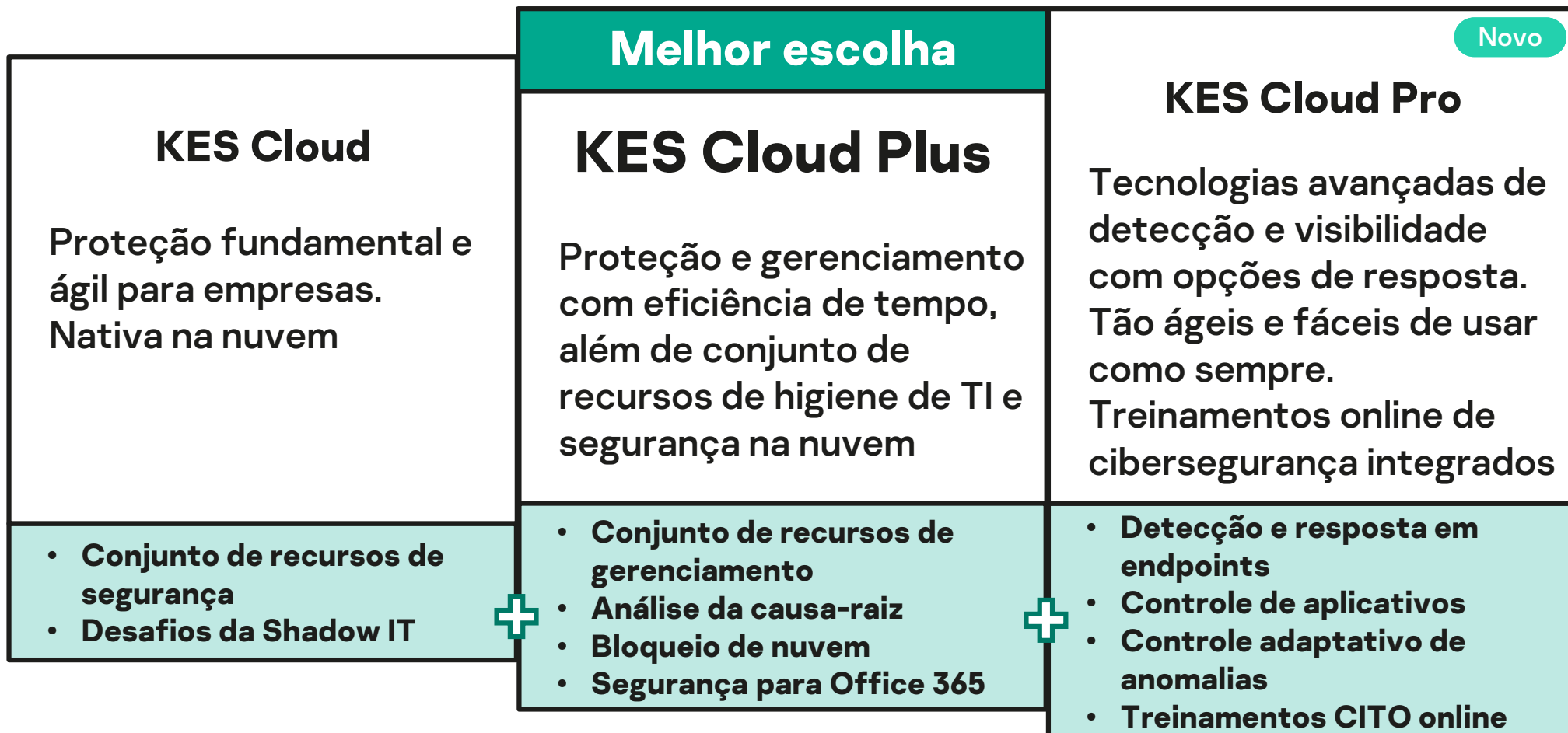
TOP3

---

**45**

Primeiras  
colocações





 licença = usuário

Dispositivos protegidos



Proteção para Microsoft 365

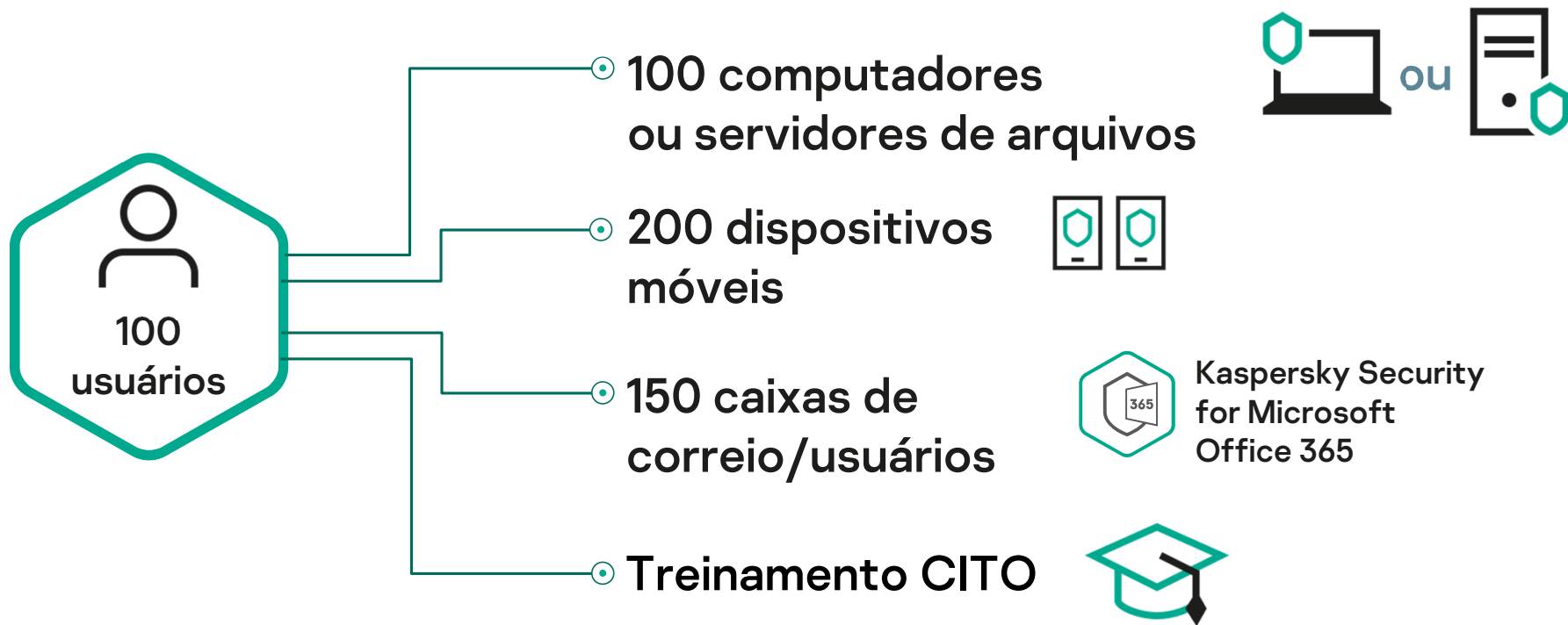


Treinamento Cybersecurity for IT Online



	Dispositivos protegidos	Proteção para Microsoft 365	Treinamento Cybersecurity for IT Online
Kaspersky Endpoint Security Cloud	1 computador ou servidor de arquivos e 2 dispositivos móveis	✗ Não incluso	✗ Não incluso
Kaspersky Endpoint Security Cloud Plus	1 computador ou servidor de arquivos e 2 dispositivos móveis	1.5x usuários Microsoft 365	✗ Não incluso
Kaspersky Endpoint Security Cloud Pro	1 computador ou servidor de arquivos e 2 dispositivos móveis	1.5x usuários Microsoft 365	Módulos teóricos Trabalhos interativos Ambiente simulado

A compra de 100 licenças do nível Pro abrange:



---

## Benefícios

37

A segurança como serviço é a saída para os serviços profissionais ou gerenciados. Uma oferta automatizada é atraente por ser econômica e compensar a falta de recursos de TI e/ou tempo.

### **Benefícios do Kaspersky Endpoint Security Cloud**

- Tempo mais rápido para proteção
- Sem investimento de capital
- Licenças por assinatura anuais e mensais
- Servidor gratuito para reimplementar tarefas críticas aos negócios
- Sempre a versão do produto mais recente e atualizada
- Chega de 'remendar sextas feiras' em servidores
- Gerencie de qualquer lugar, via console da web
- Ganhe tempo para tarefas vitais para os negócios
- Produtividade dos funcionários incrementada



**Kaspersky  
Endpoint Security  
Cloud**

# Interface da web sob medida para administradores de TI sem tempo a perder

38

The screenshot shows the 'Getting started' page of the Kaspersky Endpoint Security Cloud Plus web interface. A progress bar at the top indicates that 8 out of 9 steps are completed. Below the progress bar, there is a 'Hot features' section with three items:

- Endpoint Detection and Response Preview is enabled:** The feature allows you to detect and root out advanced attacks, perform root-cause analysis with a visualized threat de-escalation chain graph, and drill down to details for further review.
- Data Discovery is enabled:** This feature provides you with an overview of your documents and images with critical or personal information that are located in Office 365 cloud storages.
- Kaspersky Security for Microsoft Office 365 is now available under your Kaspersky Endpoint Security Cloud license:** To protect your Office 365, create a workspace for Kaspersky Security for Microsoft Office 365. After a workspace is created, you can enter the activation code that you use for Kaspersky Endpoint Security Cloud. You can find the activation code in the email message that you received after the purchase.

Below the 'Hot features' section, there is a 'Preconfigured' section with two items:

- Company name is entered:** The company name that you specified when you created a workspace on Kaspersky Business Hub is shown at the top of Management Console, next to the logo.
- License is granted:** You have been granted a license for Kaspersky Endpoint Security Cloud.

The screenshot shows the 'Protection' section of the Kaspersky Endpoint Security Cloud Plus web interface. It features several widgets:

- Protection status of devices:** A donut chart showing 18 devices with 11 OK, 2 Warning, and 5 Critical.
- Status of anti-virus database updates:** A donut chart showing 16 updates with 8 During last 24 hours, 2 1 to 3 days ago, 1 3 to 7 days ago, and 5 More than a week ago.
- Operating systems on managed devices:** A donut chart showing 18 devices with 12 Windows (workstations), 0 Windows (servers), 2 macOS, 4 Android, and 0 iOS.

Below the widgets, there is a 'Threats' section with a 'TOP 10 infected devices' widget.

- UX orientada
- Aprendizado no produto
- Cenários de vídeo

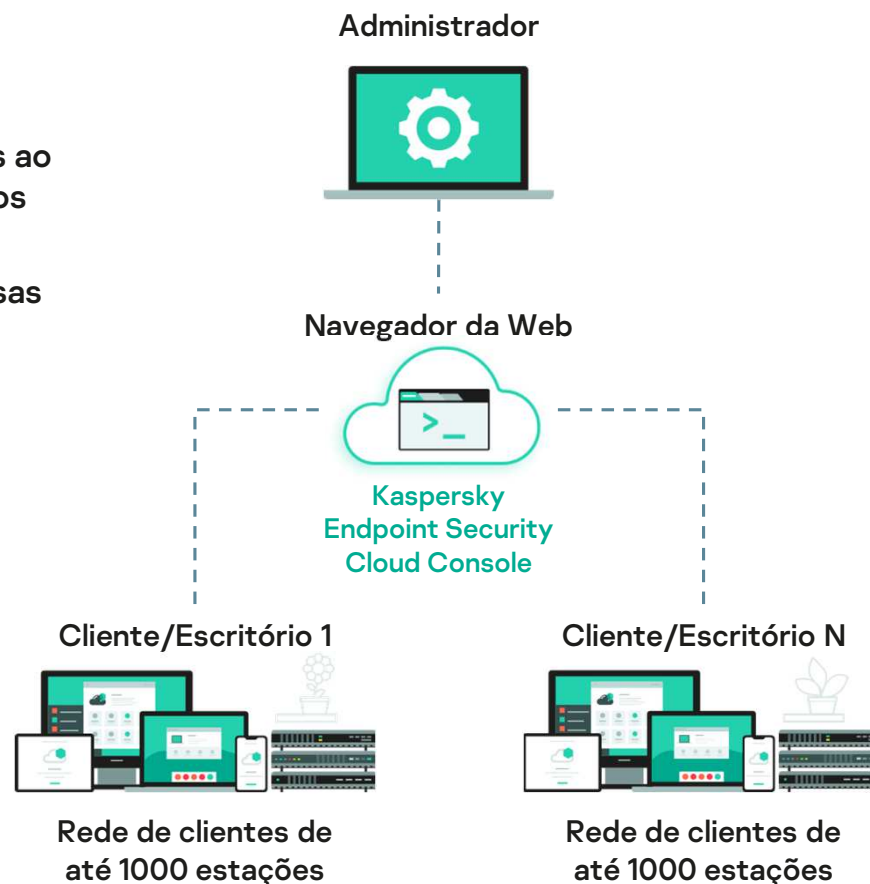
Widgets interativos  
Relatórios e exportação  
agendada

### Console multilocatário

- Facilitam o trabalho dos provedores de serviços gerenciados ao cuidar remotamente das necessidades de segurança de vários clientes sem aumentar a complexidade
- Simplifica também o gerenciamento de segurança de empresas com escritórios distribuídos
- Copie configurações de perfis de segurança nos espaços de trabalho para minimizar o tempo de configuração

### Cogerenciamento e segurança de endpoints

- Crie vários administradores para cada espaço de trabalho
- Visualize vários espaços de trabalho em uma única janela de console, podendo gerenciar várias organizações
- MSPs podem conectar administradores externos ou administradores de clientes para cogerenciamento
- Envie relatórios personalizados no prazo



## Comparativo de níveis

Kaspersky  
Endpoint Security  
Cloud

Kaspersky  
Endpoint Security  
Cloud Plus

Kaspersky  
Endpoint Security  
Cloud Pro

Novo

40

### CONJUNTO DE RECURSOS DE SEGURANÇA

Proteção contra ameaças em arquivos, e-mails e na Web	✓	✓	✓
Firewall	✓	✓	✓
Bloqueador de Ataques de Rede	✓	✓	✓
Prevenção contra ransomware e exploits	✓	✓	✓
Avaliação de vulnerabilidades	✓	✓	✓
Cloud Discovery	✓	✓	✓
Controle adaptativo de anomalias <b>novo</b>			✓
Prevenção de ataques BadUSB <b>novo</b>			✓

### CONJUNTO DE RECURSOS DE GERENCIAMENTO

Bloqueio de nuvem		✓	✓
Data Discovery		✓	✓
Proteção para Microsoft Office 365		✓	✓
Controle da Web, controle de dispositivos		✓	✓
Criptografia e gerenciamento de correções		✓	✓
Controle de aplicativos <b>novo</b>			✓
Apagamento remoto <b>novo</b>			✓

### CONJUNTO DE RECURSOS DE INVESTIGAÇÃO E RESPOSTA

Análise de causa-raiz*		✓	✓
EDR (varredura de IoC, resposta automatizada, isolamento com um clique) <b>novo</b>			✓
Treinamento de TI			✓

\* era Preview do EDR.



# Vamos conversar?

OSA IT SOLUTIONS

Rua Flórida, 1703 – CJ. 62 – Cidade Monções

São Paulo – Brasil

Tel: +55 (11) 5461-1374

[www.osait.com.br](http://www.osait.com.br)

**kaspersky**

Sales  
Specialist

**kaspersky**

Certified  
Professional

**kaspersky**