Respondendo às suas atuais e futuras necessidades de TI

Abordagem de cibersegurança em fases

kaspersky

Construir uma base de segurança para a sua organização escolhendo o produto ou serviço certo é apenas o primeiro passo. Desenvolver uma estratégia de segurança virtual corporativa com uma visão de futuro é a chave para o sucesso a longo prazo.

O portfólio corporativo da Kaspersky reflete as demandas de segurança das empresas de hoje, respondendo às necessidades das organizações em diferentes níveis de maturidade com uma abordagem por estágios Esta abordagem combina diferentes camadas de proteção contra todos os tipos de ameaças virtuais para detectar os ataques mais complexos, responder de forma rápida e adequada a qualquer incidente e evitar ameaças futuras.

Tipos de ameaças e a experiência necessária para combatê-las

À medida que os ambientes de TI crescem em tamanho e complexidade, as empresas enfrentam ameaças cada vez mais sofisticadas que exigem o aprimoramento constante de seus conhecimentos de segurança virtual para permitir defesas eficazes.

Nossa experiência e pesquisa contínua de ameaças nos permitem dividir todas as ameaças disponíveis em categorias. A maioria das ameaças está na base da pirâmide. Essas são ameaças genéricas que exigem apenas mecanismos de defesa básicos e higiene de segurança de TI. Se você subir na pirâmide, começará a ver ameaças mais avançadas que escapam à proteção preventiva usando Táticas, técnicas e procedimentos (TTPs) conhecidos. Os agentes de ameaças nesta categoria, por exemplo, poderiam obter e reutilizar as ferramentas mais sofisticadas que seus "colegas" com melhores recursos já desenvolveram. A maioria das violações pertence a esta categoria. E, finalmente, bem no topo, existem ameaças e ataques complexos do tipo APT que usam TTPs desconhecidos. Os agentes de ameaças neste nível têm recursos ilimitados para desenvolver ferramentas e métodos altamente sofisticados com alvos muito específicos em mente.

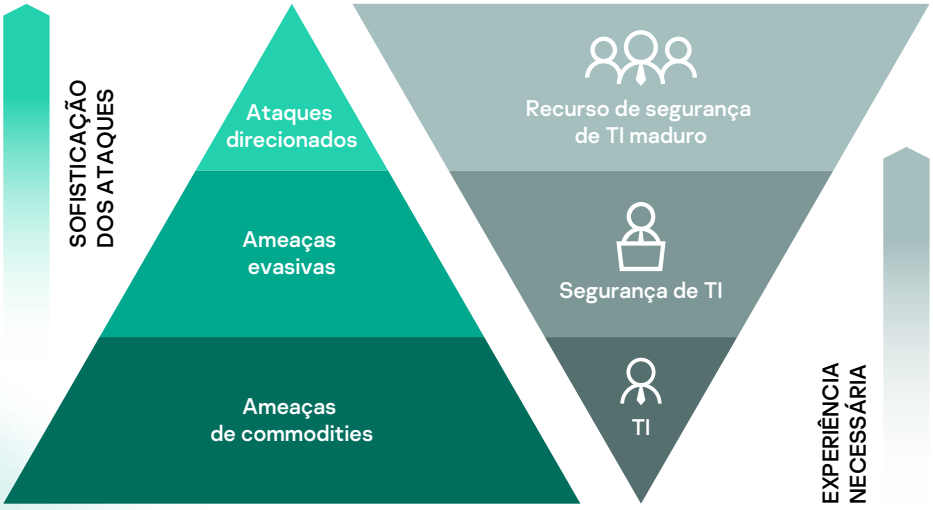


Figura 1. Tipos de ameaças e a experiência necessária para combatê-las

Para impulsionar o crescimento dos negócios com sucesso e manter a competitividade, as empresas aumentam continuamente sua confiança nas tecnologias da informação. A transformação digital contínua expande a superfície de ataque potencial por meio de sistemas cada vez mais interconectados. Com os ambientes de TI crescendo em tamanho e complexidade, as empresas enfrentam a sofisticação cada vez maior das ameaças, exigindo que avancem continuamente em sua especialização em segurança virtual para permitir defesas eficazes.

Abordagem de cibersegurança em fases

Em linha com as ameaças e o grau variável de recursos de segurança virtual de nossos clientes, empregamos uma estratégia de ir ao mercado com nossos produtos e serviços para ajudar as organizações a prevenir 90% das ameaças automaticamente, e então, sistematica e metodicamente capacitá-los a adicionar recursos novos e avançados para combater ameaças mais sofisticadas à medida que seus negócios se desenvolvem.

Levando em consideração o crescimento no número e na complexidade das ameaças, a maturidade da segurança de TI, as habilidades em segurança virtual e os orçamentos existentes, há uma necessidade clara de começar a construir uma estratégia de segurança abrangente e adaptável.

No Estágio 1, fornecemos todos os nossos produtos preventivos líderes, juntamente com suporte premium e serviços profissionais para garantir que os clientes obtenham o máximo benefício de nossas tecnologias. No Estágio 2, conforme você sobe na pirâmide, há uma necessidade crescente de combater as ameaças que contornam os mecanismos preventivos existentes. Para oferecer suporte à proteção consciente de recursos contra ameaças avançadas e evasivas, oferecemos uma solução habilitada para nuvem que complementa as habilidades básicas de segurança virtual do cliente com detecção gerenciada, priorização e resposta guiada, juntamente com um conjunto de ferramentas automatizadas que ajuda a equipe de segurança a identificar, analisar e responder às ameaças evasivas mais perigosas de maneira mais eficaz. As organizações no Estágio 3 têm mais chances de enfrentar um APT real e precisam de defesas eficazes contra TTPs desconhecidos. Para atender às necessidades de equipes de segurança de TI maduras, a Kaspersky oferece uma combinação inovadora e equilibrada de tecnologias e serviços para enfrentar os desafios das ameaças e ataques direcionados mais sofisticados da atualidade.

O Kaspersky Managed Detection and Response permite uma função de segurança de TI madura instantaneamente sem necessidade de investir em funcionários ou conhecimentos adicionais. Ao mesmo tempo, permite que os processos de triagem de incidentes sejam transferidos para a Kaspersky, para que as equipes de segurança de TI maduras possam se concentrar em responder aos resultados críticos fornecidos.

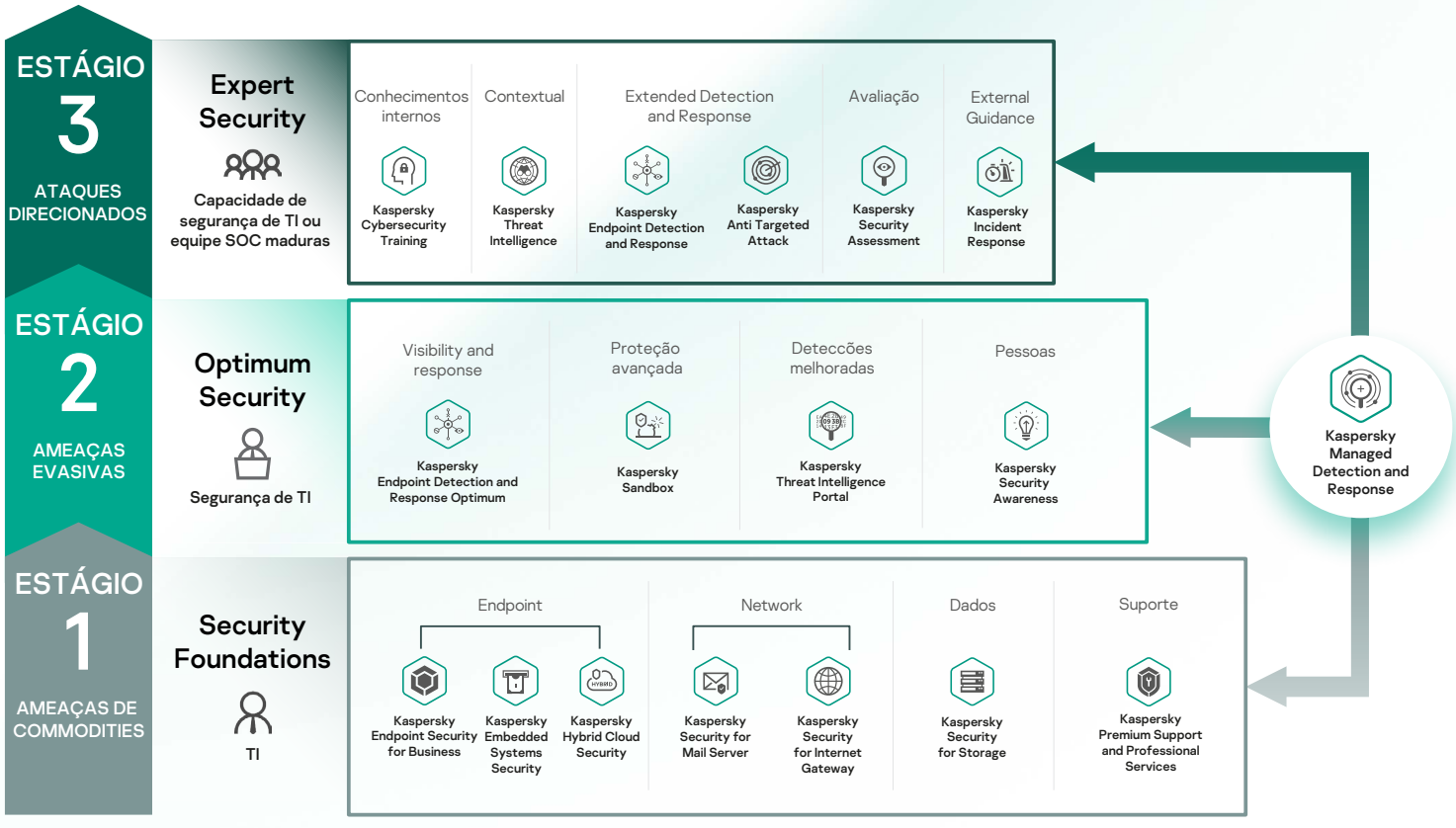


Figura 2. Abordagem de cibersegurança em fases

Security Foundations

Bloqueie o número máximo de ameaças, automaticamente.

O Security Foundations é um estágio fundamental para organizações de qualquer porte e complexidade de infraestrutura na criação de uma estratégia de defesa integrada contra ameaças complexas. Ele fornece prevenção automatizada multivetorial de um grande número de possíveis incidentes causados por ameaças de commodities. Esse estágio geralmente é suficiente para empresas menores com equipes de TI apenas.

As empresas não podem pular este estágio e passar diretamente para a implementação de tecnologias avançadas de detecção e resposta. Isso ocorre porque a maioria dessas tecnologias requer envolvimento humano que é, obviamente, caro e requer experiência. Tão caro, que a equipe de segurança de TI fica sobrecarregada com alertas, sem que a maioria das ameaças sequer sejam impedidas. E, em vez de caçar proativamente ameaças ocultas e responder a incidentes, a equipe de segurança de TI perde tempo classificando e priorizando milhares de alertas, deixando a maioria deles intocados.

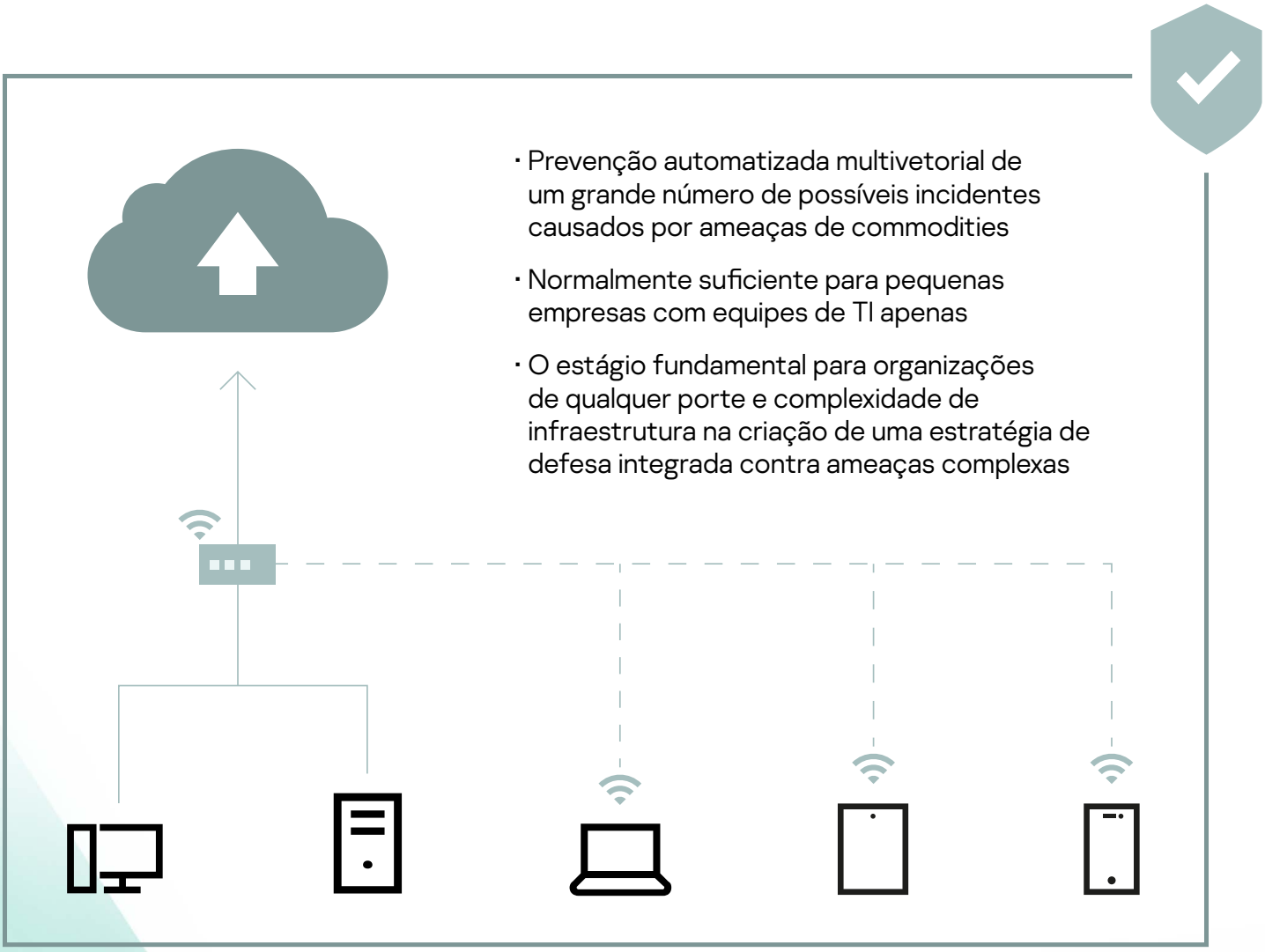


Figura 3. As principais características do Estágio 1

Optimum Security

Concentre-se na detecção avançada e em uma resposta rápida às ameaças que fogem da proteção preventiva.

Com o tamanho e a complexidade crescentes dos ambientes de TI que dão suporte ao desenvolvimento e ao crescimento dos negócios, as organizações também aumentam sua superfície de ataque potencial. Eles se tornam alvos mais atraentes para os criminosos virtuais e correm maior risco de enfrentar ameaças avançadas que escapam aos mecanismos de prevenção automática.

À medida que a superfície de ataque potencial aumenta, a importância de estabelecer pelo menos práticas básicas de resposta a incidentes não pode ser subestimada. Essas empresas geralmente começam a desenvolver uma função de segurança de TI dentro de seu departamento de TI, mas sua maturidade ainda é baixa. Pequenas equipes de segurança de TI exigem instrumentos para detecção automatizada de ameaças avançadas e resposta centralizada como base para o amadurecimento de sua função. O treinamento da equipe também se torna essencial para aumentar a conscientização sobre a segurança em toda a organização e motivar todos os funcionários a prestar atenção às ameaças virtuais e como lidar com elas, mesmo que isso não seja considerado uma parte específica de suas responsabilidades de trabalho.

Com base no Security Foundations, o Optimum Security permite que as organizações com ambientes de TI que estão crescendo em tamanho e complexidade combatam as ameaças de commodities e as que contornam os mecanismos preventivos existentes. Uma solução com foco em recursos é ideal para pequenas equipes de segurança de TI com conhecimentos básicos. Este estágio permite que os clientes aprimorem seus próprios recursos de detecção e resposta, enquanto se beneficiam da proteção gerenciada 24 horas por dia, 7 dias por semana. Ao mesmo tempo, um portfólio de produtos de treinamento em forma de jogos baseados em computador ajuda a moldar as habilidades de ciber higiene dos funcionários e motivá-los a manter práticas seguras.

- Security Foundations implementado com sucesso
- O ambiente de TI está crescendo em tamanho e complexidade, criando uma superfície de ataque cada vez maior
- Uma pequena equipe de segurança de TI está instalada, com alguma experiência
- A capacidade de resposta a incidentes é importante para você

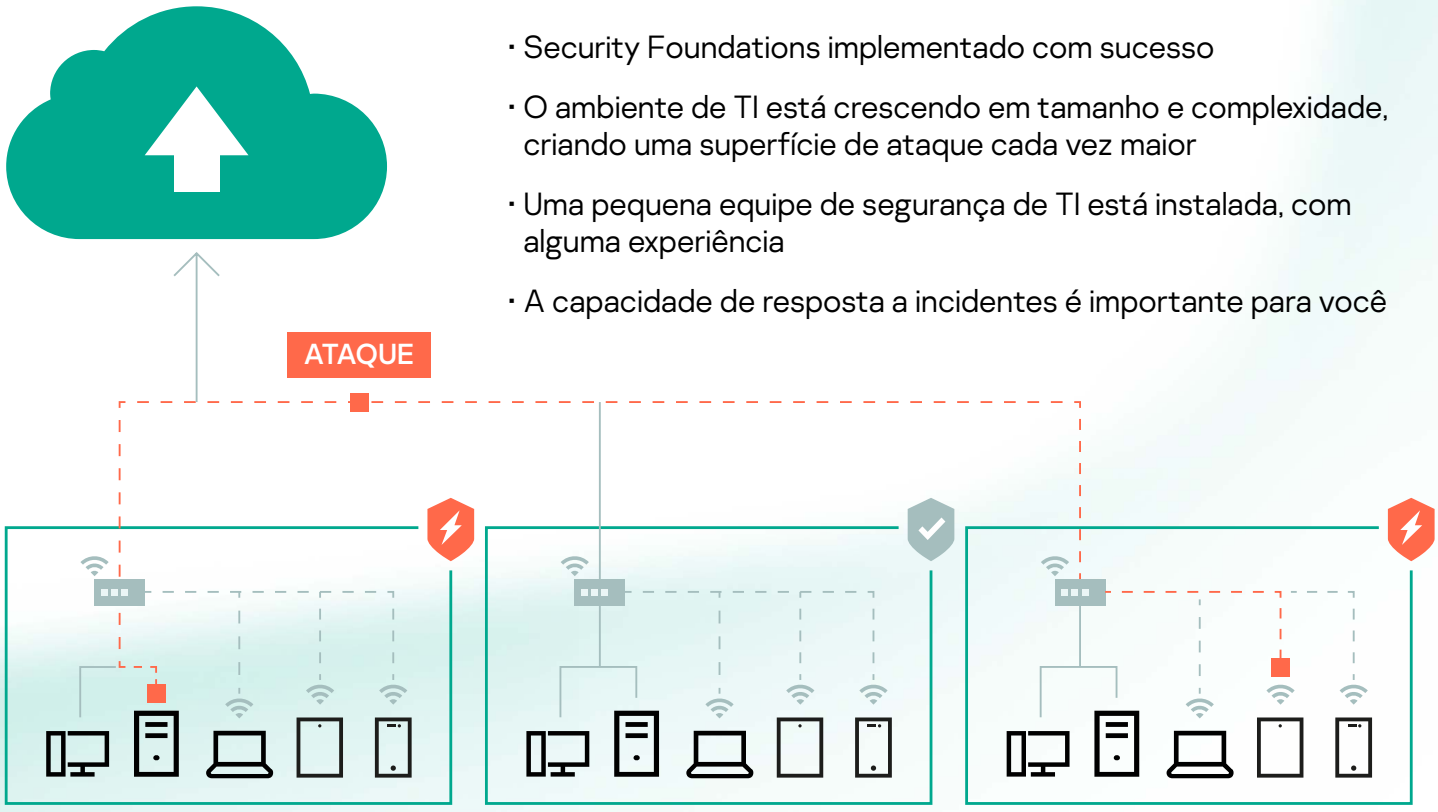
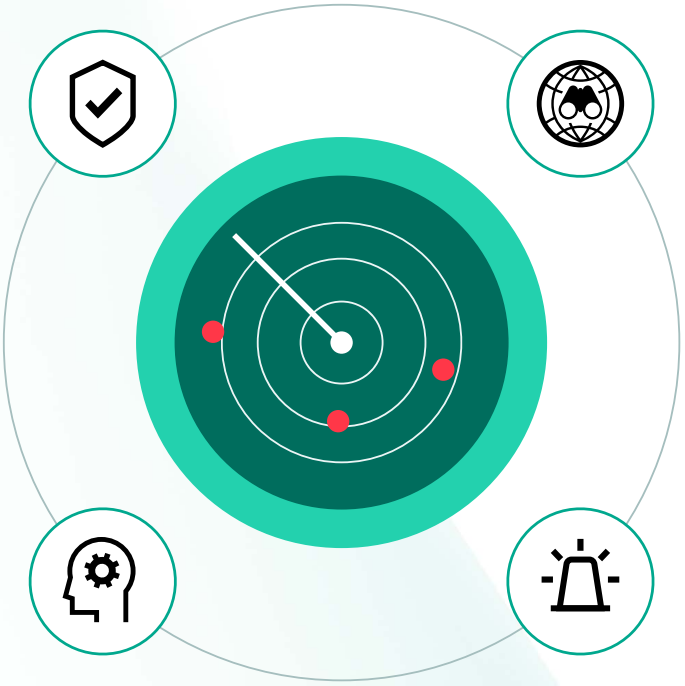


Figura 4. As principais características do Estágio 2

Expert Security

Disposição imediata para ataques complexos e semelhantes a APT.

A adoção de práticas manuais de caça a ameaças e casos de uso avançados para inteligência de ameaças e, ao mesmo tempo, ter uma equipe totalmente equipada com profundo conhecimento em tópicos específicos, como análise forense digital e análise de malware, será vital para as organizações no Estágio 3. Eles se beneficiarão ao estabelecer relações de confiança com um parceiro altamente qualificado para complementar rapidamente suas capacidades existentes com conjuntos de habilidades mais específicas quando necessário. O Kaspersky Expert Security oferece uma plataforma de detecção e resposta estendidas, juntamente com orientação especializada inigualável, avaliação, inteligência de ameaças e treinamento de habilidades, que se combinam para cobrir as necessidades de segurança de ponta a ponta de qualquer empresa com uma função de segurança de TI madura para enfrentar as complexas ameaças, ataques do tipo APT e direcionados de hoje.



- Os ambientes de TI estão se tornando complexos e distribuídos
- A equipe de segurança de TI é madura ou um Centro de Operações de Segurança foi estabelecido
- A propensão a riscos é baixa devido a custos mais altos de incidentes de segurança e violações de dados
- A conformidade regulatória é uma preocupação

Figura 5. As principais características do Estágio 3

Por que a Kaspersky

Nossa missão é construir um mundo mais seguro. Acreditamos em um futuro onde a tecnologia melhora a vida de todos nós. É por isso que nós o protegemos: para que todas as pessoas, nos quatro cantos do mundo, tenham acesso às oportunidades intermináveis que a tecnologia oferece.

Somos uma empresa mundial com uma visão global e focada em mercados internacionais. Nós operamos em 200 países e territórios e temos 34 escritórios em mais de 30 países. Nossa equipe é formada por mais de 4.000 especialistas altamente qualificados.

Estamos constantemente inovando, oferecendo proteção eficaz, utilizável e acessível. Nossa profunda inteligência de ameaças e experiência em segurança estão constantemente se transformando em soluções e serviços de segurança inovadores para proteger empresas, infraestrutura crítica, governos e consumidores em todo o mundo. Nosso portfólio de segurança abrangente inclui soluções e serviços líderes de proteção, detecção e resposta para combater ameaças digitais sofisticadas e em evolução. Mais de 400 milhões de usuários são protegidos pelas tecnologias da Kaspersky, e ajudamos 250.000 clientes corporativos a proteger o que é mais importante para eles.

www.kaspersky.com.br