Por que escolher Darktrace?

Principais diferenciais

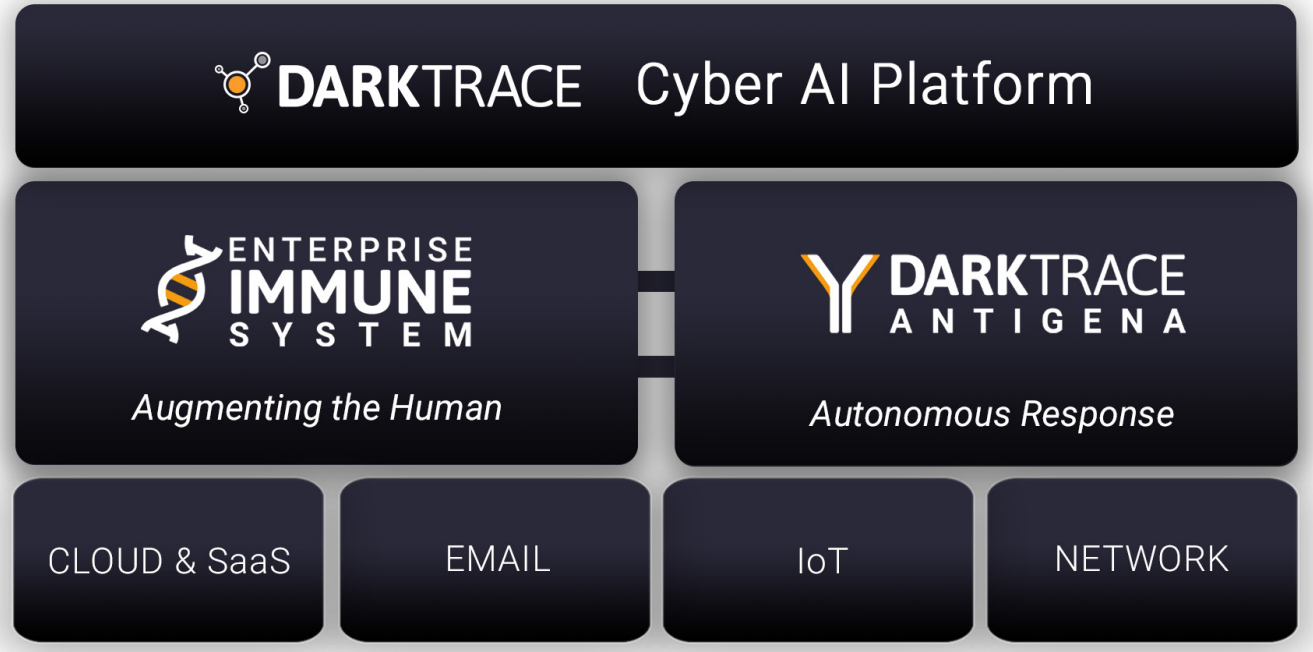
Darktrace é a única plataforma que:

- Aprende o que é normal 'na prática' para detectar ataques inéditos e ameaças internas
- Oferece uma proteção unificada e sob medida para e-mails, nuvem, IoT e rede
- Neutraliza ataques, com velocidade extrema e precisão cirúrgica
- Automatiza as investigações de ameaças com velocidade e abrangência, reduzindo em 92% o tempo de triagem

O objetivo deste documento é esclarecer o status exclusivo da Darktrace na área de defesa cibernética da IA. Fundada e sediada em Cambridge, a Darktrace é uma empresa global de tecnologia que está na vanguarda da Ciber IA há mais de 6 anos.

Nas avaliações de concorrência, as empresas sempre escolhem a Darktrace porque somos capazes de oferecer mais cobertura, uma detecção mais rápida e – graças à Antigena – uma resposta autônoma. Isso é demonstrado por nossa avaliação de US$ 1,65 bilhão (em setembro de 2018) e por nossa participação de mercado, com mais de 3.000 empresas em todo o mundo que já contam com a nossa tecnologia para proteger suas organizações no mundo todo.

Neste documento, oferecemos uma poderosa validação feita por analistas independentes, a mais notável sendo feita pela respeitada especialista da indústria, Alissa Knight, que em seu recente relatório 'Patterns of Life' (Aite Group), afirma: "A Darktrace é o único fornecedor ao qual dei cinco, a nota máxima, até hoje." Também destacamos áreas fundamentais nas quais nos diferenciamos de outras tecnologias que dizem estar à altura da Darktrace.



Abordagem e impacto exclusivos para seus negócios

Com base no que sabemos sobre as outras tecnologias do mercado, a Darktrace é única porque:

1. A Darktrace é a única plataforma que aprende, na prática, a criar uma proteção sob medida para a sua organização

A entrada dos ataques nas organizações é inevitável nos dias atuais,e já não é mais possível identificar esses ataques em andamento através do ato de antecipar tudo que pode dar errado.

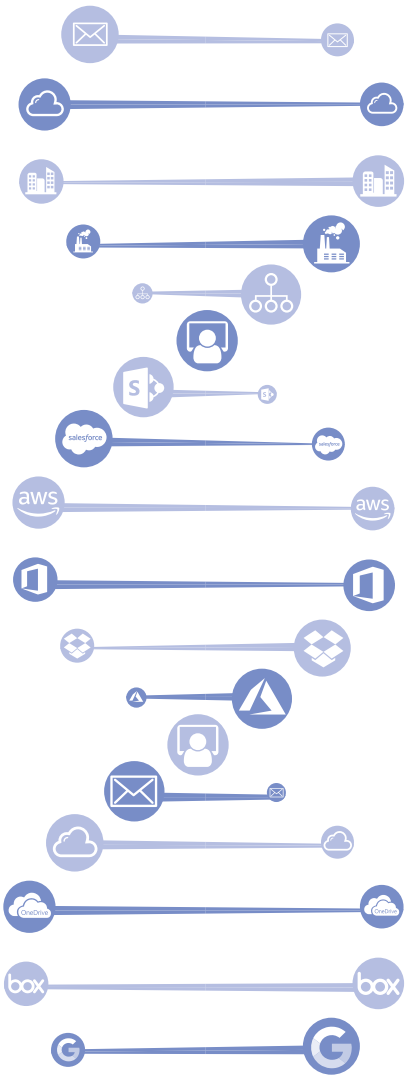
A Darktrace recorre a uma analogia do sistema imunológico humano

– suas defesas conhecem os seus ataques históricos e agem como uma membrana protetora, enquanto o Enterprise Immune System complementa isso tudo ao aprender sobre as pessoas, sistemas e dados em seu negócio digital, bem como ao detectar as atividades estranhas e incomuns que são as características inconfundíveis do surgimento de um ataque. Basicamente, não tentamos capturar os ataques em andamento pelo que aparentam ser, e sim quando tentam agir.

A Darktrace é a única que oferece uma tecnologia que realmente aprende 'na prática' compreendendo todo o ambiente digital da sua empresa. Isso cria uma compreensão sob medida do 'DNA' da sua organização para permitir a detecção precoce de ameaças. As ameaças que entram em seu ambiente digital tipicamente não serão ataques históricos, e sim ameaças inéditas que burlaram as suas ferramentas de defesa existentes ou os funcionários e terceiros que apresentam um comportamento inadequado.

Há uma tendência cada vez maior para o uso de IA em segurança cibernética e, em particular, isso fica claro à medida que os sistemas de IA são treinados em ataques históricos para serem capazes de reconhecer eficientemente a repetição deles no futuro. Independentemente dessa abordagem ser ou não aplicada no endpoint como um mecanismo AV de última geração ou nas redes e na nuvem, a Darktrace acredita que trata-se apenas de um ganho marginal em comparação aos sistemas tradicionais que baseiam-se em ataques históricos para produzir regras, assinaturas, heurísticas e inteligência de ameaças.

Por outro lado, as abordagens para a detecção de ameaças avançadas do Enterprise Immune System são realmente complementares aos investimentos que você já possui e reduzem significativamente o risco geral da organização, por deixar os invasores expostos.



2. A Darktrace é a única plataforma que oferece a cobertura total de seus negócios digitais

A Darktrace ficou famosa por trazer a abordagem do sistema imunológico às redes, mas não parou por aí. Um dos objetivos fundamentais do design do produto é continuar a expandir o sistema imunológico onde quer que os clientes levem seus negócios digitais.

Neste momento, o sistema imunológico pode abranger:

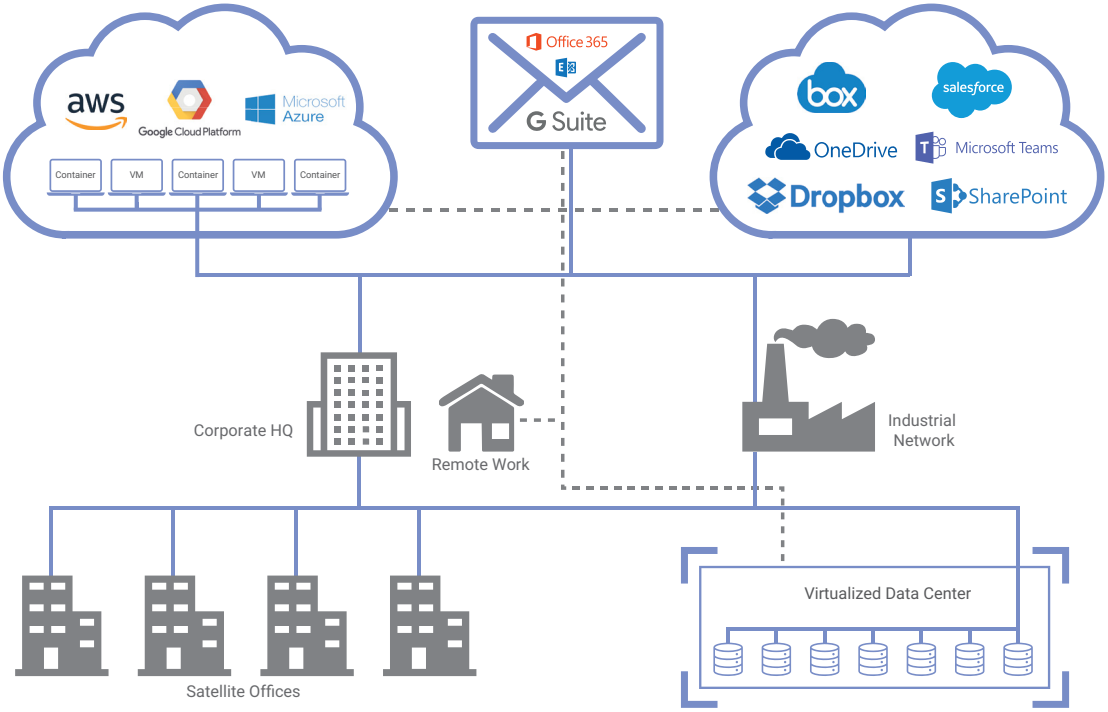
- Ambientes de nuvem pública e privada, tais como o AWS (com o VPC Traffic Mirroring), Microsoft Azure (com o vTAP da Azure) e o Google Cloud, quer haja cargas de trabalho de computação tradicionais ou abordagens modernas como contêineres, kubernetes etc.
- Ambientes SaaS como Salesforce, Office365, SharePoint, OneDrive, Google Suite, Dropbox, Box etc.
- Sistemas de e-mail para que os ataques em andamento provenientes de e-mails mal-intencionados possam ser rastreados e interditados após a primeira vítima (paciente zero), e não a 200ª.
- Ambientes industriais, desde usinas nucleares a fábricas de chocolate, fabricantes de automóveis e equipes de corrida de Fórmula 1.
- Ambientes de IoT que vão desde prédios e cidades inteligentes até a navegação global e semi-autônoma, os quais em breve também alcançarão a órbita da Terra em enxames de microssatélites.
- Centrais de dados tradicionais ou virtualizadas, desde as pequenas até as gigantes.
- E, claro, as redes de campus universitários, onde tudo começou.

Os perpetradores de ameaças cada vez mais não estão limitando seus ataques a uma tecnologia de cada vez e, como defensores, é essencial que as proteções sejam unificadas em toda a empresa digital. Algo tão simples quanto uma senha comprometida pode resultar em um ataque concomitante contra várias instalações. Ser capaz de enxergar isso em tempo real é fundamental para o gerenciamento significativo de incidentes – não faz mais sentido lidar com a segurança de acordo com cada tecnologia.

Além de unificar a detecção, a Darktrace possui a crença inabalável na visibilidade total. Para equipes de segurança atuais, as ferramentas devem facilitar a capacidade de explorar e enxergar à vontade o que acontece em vários ambientes, em vez de simplesmente emitir alertas de segurança.

À medida que nosso relacionamento com você se desenvolver, mantenha-nos atualizados sobre seus planos futuros de tecnologia para que continuemos a desenvolver a cobertura que mantém a segurança dos negócios, na velocidade com a qual você deseja se modernizar.

> “O software da Darktrace sinaliza as ameaças cibernéticas nas redes integradas à nuvem, independentemente de sua origem.”
>
> **- Forrester**



3. A Darktrace Antigena é a única tecnologia capaz de interromper ataques em segundos, mesmo que você nunca os tenha antecipado

Muitos clientes observam que seus profissionais que respondem a incidentes encontram-se sob uma imensa corrida contra o tempo para reagir a ataques rápidos ou que ocorrem fora do turno de trabalho. Embora seja comum o mercado oferecer integrações aos sistemas de fluxo de trabalho ou SOAR para adotar ações (isso também é possível com o sistema imunológico da Darktrace), todos estes registros precisam ser configurados especificamente por sua equipe, os quais podem ser uma atividade de engenharia significante a ser produzida e manter atualizada.

A resposta autônoma é o próximo patamar de maturidade, no qual nossa plataforma pode reagir a situações inéditas a fim de manter seus principais objetivos de segurança. Talvez isso consista em interromper um acesso mais profundo à rede, em interceptar os ataques a dados com pedido de resgate ou em garantir que a perda inesperada de dados seja sempre suspensa até que a equipe de segurança tenha a oportunidade de investigar.

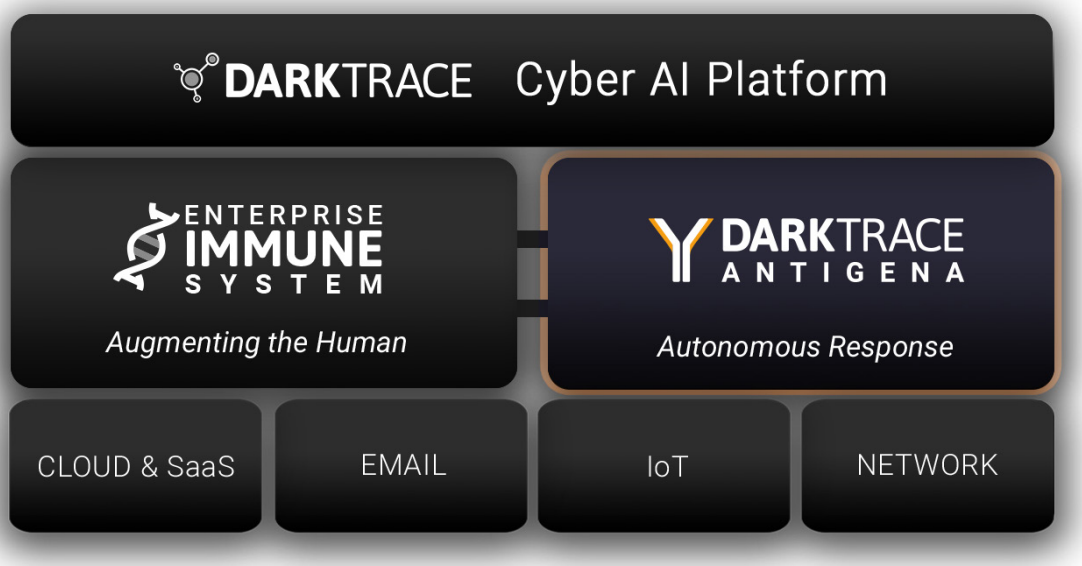
E, crucialmente, o sistema decide por si próprio como reagir cirurgicamente: visando especificamente o mau comportamento, interagindo com as defesas e a infraestrutura existentes e continuando a monitorar o incidente, caso o invasor mude de tática e seja necessária uma intervenção maior.

Isso só é possível porque a plataforma realmente aprende, na prática, a entender como sua empresa opera. Com isso, os sistemas infectados podem permanecer na rede sem que sejam uma ameaça, enquanto os funcionários e sistemas podem continuar a desempenhar suas funções.

A Darktrace inventou a resposta autônoma (Autonomous Response) em 2016, a qual agora é adotada por centenas de redes de clientes em todo o mundo. Neste exato momento, a Antigena responde, a cada 3 segundos, a uma ameaça cibernética em algum lugar do mundo e o conceito foi adotado pela Gartner como um objetivo principal da modernização da segurança para o futuro.

Além de adotar ações em redes e nuvem (disponíveis agora) e em SaaS (disponível na próxima versão v4.1), a Antigena Email expande essa proteção para os e-mails. Ao correlacionar a compreensão da IA da infraestrutura, SaaS e do ambiente de e-mail, a Darktrace é a única capaz de detectar uma infecção em qualquer ambiente e executar automaticamente a análise de causas primárias para verificar se ela teve origem em algum e-mail. Caso afirmativo, ela protegerá instantaneamente todos os outros funcionários.

A isso chamamos de resposta autônoma estratégica – onde o aprendizado com o Paciente Zero permite a proteção estratégica do restante da empresa, sem a intervenção humana. Do ponto de vista das operações, alguém ainda precisa limpar o laptop da primeira vítima, mas isso é muito melhor do que limpar 200 ou algo muito pior.



4. Os recursos adicionais da Darktrace oferecem a investigação orientada por IA com velocidade e abrangência

Muitas equipes encontram-se sob uma grande corrida contra o tempo e não têm recursos disponíveis para realizar investigações completas sobre os eventos de segurança. Às vezes, isso pode resultar na omissão de detalhes importantes dos incidentes. Talvez algumas das atividades de comando e controle passem despercebidas, talvez outros dispositivos estejam infectados, mas são negligenciados. Ou talvez foi gasto um tempo valioso documentando incidentes, em vez de gerenciar riscos.

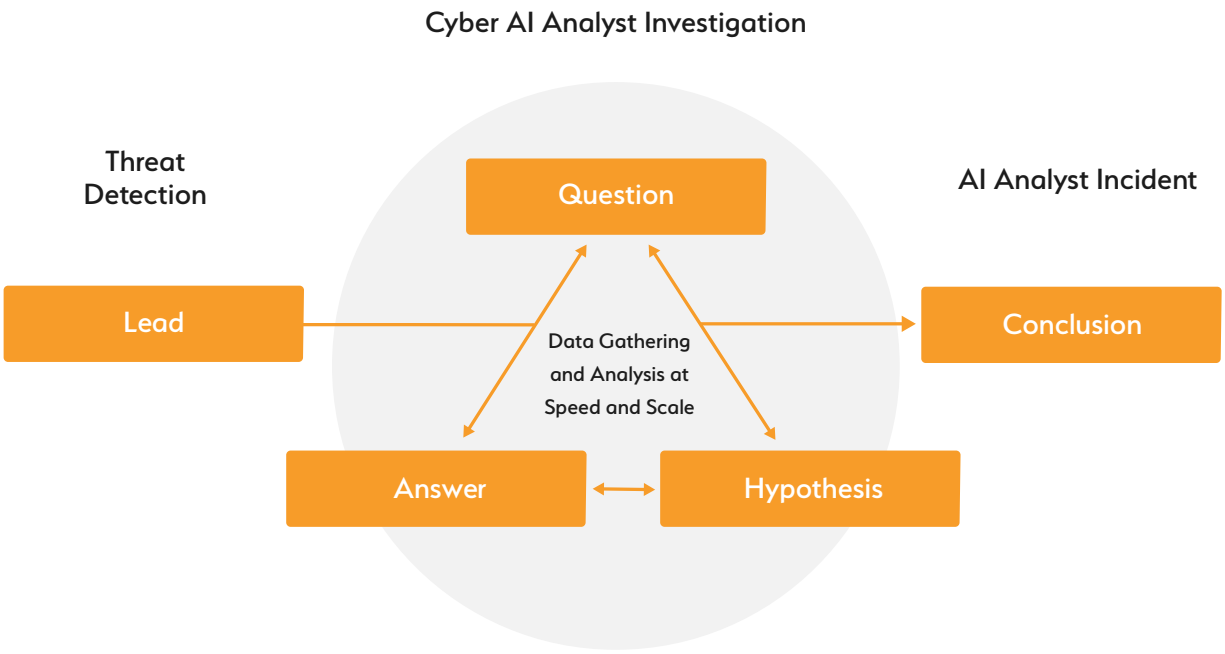
O recente lançamento do AI Analyst pela Darktrace agora oferece uma investigação completa de incidentes para interrelacionar automaticamente as evidências aos sinais de ataques em diferentes tecnologias e infra-estruturas, associando-os ao ciclo de vida de um ataque, incluindo respostas autônomas e produzindo um painel dinâmico da situação e relatórios escritos (em frases e parágrafos), que podem ser armazenados para gerar um histórico de registros que são compartilhados com as equipes que precisam agir (por exemplo, a equipe que realiza bloqueios de rede ou a equipe que realiza a limpeza de computadores) ou então compartilhados com o gerenciamento.

Dessa maneira, a plataforma não apenas exibirá alertas de alta fidelidade/pistas para investigação, como também investigará automaticamente 100% dessas pistas de maneira semelhante a um especialista humano, só que com a consistência, velocidade e abrangência da IA. Assim, a equipe de segurança pode entender rapidamente o que está acontecendo, mesmo no ambiente mais complexo, sem a necessidade de profunda pesquisa.

Tente compreender por um momento a grandiosidade disso; 100% dos alertas são investigados e relatados, no idioma de sua escolha, 24 horas por dia, 7 dias por semana. Isso permite que a sua equipe se concentre em atividades de gerenciamento de risco de alto valor que por sua vez possibilitarão negócios, em vez de análises mundanas e comuns que podem tirar o foco dos principais negócios da empresa.

Ao reduzir o tempo de triagem em até 92%, as equipes de segurança podem disseminar rapidamente informações fundamentais, tais como as mudanças necessárias nos firewalls ou nos computadores que precisam de limpeza, em apenas alguns segundos após receber o alerta. Eles também podem pensar de maneira mais estratégica sobre outras ações preventivas que podem ser tomadas para reduzir o risco geral para a organização.

De acordo com Chris Kissel, diretor de pesquisa da IDC: "Ao investigar automaticamente os eventos de segurança, o AI Analyst ajuda a reduzir os dados irrelevantes mais do que qualquer outra tecnologia." Não existe outro fornecedor no mercado capaz de oferecer a mesma investigação e análise por IA de ameaças cibernéticas.



Validação independente

No evento Gartner Security and Risk Management Summit de 2019, um analista sênior da Gartner, David Mahdi, argumentou a favor da resposta autônoma baseada em IA no discurso de abertura da conferência. Além disso, um segundo analista da Gartner, Lawrence Pingree, afirmou em seu discurso que "a próxima fase de nossa jornada em direção à segurança autônoma é a tomada de decisões por resposta autônoma."

Embora seja importante que a Gartner tenha reconhecido a resposta autônoma como algo essencial no cenário atual de ameaças cibernéticas, a Darktrace foi a empresa pioneira na resposta autônoma contra ameaças cibernéticas emergentes, sendo isso o que nós temos feito nos últimos 3 anos.

O relatório 'Patterns of Life' do Aite Group (disponível mediante solicitação) cita a Darktrace no contexto de outras tecnologias. O autor é Alissa Knight, uma respeitada especialista e profissional em segurança citada com frequência nas principais publicações do setor, como a Forbes. São algumas das citações mais importantes:

Sobre Tecnologia e Concorrência

"Depois de analisar todas as soluções disponíveis, acredito que a oferecida pela Darktrace é uma das poucas realmente capazes de fazer uma análise de ameaças de redes. Sua capacidade de enxergar e responder de maneira autônoma aos 'known knowns' e aos 'known unknowns' (os conhecidos que já conhecemos e os desconhecidos que já conhecemos) é incomparável com qualquer outro produto existente no mercado e, graças aos seus recursos expandidos, a Darktrace alcançou a liderança na competição de análises de ameaças de redes."

"De acordo com as notas resultantes de cada categoria, minha nota geral para a solução Darktrace é cinco, a nota máxima, sendo essa a primeira vez que dei uma pontuação perfeita a um fornecedor."

Recurso	Classificação de 1 a 5
Instalação	●●●●●
UX	●●●●●
Prevenção	●●●●●
Componentes	●●●●●
Arquitetura	●●●●●
Detecção	●●●●●
Experiência de suporte	●●●●●
Preços	●●●●●
Geral	●●●●●

Fonte: Aite Group

Sobre o Suporte Técnico

Vale ressaltar que fornecemos suporte técnico a todos os clientes da Darktrace, sem nenhum custo adicional. De acordo com conversas com um cliente da Darktrace, Knight observou:

"O cliente não teve nenhuma reclamação sequer sobre a sua interação com o suporte técnico da Darktrace. Ao contrário de outros fornecedores com os quais trabalhou, todos os engenheiros de suporte com os quais interagiu ao longo de seu relacionamento de três anos com a Darktrace foram engenheiros experientes, com ampla experiência em análise de eventos."

"A princípio, um cliente receberá um analista dedicado ao seu caso e, na experiência do cliente, a empresa enviou um analista experiente com profundos conhecimentos da análise de eventos de segurança e do próprio produto em si. De acordo com a experiência do cliente com a equipe de suporte, os engenheiros da Darktrace sempre demonstraram profundos conhecimentos de pacotes, portas, ameaças etc., o que não é algo tipicamente encontrado nos fornecedores com os quais trabalhou no passado. A Darktrace foi muito presente no primeiro mês em que o cliente ficou com o dispositivo."

> "Minha nota geral para a solução Darktrace é cinco, a nota máxima, sendo essa a primeira vez que dou uma pontuação perfeita a qualquer fornecedor."
>
> **- Aite Group**

Conclusão

Darktrace é a inventora dos sistemas de IA de autoaprendizagem paradefesa cibernética e, por capitalização de mercado e número de clientes, é a líder inquestionável do setor. Temos o conjunto mais amplo de produtos para oferecer suporte a toda a sua estrutura de negócios, com uma área de desenvolvimento de produtos extremamente dinâmica e com altos investimentos. Avanços recentes como o AI Analyst, apenas seis meses após o lançamento da Antigena Email, mostram que a nossa disposição e capacidade de resolver problemas dos clientes no mundo real são enormes.

Temos orgulho de ser uma das principais empresas de tecnologia do mundo com operações de abrangência global. Os especialistas e analistas do setor concordam que, apesar de outras tecnologias estarem começando a adotar a nossa abordagem, nenhuma delas foi capaz de desenvolver a competência, a capacidade de implantação e a facilidade de uso palas quais somos reconhecidos como líderesno mundo todo. Com mais de 3.000 clientes em todos os setores, nossa plataforma está transformando a maneira como as empresas estão protegendo sua infraestrutura digital.

Diferenciadores Principais

A Darktrace é a única plataforma que:

- Aprende o que é normal 'na prática' para detectar ataques inéditos e ameaças internas
- Oferece uma proteção unificada e sob medida para e-mails, nuvem, IoT e rede
- Neutraliza ataques, com velocidade extrema e precisão cirúrgica
- Automatiza investigações de ameaças com velocidade e abrangência, reduzindo em 92% o tempo de triagem

> "A capacidade da Darktrace de enxergar e responder de maneira autônoma aos 'known knowns' e aos 'known unknowns' (os conhecidos que já conhecemos e os desconhecidos que já conhecemos) é incomparável com qualquer outro produto existente no mercado, e é por isso que a Darktrace alcançou a liderança na competição de análises de ameaças de redes."
>
> **- Aite Group**

Para mais informações:

Agendar uma demonstração

Baixar a Antigena Artigo tecnico

Ouça nossos clientes