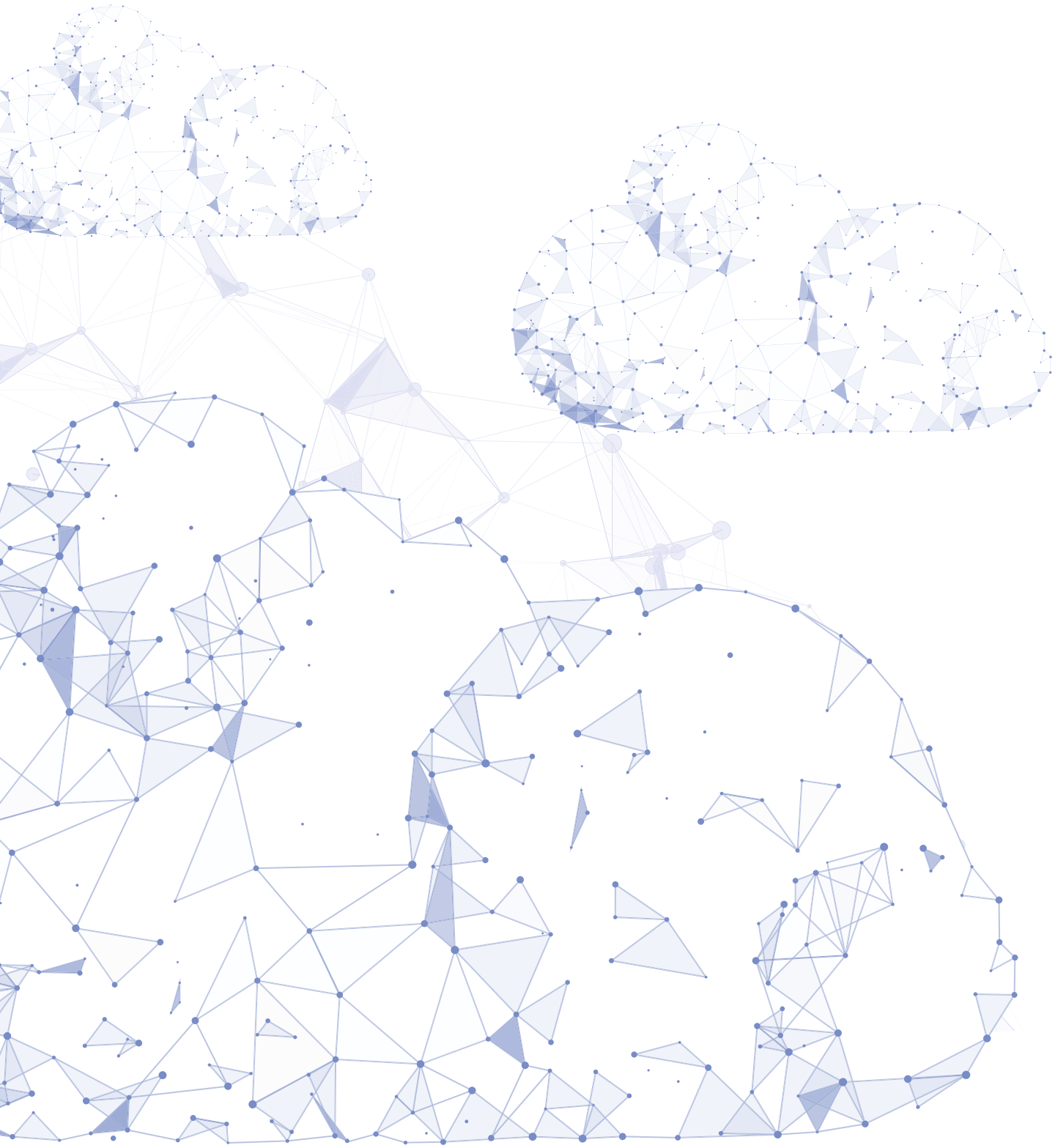
DARKTRACE



IA cibernética da Darktrace

Um sistema imunológico para segurança na nuvem

> À medida que as organizações aumentam seus recursos digitais em ambientes híbridos, com várias nuvens e de IoT, elas enfrentam mais áreas para proteger e controlar. Isso significa também mais oportunidades para os criminosos danificarem a confiabilidade operacional, empreenderem novos tipos de crimes e afetarem diretamente o funcionamento de uma empresa.
>
> – Forrester

Introdução

Conteúdo

Desde pequenas empresas que buscam reduzir custos até centros de inovação corporativos que lançam projetos de transformação digital, a jornada em larga escala para a nuvem reformulou fundamentalmente os negócios digitais e o paradigma tradicional do perímetro de redes. À medida que esse perímetro se dissolve, a infraestrutura híbrida e de várias nuvens se torna parte da mobília de uma área digital cada vez mais diversificada, capacitando as organizações a ultrapassar os limites superiores da inovação enquanto expandem a superfície de ataque a um ritmo alarmante.

Obviamente, essa tendência representa uma faca de dois gumes da era digital, e os desafios de segurança que os líderes empresariais devem enfrentar em sua jornada para a nuvem são difíceis de avaliar. A "nuvem" em si envolve uma ampla variedade de sistemas e serviços, e uma única equipe de segurança pode ser responsável por proteger cargas de trabalho em nuvem no AWS e Azure, em comunicações por e-mail no Microsoft 365, em dados de clientes no Salesforce, em compartilhamento de arquivos pelo Dropbox e em servidores virtualizados em centrais de dados tradicionais no local.

Esse complexo quebra-cabeças de plataformas baseadas na nuvem geralmente impulsiona a eficiência, flexibilidade e inovação à custa de uma estratégia de segurança coerente e tratável. A nuvem, em todas as suas diversas formas, é um território desconhecido para equipes de segurança tradicionais, e as ferramentas e práticas anteriores são geralmente muito lentas, em silos ou nem mesmo aplicáveis para defender ambientes híbridos e de várias nuvens contra ataques avançados.

Embora muitas soluções de segurança nativas da nuvem possam auxiliar com análises de conformidade e registros, elas raramente são robustas e unificadas o bastante para fornecer cobertura suficiente – pois, além de continuar a incentivar uma abordagem de segurança obsoleta, recorrem a regras, assinaturas ou suposições anteriores e, portanto, não são capazes de indentificar novas ameaças e agentes internos sutis antes que tenham tempo de se transformar em uma crise.

Pior ainda, a falta de visibilidade e controle que as equipes de segurança enfrentam nessa área – juntamente com a mentalidade nova e não familiar que a agilidade e velocidade da nuvem requerem – também a tornam um alvo atraente para os criminosos cibernéticos que invariavelmente buscam gerar lucros máximos enquanto evitam a detecção. A segurança na nuvem não avançou o suficiente e os criminosos cibernéticos sabem muito bem disso.

No entanto, em muitos aspectos, as organizações atuais precisam mais do que apenas segurança na nuvem, precisam de segurança em toda a empresa e de uma plataforma unificada que possa operar na velocidade dos negócios digitais, adaptar-se a ameaças futuras e correlacionar as características sutis de um ataque avançado à medida que amplia sua presença em uma rede.

A Plataforma de IA Cibernética

Limitações da abordagem em silos para segurança na nuvem

Os prestadores de serviços em nuvem e fornecedores externos oferecem uma variedade de soluções de segurança "nativas da nuvem" que ajudam os clientes a defender sua parcela do modelo de responsabilidade compartilhada. No entanto, essas soluções pontuais – sejam nativas ou externas – geralmente são mal preparadas para detectar e responder a ameaças avançadas na nuvem.

Controles nativos: Necessários, mas insuficientes

Os controles de segurança nativos geralmente são projetados exclusivamente para um único provedor de nuvem, oferecendo cobertura para apenas uma parte de uma ampla empresa híbrida e de várias nuvens. Isso limita drasticamente o escopo de detecção e adiciona complexidade a uma segurança já complexa.

Em geral, os controles nativos podem ajudar na conformidade, coleta de registros e criação de políticas estáticas, mas não foram projetados para detecção e resposta avançadas a ameaças em vários silos e serviços de nuvem.

Controles de terceiros: úteis, mas insuficientes

Controles de terceiros, como CASBs e CWPPs, também são úteis, mas insuficientes. Os CASBs, por exemplo, podem ajudar na descoberta, criação de políticas granulares e conformidade, mas geralmente não conseguem detectar ameaças cibernéticas que ocupam a extremidade mais avançada do espectro - desde credenciais comprometidas e ransomware, até funcionários insatisfeitos e espionagem corporativa.

Embora os controles de terceiros ofereçam normalmente visibilidade em toda a nuvem, eles não têm nenhum conhecimento da rede física de uma organização. Trata-se de uma limitação significativa – correlacionar percepções da nuvem e da rede corporativa é frequentemente a única maneira de um sistema de segurança identificar a presença de uma ameaça emergente.

Um sistema imunológico que vá além da nuvem

Acionada por inteligência artificial, a Cyber AI Platform da Darktrace preenche essas lacunas críticas com uma abordagem exclusiva a nível da empresa, detectando e respondendo a ameaças baseadas na nuvem que outras ferramentas não identificam.

Semelhante ao sistema imunológico humano, a tecnologia desenvolve um senso inato de "self", aprendendo o "padrão de vida" normal para cada usuário, dispositivo e contêiner em ambientes híbridos e com várias nuvens. Com a análise contínua do comportamento de todos e de tudo na empresa, a IA de autoaprendizagem da Darktrace pode correlacionar de modo único os sinais fracos e sutis de um ataque avançado, sem definir com antecedência o que é "benigno" ou "mal-intencionado".

Embora as soluções pontuais pré-programadas possam certamente complementar essa abordagem, a Darktrace é a única tecnologia comprovada que interrompe toda a ampla variedade de ameaças cibernéticas na nuvem, desde funcionários mal-intencionados e ataques externos até configurações críticas incorretas que podem expor a empresa a um futuro comprometimento – independentemente de se originarem de campanhas direcionadas de spear-phishing, aquisições de controle de contas corporativas, ou exfiltração lenta e discreta de dados ou movimentação lateral na nuvem.

Proteção unificada e sob medida

Com um entendimento da propriedade digital de toda a empresa, a Darktrace correlaciona todas as atividades no local com o tráfego em ambientes híbridos e com várias nuvens em tempo real. Isso permite entender que um comportamento normal observado isoladamente na nuvem pode apontar para uma imagem maior da atividade mal-intencionada.

Por exemplo, podemos ver que um usuário fez login no AWS na nuvem. Isoladamente, esse evento não é mal-intencionado, mas a Darktrace também sabe que a conta do Microsoft 365 do mesmo usuário provavelmente foi comprometida momentos antes, pois um local de logon altamente incomum foi detectado. A Darktrace entende que a conexão ao AWS é de fato altamente suspeita.

> Os líderes de segurança cada vez mais pretendem melhorar sua eficiência desmembrando produtos pontuais em plataformas de segurança mais amplas.
>
> **– Gartner**

Correlação de informações em nível de contêiner

Apesar da crescente adoção de contêineres pelos desenvolvedores, a segurança geralmente fica para trás. A natureza virtualizada dos contêineres dificulta o monitoramento do tráfego no servidor. Enquanto os sistemas baseados em regras rastreiam dados somente em servidores, a Darktrace tem a capacidade de proporcionar visibilidade nos ambientes em contêineres com servidores individuais.

Fundamentalmente, a Darktrace estende a visibilidade desse contêiner e o conecta à atividade em toda a infraestrutura digital (ambientes industriais, em nuvem, de IoT, e-mail e todos os outros). Uma anomalia no tráfego de rede de um contêiner pode, portanto, ser vinculada a um banco de dados em nuvem, que pode ser correlacionado a conta de e-mail de uma empresa.

Consulte na página 14 cenários de implantação

AI Analyst: investigação automatizada de ameaças

O Cyber AI Analyst dá um passo adiante ao investigar automaticamente as ameaças detectadas pelo Enterprise Immune System e produzir um painel situacional dinâmico, além de relatórios gerados pela IA que comunicam todo o escopo de um incidente de segurança.

Ao correlacionar o tráfego da nuvem em tempo real com o restante da rede, o AI Analyst pode realizar centenas de investigações simultaneamente, reunindo vários alertas e indicadores e desenvolvendo uma compreensão significativa dos incidentes com extrema rapidez. Depois, ele comunica seus resultados e recomendações na forma de incidentes do AI Analyst, que são enriquecidos com informações contextuais e de segurança que podem ser analisadas e acionadas por executivos e usuários finais.

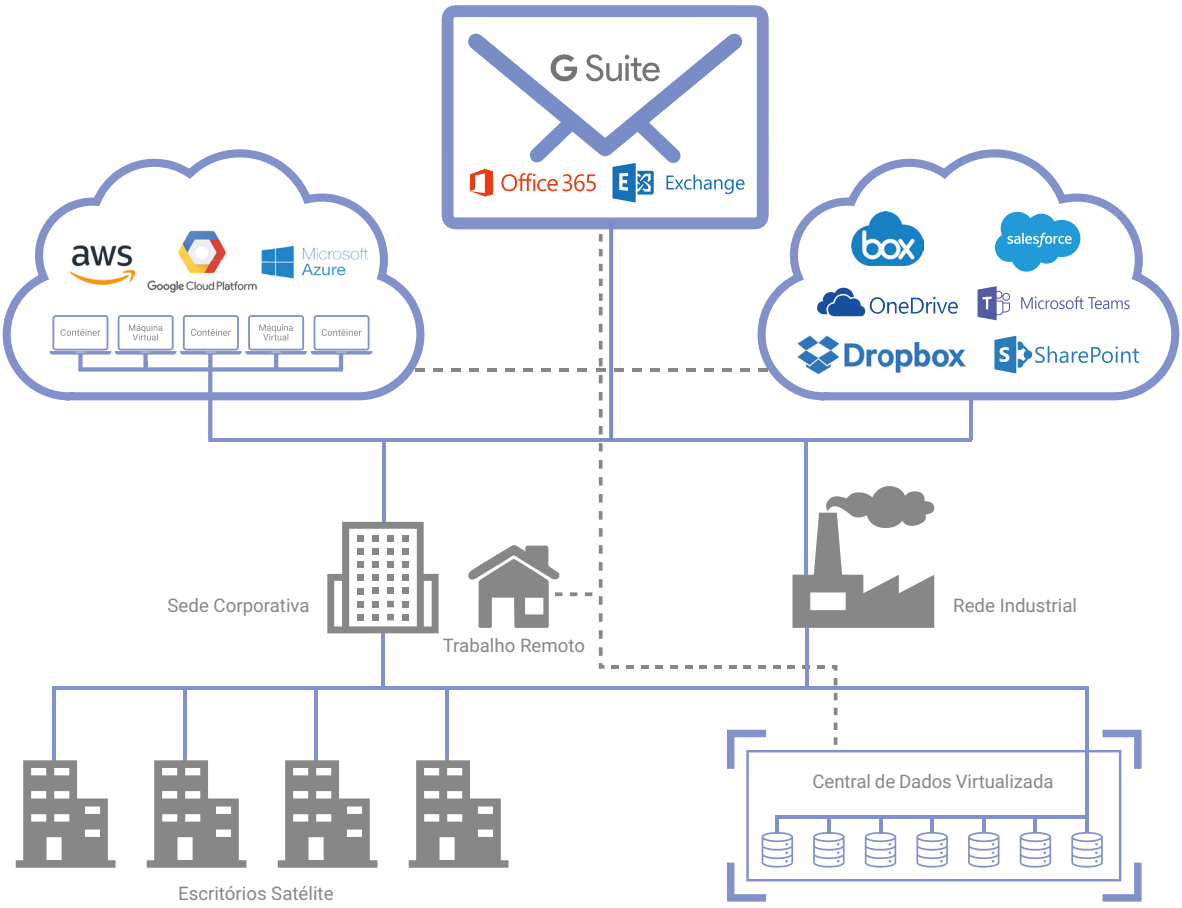


Figura 1: Cobertura unificada da Darktrace de todo o acervo digital

Credenciais comprometidas

29% das violações de dados envolvem o uso de credenciais roubadas

Fonte: Verizon 2019

Os criminosos cibernéticos avançados podem roubar credenciais de contas corporativas de várias maneiras, desde ataques de engenharia social a malware "inteligente" que vasculha o tráfego e os ativos efêmeros da nuvem em busca de senhas. Com os dados roubados disponíveis para compra e venda na Dark Web, a frequência e a gravidade do roubo de credenciais estão aumentando a cada ano.

Os casos de aquisição de controle de contas abrangem apenas o primeiro estágio de uma ameaça cibernética. O objetivo final de um ataque baseado em credenciais é o uso real de senhas comprometidas para autenticar aplicativos e roubar dados. Uma vez que um invasor tem as credenciais para operar como um usuário válido, pouco pode ser feito para distinguir entre um invasor e o funcionário legítimo pelo qual ele está se passando.

Ao correlacionar dados entre ambientes híbridos e com várias nuvens, a Darktrace aprende o "padrão de vida" de cada usuário a partir de centenas de métricas, permitindo detectar imediatamente desvios no comportamento que são indicativos de uma aquisição de controle de conta. Mesmo em casos em que há um comprometimento preexistente, ao aprender o "padrão de vida" do grupo de colegas desse usuário, bem como de toda a empresa, a IA da Darktrace sinalizará retrospectivamente qualquer comportamento incomum.

Figura 2: A IA da Darktrace detecta atividade incomum relacionada a conta na nuvem comprometida

Ataque ao SharePoint

Depois de obter credenciais roubadas ou acesso ao serviço de transferência de arquivos baseado na nuvem de uma organização, os criminosos cibernéticos frequentemente executam scripts para identificar arquivos que contenham palavras-chave como "senha". A Darktrace descobriu um desses incidentes em um banco europeu, onde os invasores conseguiram encontrar um arquivo do Microsoft 365 SharePoint que armazenava senhas não criptografadas. Tendo já contornado os controles nativos da Microsoft, os invasores acreditavam que já estavam à salvo.

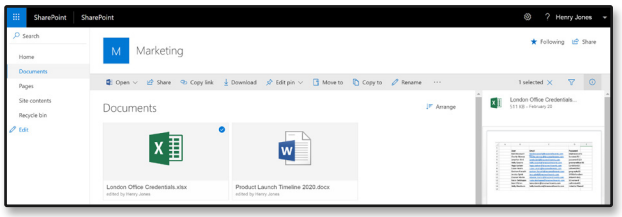


Figura 3: Arquivos confidenciais acessados no SharePoint

No entanto, a IA da Darktrace sinalizou a atividade como anômala para o usuário corporativo, seu grupo de colegas e a organização em geral, detectando o acesso incomum a esses arquivos confidenciais, entre outros indicadores. Por fim, a compreensão diferenciada e em constante evolução da IA sobre o que é "normal" em toda a organização se mostrou essencial, pois o acesso suspeito a arquivos pode muito bem ter sido benigno em outras circunstâncias.

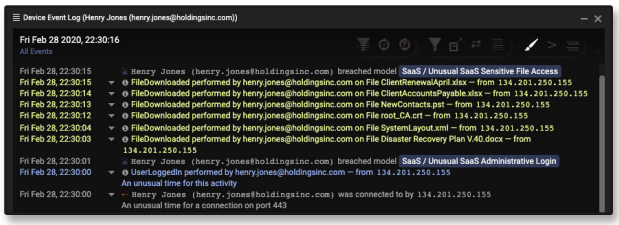


Figura 4: A Darktrace traz à tona downloads de arquivos confidenciais

Esses invasores provavelmente teriam aproveitado as senhas de texto não criptografado para aumentar seus privilégios e se infiltrar ainda mais na organização. No entanto, aprendendo "padrões de vida" exclusivos para todos os usuários e dispositivos da organização, a IA da Darktrace alertou a equipe de segurança sobre o incidente antes que ele se transformasse em uma crise.

Tentativa de login no SaaS do Equador

Em uma organização internacional, a Darktrace identificou um comprometimento em uma conta do Microsoft 365 que contornou os controles nativos do Azure Active Directory. Como a organização tinha escritórios em todos os cantos do mundo, a IA da Darktrace identificou um login de um endereço IP historicamente incomum para esse usuário e seu grupo de colegas e alertou imediatamente a equipe de segurança. A Darktrace alertou para o fato de que uma nova regra de processamento de e-mails, que apaga e-mails recebidos, foi configurada na conta. Isso era um indicador claro de comprometimento e a equipe de segurança conseguiu bloquear a conta antes que o invasor causasse danos.

Quando a equipe de segurança fez uma investigação mais aprofundada do incidente, descobriu que o usuário havia recebido um e-mail de phishing algumas horas antes da Darktrace detectar a ameaça. Embora a empresa também tenha implantado a Proteção Avançada contra Ameaças (do inglês Advanced Threat Protection, ATP) da Microsoft para o Microsoft 365, defesas estáticas, como a ATP, apenas são capazes de detectar ataques de phishing correlacionando links em e-mails com endereços mal-intencionados conhecidos, e o link de phishing não apareceu na lista. Isso demonstrou as limitações claras de uma abordagem baseada em assinaturas nessa área, e a organização logo implantou a tecnologia Autonomous Response da Darktrace, a Antigena, para proteção adicional no Microsoft 365, dada sua capacidade de detectar e-mails de phishing com ameaças semelhantes sem depender de listas negras.

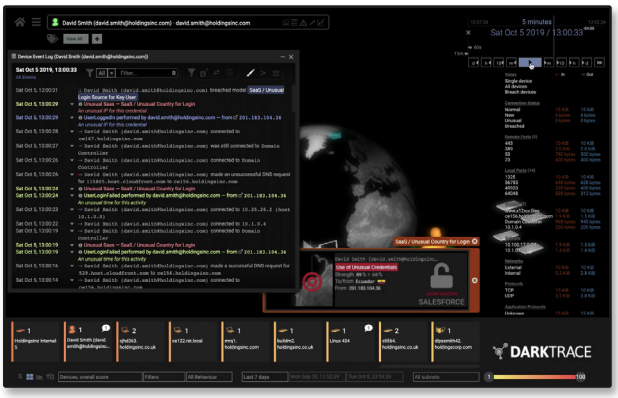


Figura 5: A IA da Darktrace detecta o local incomum de login do SaaS

Login incomum no Banco do Panamá

Uma conta do Microsoft 365 foi usada em um ataque de força bruta contra um banco conhecido no Panamá, com logins originários de um país que se desviava dos "padrões de vida" normais das operações da empresa.

A Darktrace identificou 885 logins durante um período de 7 dias. Embora a maioria das autenticações se originasse de endereços IP no Panamá, 15% das autenticações tinham origem em um endereço IP 100% raro e localizado na Índia. Uma análise adicional revelou que esse endpoint externo foi incluído em várias listas negras de spam e que havia sido associado recentemente a comportamentos abusivos on-line – possivelmente varreduras não autorizadas na Internet ou atividades de hackers.

Figura 6: A interface do usuário mostrando os locais de login

A Darktrace então testemunhou o que parecia ser um abuso da função de redefinição de senha, pois foi observado que o usuário na Índia alterava os privilégios da conta de uma maneira altamente incomum. O que marcou a atividade como particularmente suspeita foi o fato de, após a redefinição da senha, terem sido observadas tentativas malsucedidas de login de um IP normalmente associado à organização, sugerindo que o usuário legítimo foi bloqueado.

03/12 20:45:39	Saas::Admin	Regular	UpdateUser
03/12 20:45:39	Saas::Admin	Regular	ChangeUserLicense
03/12 20:26:43	Saas::Login	Regular	UserLoggedIn
03/12 20:26:43	Saas::FailedLogin	Regular	UserLoginFailed
03/12 20:26:36	Saas::FailedLogin	Regular	UserLoginFailed
03/12 18:31:31	Saas::Login	Regular	UserLoggedIn
03/12 17:57:46	Saas::Admin	Regular	ChangeUserLicense
03/12 17:57:46	Saas::Admin	Regular	UpdateUser
03/12 17:06:57	Saas::Admin	Regular	UpdateUser

Figura 7: A atividade associada à conta SaaS, destacando as credenciais alteradas

Ataque automatizado de força bruta

A Darktrace detectou vários eventos de login malsucedidos em uma conta SaaS diariamente ao longo de uma semana. Cada lote de tentativas de login era realizado exatamente às 18h40 em seis dias. A consistência na hora do dia e no número de tentativas de login era indicativa de um ataque automatizado de força bruta, programado para ser interrompido após um certo número de tentativas malsucedidas para evitar bloqueios.

A Darktrace considerou esse padrão de tentativas malsucedidas altamente anômalo e, portanto, alertou a equipe de segurança. Se a Darktrace não correlacionasse vários indicadores fracos e acionasse sinais sutis de ameaça emergente, esse ataque automatizado poderia ter continuado por semanas ou meses, possibilitando suposições fundamentadas sobre a senha dos usuários com base em outras informações já coletadas.

Figura 8: Um gráfico que ilustra as tentativas repetidas de login

Aquisição do controle de conta do Microsoft 365

Depois de clicar em um link mal-intencionado em um e-mail direcionado, um funcionário inseriu suas credenciais em uma página de login falsificada que registrava as teclas digitadas. Agora, munidos de suas credenciais, os invasores retornaram ao Microsoft 365 e usaram as credenciais para fazer o login remotamente. A Darktrace detectou os locais incomuns: Bulgária e Indonésia.

Aprendendo os padrões de onde os usuários trabalham e de quando e como acessam os serviços na nuvem, a IA da Darktrace identificou, e poderia ter impedido, essas solicitações incomuns de login. Nesse caso, os recursos de segurança nativos não identificaram nem impediram esses logins mal-intencionados.

Depois de entrarem na conta do Microsoft 365 do funcionário, os invasores se propagaram para mais vítimas, continuando o ciclo. Aqui, a Darktrace testemunhou outra mudança de comportamento, testemunhando 99 e-mails com a linha de assunto "aviso de remessa" sendo enviados para diversas empresas. Embora esse comportamento possa ser normal para alguns funcionários, estava fora do padrão de vida desse usuário específico.

A Darktrace observou também a criação de uma nova regra de encaminhamento de caixa de entrada – geralmente criada por invasores para espalhar spam ou ocultar suas atividades.

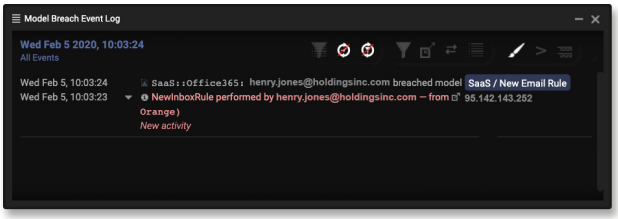


Figura 9: A Darktrace detecta a regra de processamento de caixa de entrada

Com a exclusão automática de e-mails após o envio, o rastro de provas é destruído no sistema de e-mail. No entanto, com o monitoramento independente dos e-mails e das atividades da conta SaaS, a Darktrace obteve um panorama completo das atividades do invasor. A capacidade da plataforma de aprender identidades e comportamento em toda a empresa permitiu detectar a atividade suspeita.

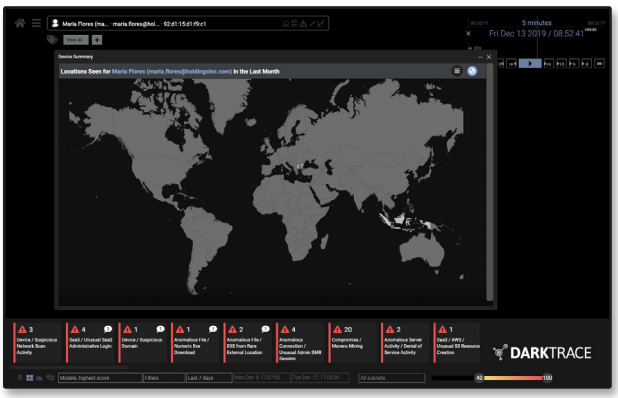


Figura 10: Os locais incomuns de login

Funcionários mal-intencionados

> A IA da Darktrace se adapta durante o trabalho, protegendo nossa infraestrutura de rede e nuvem em tempo real e permitindo que defendamos a nuvem com confiança
>
> **CISO, Aptean**

As ameaças internas na nuvem geralmente representam mais ameaças cibernéticas para as organizações do que invasores externos, pelo motivo óbvio: já estão dentro. Um funcionário com intenções nefastas está em uma posição única para burlar as ferramentas tradicionais devido ao seu acesso privilegiado e conhecimento profundo da rede.

Os serviços em nuvem expandiram amplamente o escopo das ameaças internas, com o grande número de aplicativos apresentando uma variedade de vetores para a exfiltração de dados e a visibilidade limitada nesse domínio, permitindo que a exfiltração de dados passe despercebida.

Por natureza, as ferramentas de segurança herdadas não identificam as atividades mal-intencionadas que já ocorrem na organização. A segurança na nuvem agora exige uma abordagem mais abrangente que analise o tráfego em toda a área digital e construa continuamente um "padrão de vida" em evolução constante para a organização.

Independentemente de ser um vendedor saindo da empresa e levando informações de clientes com ele ou um administrador de TI descontente manipulando sutilmente dados críticos, a inteligência artificial pode ser usada para detectar qualquer atividade anômala e incomum que indique uma ameaça cibernética.

Figura 11: Funcionário de TI insatisfeito

Funcionário de TI insatisfeito

A Darktrace testemunhou um caso de ameaça interna depois que um funcionário foi demitido de seu cargo de administrador de sistemas de TI. A organização havia sido forçada a fazer uma série de demissões no escritório naquela semana, mas esqueceu de pegar o laptop do funcionário ou excluir sua conta corporativa. O ex-administrador de TI fez login na conta SaaS e baixou rapidamente muitos arquivos confidenciais, inclusive detalhes de contato e números de cartão de crédito, do banco de dados de clientes.

Figura 12: O Threat Visualizer mostrando um grande aumento no número de conexões

Eles então tentaram transferir secretamente esses arquivos para um servidor doméstico usando um dos serviços regulares de transferência de dados da empresa. Antes disso, eles criaram uma nova conta para gerar uma porta dos fundos, garantindo que eles ainda mantivessem sua presença na empresa depois que a equipe de TI finalmente conseguisse fechar a conta corporativa.

O administrador de TI sabia que esse serviço específico não era apenas sancionado pelas políticas corporativas, mas também baseado na nuvem, e pressupôs que a equipe de segurança teria visibilidade limitada nessa área. Contudo, a Darktrace analisa dinamicamente logins e eventos de acesso a arquivos nos serviços corporativos na nuvem, correlacionando-os com os "padrões de vida" aprendidos sobre todos os usuários da organização à luz de novas evidências. Como um sistema unificado de autoaprendizagem, a Cyber AI Platform da Darktrace captou imediatamente os downloads de arquivos extraordinariamente grandes, a criação de novas contas e a exfiltração, e sua tecnologia Autonomous Response, a Antigena, entrou em ação para bloquear a tentativa de upload.

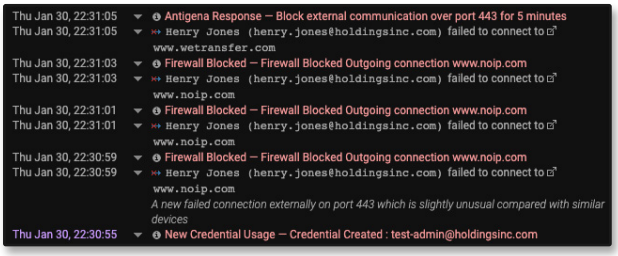


Figura 13: A Darktrace Antigena acionando uma resposta autônoma direcionada

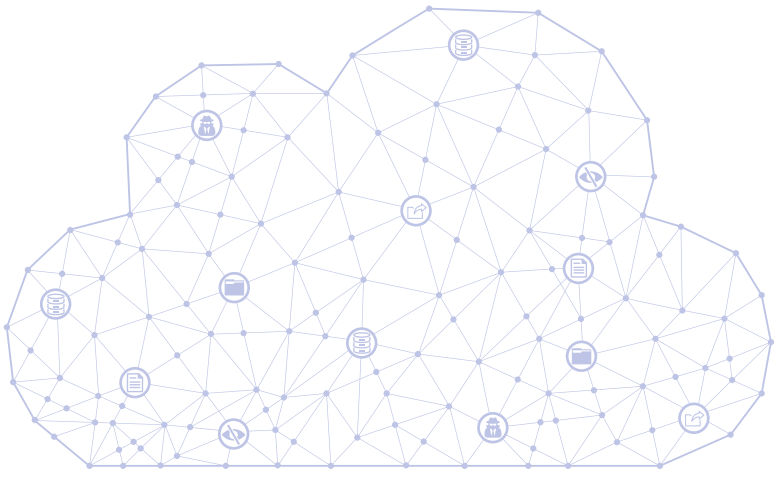
A investigação subsequente revelou que o funcionário tentou primeiro enviar esses arquivos para um servidor pessoal em casa. Quando isso não funcionou, ele tentou continuamente exfiltrar os dados para várias outras fontes. No entanto, como a Antigena pode se adaptar dinamicamente às ameaças à medida que elas se desdobram e aumentar sua resposta na mesma proporção, ela pôde interromper com precisão essas tentativas em todas as situações.

Quando todas as tentativas falharam, o funcionário tentou transferir todos os arquivos para um servidor interno que ele costumava usar na empresa na tentativa de enviar os arquivos a partir desse local, mas a Darktrace interveio e neutralizou também essa conexão.

Figura 14: A Antigena bloqueia a tentativa de funcionários de transferir arquivos pela nuvem

Enquanto essa atividade sutil evitava facilmente os controles nativos do provedor de nuvem, a IA da Darktrace detectou o comportamento ameaçador em segundos. Como aprende continuamente o "normal" para cada usuário e dispositivo, o sistema conseguiu correlacionar de modo inteligente conexões e downloads altamente suspeitos do dispositivo do administrador de TI, mesmo que o serviço na nuvem tenha sido usado regularmente para fins legítimos por outros funcionários.

A Plataforma de IA da Darktrace alertou instantaneamente a equipe de segurança e forneceu informações detalhadas e precisas sobre a natureza do comprometimento, levando-os a revogar as credenciais, além de recuperar e proteger rapidamente os dados.



Erro de configuração

> Quase todos os ataques bem-sucedidos a serviços na nuvem resultam de erros de configuração do cliente.
>
> **– Neil MacDonald, Gartner**

A configuração de controles de segurança em ambientes híbridos e com várias nuvens é geralmente um processo complexo, pois as soluções nativas e externas nessa área são variadas, incompatíveis e insuficientes. A falta de familiaridade com a nuvem geralmente leva a configurações incorretas críticas que expõem os negócios a ataques. Os desenvolvedores modernos agora podem criar uma instância de nuvem em minutos, geralmente sem precisar consultar a equipe de segurança da empresa. Como consequência, a maioria das organizações não tem visibilidade de seus próprios ambientes de nuvem, e as instalações apressadas podem resultar na abertura de lacunas de vulnerabilidade que passam despercebidas por meses.

As possíveis ramificações de uma configuração incorreta surgiram com a violação de dados da Capital One, que afetou mais de 100 milhões de pessoas ao explorar uma vulnerabilidade na nuvem. Essa importante instituição financeira com uma postura madura de segurança na nuvem foi informada somente após receber uma dica de alguém de fora que havia encontrado os dados roubados três meses após a violação.

A inteligência artificial agora é usada para entender os "padrões de vida" normais para cada usuário, dispositivo e contêiner, reconhecendo os padrões sutis de comportamento associados a uma configuração incorreta. Com o emprego da tecnologia de autoaprendizagem como a Cyber AI Platform da Darktrace, as organizações podem obter o conhecimento necessário de ambientes complexos de nuvem para identificar vulnerabilidades latentes em seus estágios iniciais, antes de se transformarem em crises.

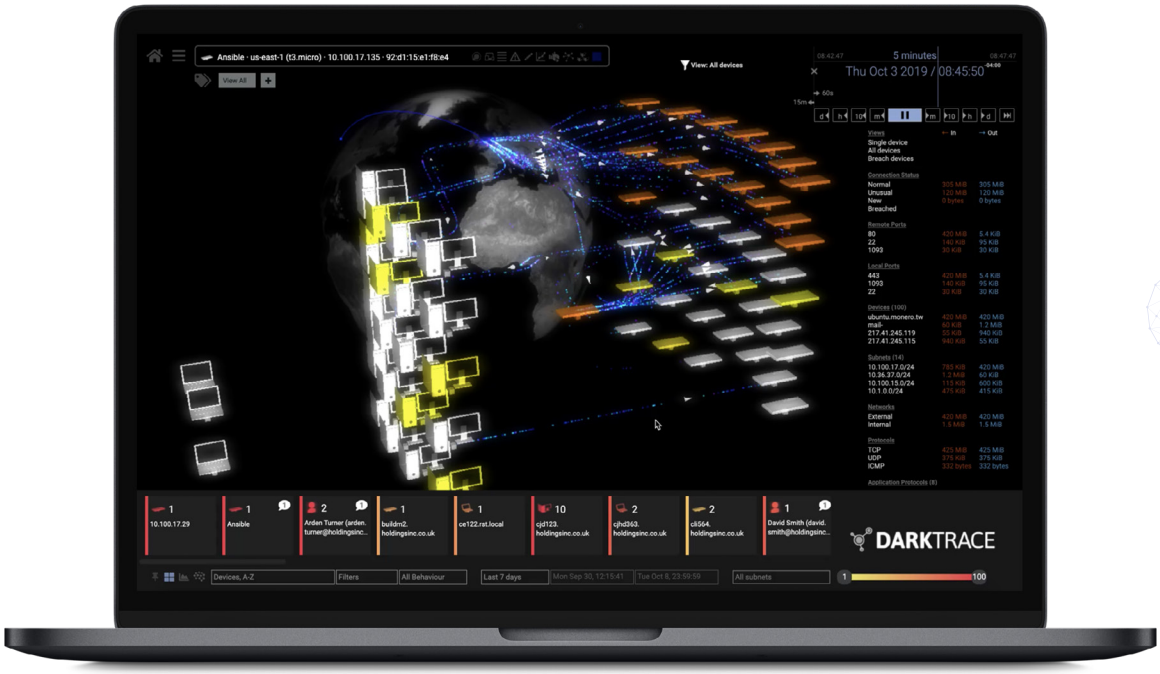


Figura 15: Um erro de configuração no DevOps que leva à rápida disseminação de malware de mineração de criptografia

Ataque do Shodan à vulnerabilidade na nuvem

Uma empresa de serviços financeiros hospedava vários servidores críticos em máquinas virtuais na nuvem, alguns dos quais eram para estar voltados ao público e outros não. Ao configurar os controles da nuvem nativa, eles erroneamente deixaram um servidor importante exposto à Internet quando ele deveria estar isolado por trás de um firewall. Isso poderia ter acontecido por vários motivos, possivelmente por causa de uma migração rápida e caótica, ou possivelmente devido à falta de familiarização com os controles nativos fornecidos pelo seu CSP.

Enquanto a equipe de segurança desconhecia completamente a configuração incorreta, o servidor exposto acabou sendo descoberto e foi alvo de criminosos cibernéticos que faziam uma varredura da Internet por meio da Shodan. Em segundos, a IA da Darktrace detectou que o dispositivo estava recebendo uma quantidade incomum de tentativas de conexão de uma grande variedade de fontes externas raras e alertou a equipe de segurança sobre a ameaça.

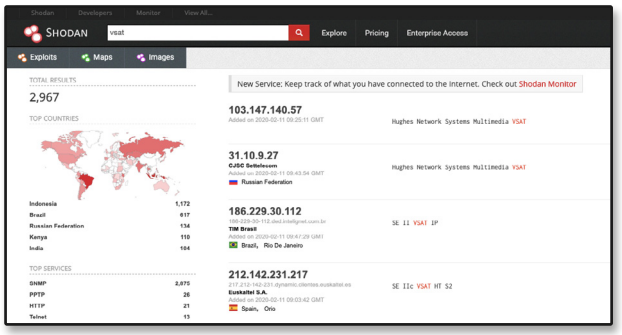


Figura 16: O site da Shodan foi usado para varredura de vulnerabilidades

PII não criptografadas na AWS

A administração de uma cidade dos EUA no processo de terceirização de bancos de dados para o AWS não consultou adequadamente os protocolos que o servidor usava para baixar informações. Como resultado, os endereços, números de telefone e números de registro de veículos de seus cidadãos estavam sendo carregados em um banco de dados externo por meio de conexões não criptografadas.

Esses dados altamente confidenciais destinavam-se ao acesso limitado por funcionários selecionados da administração da cidade, mas um lapso da segurança disponibilizou os dados a qualquer invasor capaz de fazer uma varredura no perímetro da rede e coletar os pacotes repletos de dados que apareciam.

A organização não tinha inicialmente conhecimento da configuração incorreta, que permanecia despercebida para a segurança. No entanto, quando a Darktrace detectou uma conexão incomum com um IP externo raro de um dispositivo de desktop dentro da empresa, verificou que essa comunicação estava revelando dados públicos confidenciais, que poderiam ser acessados por um invasor a fim de coletar material para futuros ataques de spear-phishing ou mesmo falsificação de identidade. A visibilidade completa e em tempo real fornecida pela Darktrace revelou esse ponto cego perigoso e permitiu à equipe de segurança corrigir a configuração incorreta.

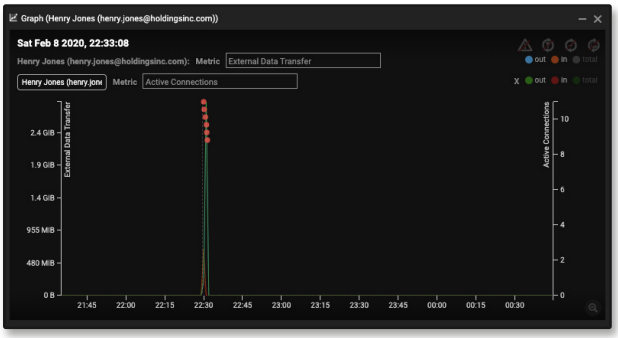


Figura 17: O Threat Visualizer mostrando mais de 2 GB de dados sendo transferidos externamente

Malware de mineração de criptomoedas instalado inadvertidamente

A Darktrace detectou um erro de um engenheiro júnior de DevOps em uma organização multinacional com cargas de trabalho no AWS e no Azure e aproveitou sistemas em contêineres como Docker e Kubernetes. O engenheiro baixou acidentalmente uma atualização que incluía um minerador de criptografia, o que levou a uma infecção em vários sistemas de produção na nuvem.

Após a infecção inicial, o malware começou a enviar beacons para o servidor externo de comando e controle, que foram capturados imediatamente pela Darktrace. Com a conexão externa estabelecida e as instruções da missão de ataque entregues, a infecção por malware de criptografia se espalhou rapidamente pela extensa infraestrutura de nuvem da organização, infectando 20 servidores em menos de 15 segundos.

Graças à IA da Darktrace, o ambiente de nuvem da organização não era um ponto cego, com uma visão dinâmica e unificada de toda a infraestrutura híbrida e com várias nuvens, permitindo à equipe de segurança conter o ataque em questão de minutos, em vez de horas ou dias. Embora o ataque se movesse com extrema rapidez, a Darktrace o capturou antes que os custos começassem a aumentar.

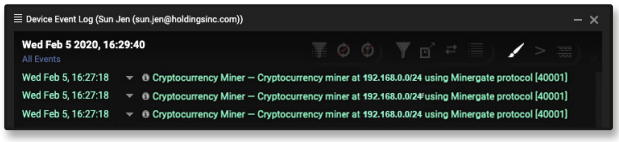


Figura 18: O malware de mineração de criptografia detectado em tempo real

IP exposto no Azure

Uma empresa de manufatura líder na Europa usava um servidor Microsoft Azure para armazenar arquivos que continham detalhes de produtos e projeções de vendas. Embora os arquivos no servidor e o IP raiz tenham sido protegidos com um nome de usuário e senha, esses dados confidenciais foram deixados sem criptografia. Uma atividade anômala foi detectada quando um dispositivo baixou um arquivo ZIP de um endereço IP externo raro que a Darktrace considerou altamente atípico.

Descobriu-se mais tarde que o IP externo era um servidor Microsoft Azure configurado recentemente e que o arquivo ZIP estava acessível a qualquer pessoa que conhecesse a URL, que poderia ter sido obtida simplesmente interceptando o tráfego de rede, interna ou externamente. Invasores mais dedicados poderiam ter forçado o parâmetro de chave do arquivo do URL.

A perda ou vazamento desses arquivos confidenciais poderia colocar toda uma linha de produtos em risco, mas, ao relatar esse incidente assim que foi detectado, a Darktrace ajudou a evitar a perda de valiosa propriedade intelectual e passou a ajudar a equipe de segurança na revisão de suas práticas de armazenamento de dados na nuvem para proteger melhor as informações de seus produtos no futuro.

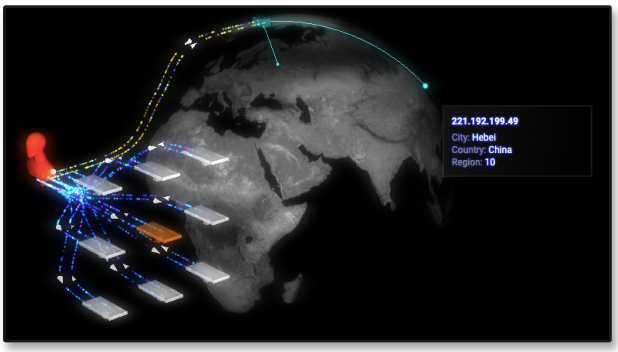
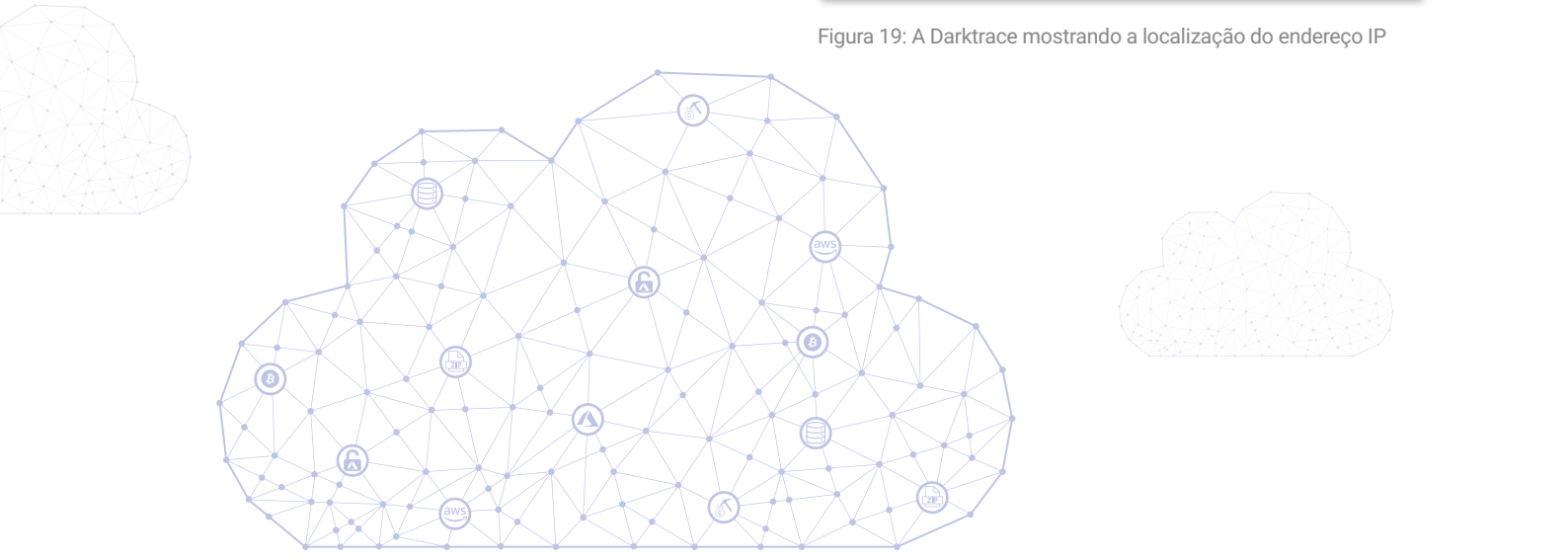


Figura 19: A Darktrace mostrando a localização do endereço IP



Engenheiro de DevOps extremamente cuidadoso

Em um grupo de seguros, um engenheiro de DevOps estava tentando criar uma infraestrutura de backup paralela no AWS para replicar os sistemas de produção da central de dados da organização. A implantação técnica foi perfeita e os sistemas de backup foram criados. No entanto, o custo de operação do sistema seria de vários milhões de dólares por ano.

O engenheiro de DevOps desconhecia os custos associados ao projeto e mantinha o gerenciamento em sigilo. A infraestrutura na nuvem foi lançada e os custos começaram a aumentar. No entanto, a IA da Darktrace alertou para esse comportamento incomum, e a equipe de segurança pôde tomar medidas preventivas imediatamente.

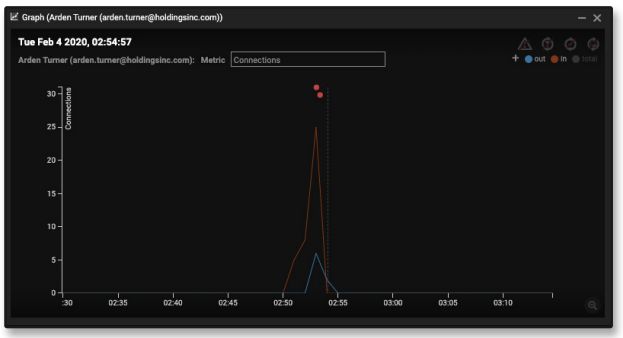


Figura 20: O Threat Visualizer mostrando um aumento nas conexões internas e externas

Cenários de implantação

Nuvem híbrida (IaaS)

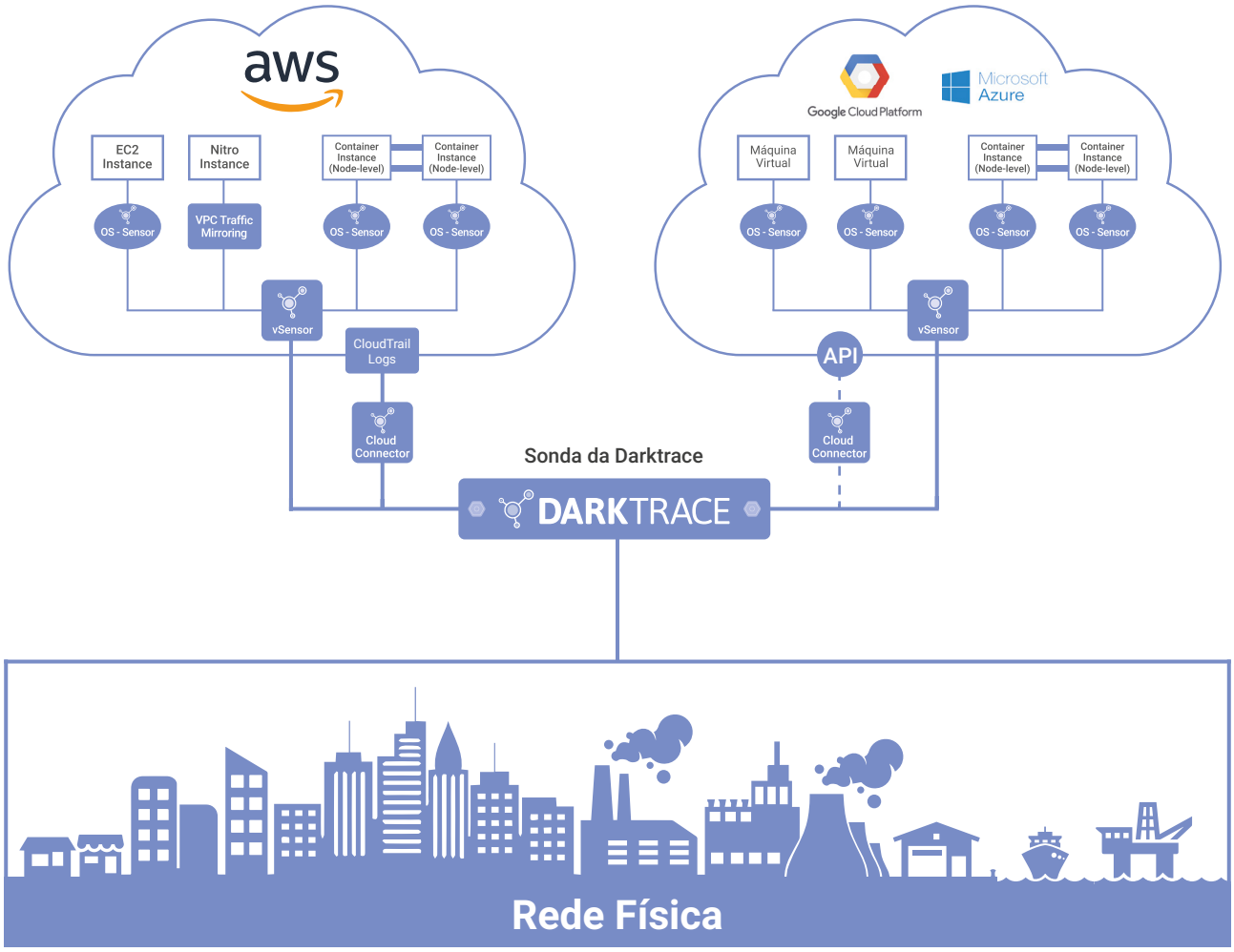
Para organizações com infraestrutura de nuvem híbrida, a Darktrace implanta sondas virtuais ou "vSensors" que capturam o tráfego em tempo real na nuvem e o correlacionam com o restante dos negócios.

Na AWS, os vSensors consomem tráfego em tempo real das instâncias do Nitro por meio do VPC Traffic Mirroring. Os metadados do AWS Nitro podem ser capturados diretamente, sem a necessidade de uma análise adicional em nível de servidor. Para instâncias que não são Nitro, a Darktrace implanta "OS-Sensors" em todos os terminais, sendo que cada OS-Sensor alimenta o tráfego para um vSensor local que, por sua vez, alimenta os metadados relevantes para uma sonda principal da Darktrace na nuvem ou na rede corporativa para análise.

Na Azure, GCP e outros, a Darktrace implanta vSensors e OS-Sensors para capturar tráfego em tempo real, conforme descrito acima. A Darktrace também é compatível com vTAP da Azure, e uma capacidade equivalente para o GCP está em desenvolvimento.

Os clientes da AWS e da Azure também podem implantar "Darktrace Connectors" para monitorar a atividade de administração do sistema em nível de API, como atividades de login e criação de recursos.

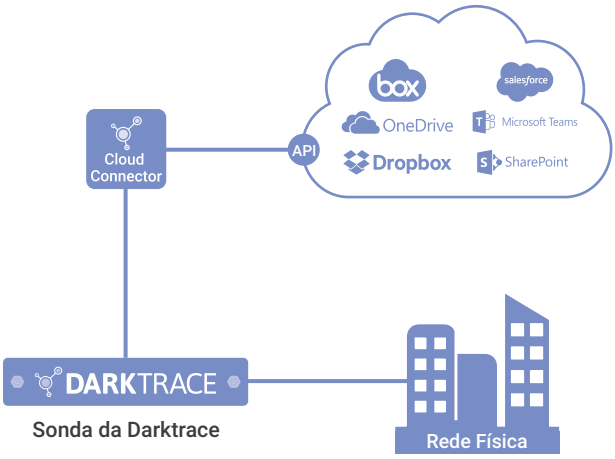
Finalmente, a Darktrace captura o tráfego de contêineres no Docker e no Kubernetes por meio de um OS-Sensor especializado, que alimenta os dados de maneira semelhante a um vSensor local e, por sua vez, uma sonda Darktrace principal para análise.



Nuvem híbrida (SaaS)

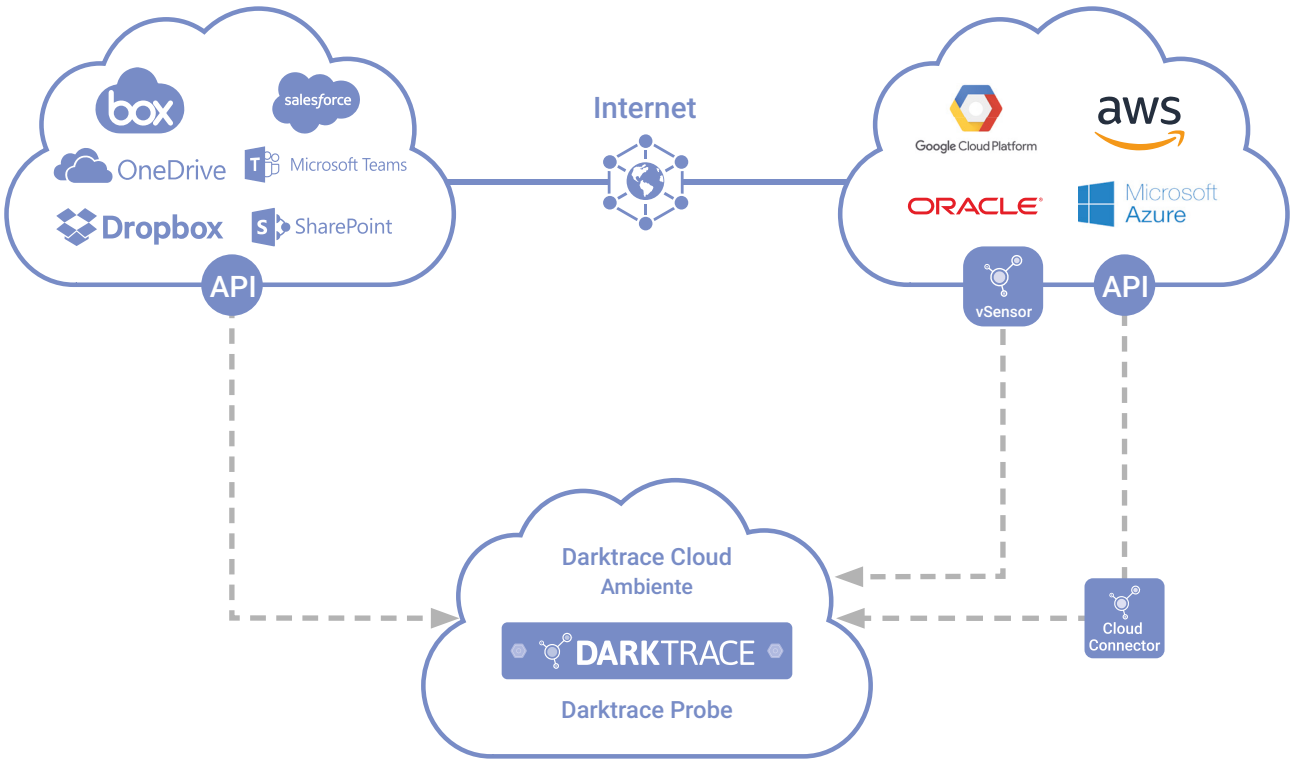
Para implantações híbridas de SaaS, os Darktrace Connectors são instalados remotamente na sonda principal da Darktrace (física ou na nuvem) para consultar as APIs de segurança das soluções SaaS relevantes. Isso abrange o Microsoft 365, o Salesforce, o Dropbox, o Box, o Egnyte e muito mais.

Após a implantação dos Connectors, a Darktrace analisa e correlaciona continuamente os dados SaaS com o tráfego no restante da empresa em uma visualização unificada.



Somente nuvem (IaaS e/ou SaaS)

Se um cliente aproveitar a nuvem, mas não tiver uma rede local, a Darktrace poderá oferecer uma implantação apenas na nuvem como um serviço dedicado. Para implantações apenas na nuvem, a Darktrace gerencia uma sonda principal de nuvem que recebe tráfego de sensores e conectores nos ambientes IaaS e/ou SaaS do cliente.



Conclusão

Conforme as organizações confiaram cada vez mais nos serviços de nuvem e nos aplicativos de SaaS para simplificar as suas práticas comerciais, o paradigma familiar do perímetro de rede se dissolveu, deixando em seu lugar um acervo digital permeável e em constante mudança.

Embora os benefícios da computação em nuvem garantam a continuidade da migração, os desafios de segurança exclusivos apresentados pela nuvem exigirão tecnologias de autoaprendizagem que possam se mover na velocidade e na escala das implantações na nuvem. Além disso, o crescente surgimento de ambientes híbridos e com várias nuvens exige uma única plataforma de segurança que possa correlacionar a atividade entre esses diversos sistemas em tempo real.

A Darktrace, por ser líder global no campo de inteligência artificial para segurança virtual, representa a solução mais eficaz e comprovada para detectar ameaças jamais vistas antes e incidentes virtuais anormais onde quer que eles ocorram na nuvem. Em vez de depender de regras e políticas predefinidas, a tecnologia abraça a incerteza inerente ao complexo ambiente digital dos dias de hoje.

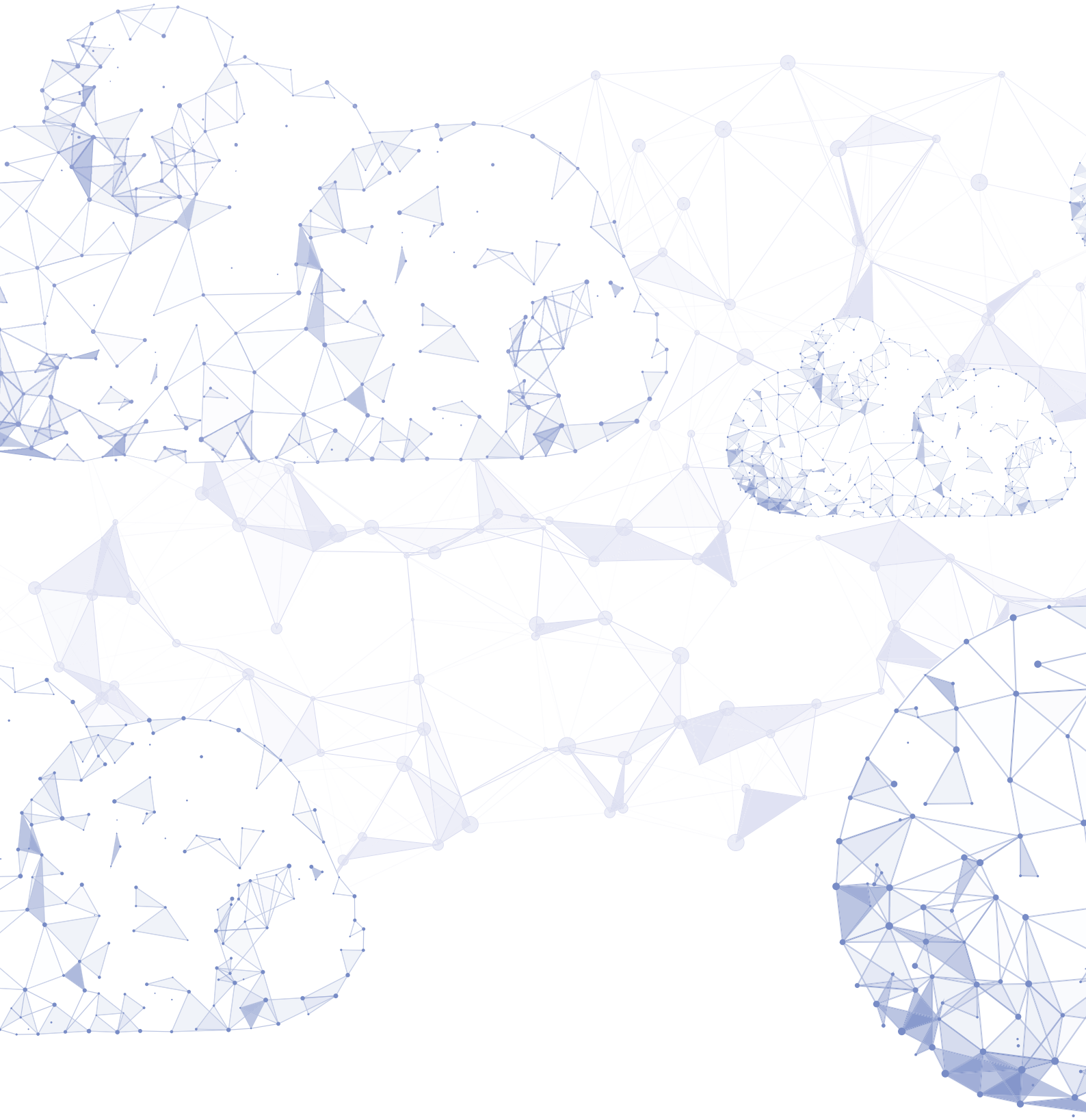
Independentemente de se deparar com uma ameaça interna, um invasor com o objetivo de obter dados confidenciais em contêineres de teste ou uma configuração incorreta importante que possa ser explorada como vulnerabilidade no futuro, a Cyber AI Platform da Darktrace ajuda a eliminar os pontos cegos e a proteger seus dados, onde quer que eles estejam.

Principais conclusões

- Aprende o "self" para detectar ameaças baseadas na nuvem que outras ferramentas não identificam
- Correlaciona a atividade em ambientes híbridos e com várias nuvens
- 100% de visibilidade em tempo real que não deixa espaço para os invasores se esconderem

> A Darktrace representa uma nova fronteira na defesa virtual baseada em IA. Agora, nossa equipe tem cobertura completa e em tempo real em toda a nossa infraestrutura empresarial, industrial e na nuvem.

– CIO, Cidade de Las Vegas



Sobre a Darktrace

A Darktrace é a empresa líder mundial em IA para segurança cibernética e a criadora da tecnologia de resposta autônoma. A IA de autoaprendizagem é baseada no sistema imunológico humano e é utilizada por mais de 3.500 empresas em todo o mundo para proteger contra ameaças cibernéticas em ambientes Cloud, email, IoT, redes e sistemas industriais.

A Darktrace tem mais de 1.200 funcionários e está sediada em San Francisco e Cambridge, no Reino Unido. A IA Darktrace responde contra uma ameaça cibernética a cada 3 segundos, evitando que danos sejam causados.

Contate-nos

São Paulo: +55 (11) 4949 7696

Londres: +44 (0) 20 7930 1350

EUA: +1 415 229 9100

APAC: +65 6804 5010

info@darktrace.com | darktrace.com

@darktrace