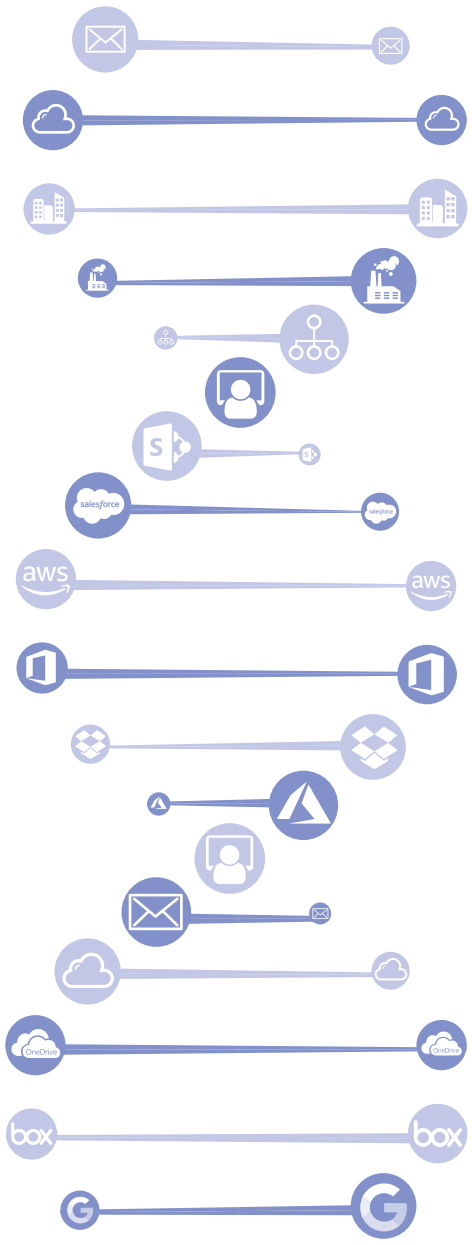
Por que escolher Antigena Email?

94% das ameaças cibernéticas são originadas por e-mail, e as antigas defesas da linha de frente continuam a decepcionar. No entanto, sempre que a Antigena Email e as defesas antigas são implantadas no mesmo ambiente, a Antigena neutraliza consistentemente as ameaças externas e a perda de dados que burlam as defesas de e-mail de linha de frente.



Por quê?

1. IA que aprende o 'self'

Antigena Email é a única solução que analisa e-mails individuais no contexto de um entendimento personalizado do 'self' (o que é 'normal' para todo o seu negócio digital, e não apenas para os e-mails:

- Como a Antigena entende o 'pattern of life' normal de seus funcionários na nuvem, SaaS, e-mail e rede, ele pode detectar ameaças sofisticadas detectando desvios sutis.
- A Antigena trata os destinatários como indivíduos e parceiros dinâmicos, não como meros endereços de e-mail, e entende todo o escopo de seus comportamentos normais
- Por outro lado, as defesas antigas analisam cada e-mail isoladamente e o correlacionam com regras e assinaturas estáticas, baseadas em ataques históricos
- As regras e assinaturas não conseguem identificar os ataques sofisticados e inéditos, os quais estão se tornando cada vez mais comuns

Em resumo, a Darktrace é a única ferramenta que realmente conhece todo o seu negócio digital, o que permite capturar ameaças avançadas por e-mail que certamente passariam despercebidas, permitindo que os e-mails comerciais legítimos passem sem ser interceptados.

2. Decisões que evoluem ao longo do tempo

A Antigena Email é a única solução que opera como um sistema unificado e em camadas, que atualiza suas decisões diante de novas evidências:

- A Antigena toma decisões durante todo o ciclo de vida de um e-mail – desde a entrega até o clique e a execução
- Os conhecimentos exclusivos da Antigena sobre eventos de rede, nuvem, e-mail e SaaS permitem ajustar sua avaliação do nível de ameaça de um determinado e-mail diante de novas evidências, e vice-versa
- As defesas antigas de e-mail operam apenas na linha de frente e são cegas para eventos de rede e nuvem passados, presentes e futuros, os quais melhorariam muito a sua tomada de decisão
- Ameaças que podem ser benignas no ponto de entrega podem ser neutralizadas caso apresentem uma ameaça posterior demonstrada no contexto da rede

3. Ação exata e precisa contra todos os tipos de ataques direcionados por e-mail

Juntos, (1) e (2) melhoram drasticamente a precisão da Antigena Email ao decidir se um determinado e-mail é bem ou mal-intencionado, o que significa que mais e-mails mal-intencionados são interditados e muito menos e-mails desejáveis são retidos, em comparação a outras soluções que não possuem este contexto.

Graças a essa abordagem exclusiva, a Antigena Email não só detém as ameaças menos avançadas e 'conhecidas' que as defesas antigas deteriam, como também é a melhor solução da categoria em deter as ameaças sofisticadas que normalmente não são identificadas por ditas defesas:

Ataques de engenharia social

- As defesas tradicionais de e-mail geralmente não conseguem deter os ataques de engenharia social, especialmente quando não incluem links ou anexos (ou seja, os e-mails 'limpos') que podem ser usados para comparação com listas negras e assinaturas. Como a Antigena Email é a única ferramenta que realmente 'conhece a sua rede', ela pode detectar desvios sutis nos metadados que revelam que e-mails aparentemente bem-intencionados são inconfundivelmente mal-intencionados.

Ataques de malwares desconhecidos e de clonagem

- Se um e-mail incluir um link ou anexo mal-intencionado, apesar de possuir um domínio desconhecido, a Antigena Email mesmo assim o identificará quando as outras soluções não o fizerem, porque o sistema não depende de listas negras ou assinaturas. A mesma lógica se aplica aos domínios spoof recém-registrados, usados em ataques sutis de clonagem.

Interceptações de contas externas

- Como a Darktrace analisa e entende os relacionamentos da sua empresa e de seus usuários com contatos externos confiáveis, a Antigena Email pode identificar inconsistências sutis que indicam uma conta comprometida, podendo executar ações autônomas para se proteger contra a ameaça. As defesas de e-mail antigas assumem a existência de confiança, o que significa que os ataques de interceptação de contas geralmente passam completamente despercebidos.

Proteção contra perda de dados recebidos e enviados

- Como a Antigena Email compreende todo o escopo do 'pattern of life' de seus usuários em todos os níveis dos negócios, ela sabe quais arquivos eles devem e não devem ter acesso e para onde devem ou não enviá-los. A Antigena não apenas neutraliza o recebimento de e-mails mal-intencionados, como também alerta sobre o envio destes – pode ser o caso de uma ameaça interna ou de alguém que está deixando a empresa com raiva, que envia arquivos para o seu próprio e-mail com a intenção de repassá-los a um concorrente ou usá-los em seu próximo cargo, ou simplesmente um funcionário que envia trabalho para casa, sem saber que isso é contra a política da empresa.

A fim de identificar ameaças de e-mail cada vez mais sofisticadas no futuro, todas as ferramentas de e-mail exigirão uma visão holística de todo o ambiente, e não apenas do conteúdo dos e-mails.

A Antigena Email é a primeira e única solução que faz isso.

A Antigena Email é a única solução que analisa dados em todo o negócio digital e frente a novas evidências – sejam elas manifestas no e-mail ou em comportamentos emergentes na rede.

Outras vantagens / casos de utilização

Aprendendo com o paciente zero

Ao correlacionar a compreensão da infraestrutura, de SaaS e do ambiente de e-mails feita pela Darktrace, a Antigena Email é a única solução capaz de detectar uma infecção na rede (Paciente Zero) e executar automaticamente a análise de causas primárias para verificar se ela teve origem por e-mail. Nesse caso, ela protegerá instantaneamente os negócios ao interceptar todos os outros e-mails que fazem parte da mesma campanha.

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. Por outro lado, outras ferramentas de segurança de e-mails podem fornecer proteção preventiva somente contra uma determinada campanha de ataque se dezenas, centenas ou até milhares de vítimas já tenham sido afetadas.

Priorização automática de pessoas fundamentais

A Antigena Email sabe quem são seus usuários podendo, assim, detectar automaticamente quais usuários têm alta prioridade, quais usuários têm mais probabilidade de virarem alvo e quais usuários têm acesso a material confidencial. Portanto, será necessária uma resposta apropriada para diferentes usuários, em vez de uma única resposta generalizada.

Resposta com precisão cirúrgica

A Antigena Email foi projetada pensando nas equipes de TI e segurança, e também em seus atarefados funcionários e executivos. Ela permite, sempre que possível, a entrega de e-mails em casos marginais, removendo apenas o aspecto mal-intencionado do e-mail e preservando o conteúdo real, o que reduz bastante ou compensa diretamente a carga de trabalho do administrador. As defesas de e-mail antigas geralmente retêm esses e-mails, o que custa tempo e dinheiro à empresa.

Como a Antigena Email aprende na prática, caso um e-mail seja demasiadamente ou muito pouco sujeito a ações, ela aprenderá automaticamente a tratar um e-mail semelhante de maneira mais apropriada no futuro, para que o administrador dos e-mails não precise criar regras complexas cada vez que desejar tratar um e-mail de maneira diferente.

Visibilidade, Medidas Forenses e Auditoria

As organizações que fazem a avaliação da Antigena e das defesas antigas de e-mail sempre dizem que a Antigena tem uma funcionalidade muito superior em termos de visibilidade, medidas forenses e auditoria de e-mails.

Isso inclui a capacidade da interface de enxergar quais usuários clicaram nos links de um e-mail, se uma mensagem foi lida ou não, quais outras pessoas receberam determinados e-mails, com quem os usuários normalmente se comunicam, detalhamentos de cabeçalhos de e-mail e muito mais.

A Antigena também permite que as equipes de segurança removam e-mails Live de suas caixas de entrada, se necessário, o que não é possível com várias outras ferramentas.

Funciona com controles padrão do Office 365

Quando as organizações implantam gateways de e-mail na linha de frente, geralmente são forçadas a desativar os controles de segurança padrão da Microsoft Office 365. Isso geralmente permite que os e-mails mal-intencionados, que seriam detidos pela Microsoft, burlem todas as ferramentas de segurança. A Antigena Email e os controles nativos da Microsoft podem ser implantados concomitantemente, para que possam trabalhar juntos e fornecer uma defesa abrangente e profunda.

Defesa anônima de e-mails

Os gateways de e-mail também exigem que as organizações alterem seu 'registro MX', o que significa que qualquer invasor pode ver imediatamente quais ferramentas estão sendo usadas, possibilitando que criem seus ataques levando-as em consideração. Como a Antigena Email não fica parada esperando, os invasores têm menos informações sobre suas ferramentas de segurança e será menos provável que almejem a sua organização.