Proteção do mundo pós-IA para serviços financeiros com zero trust

Uma abordagem estratégica para cibersegurança na era da IA

Resumo da solução

Resumo executivo: navegando pela floresta sombria

Em um mundo pós-IA, os serviços financeiros devem navegar por uma "floresta sombria" de ameaças e incertezas ocultas, onde cada interação pode representar um risco. Assim como seria preciso ter extremo cuidado em um ambiente perigoso e imprevisível, os serviços financeiros devem abordar a segurança da IA com vigilância. Este resumo descreve as medidas que as empresas de serviços financeiros podem tomar para se proteger ao entrarem neste cenário impulsionado pela IA.

Exploraremos como a IA está remodelando o cenário de ameaças, introduzindo novas vulnerabilidades, como fraudes com tecnologia de IA e ataques cibernéticos automatizados. Além disso, destacaremos as principais tendências e previsões, ajudando as organizações a antecipar o impacto da IA e responder estrategicamente.

A melhor defesa nesse ambiente de alto risco, onde nenhuma entidade, seja dentro ou fora da organização, pode ser considerada confiável, é o zero trust. Este resumo fornece um caminho claro para que empresas de serviços financeiros iniciem sua jornada zero trust, oferecendo etapas práticas para garantir um futuro de IA seguro e resiliente.

IA e o cenário de ameaças em evolução

A IA está transformando rapidamente o cenário de ameaças, introduzindo riscos complexos que desafiam os modelos de segurança tradicionais. Os ataques evoluíram e se tornaram mais eficazes em escala, permitindo que as vítimas continuem operando enquanto os invasores ameaçam expor seus dados. Embora existam muitas grandes tendências e previsões de IA, vamos analisar três tendências para 2024 e 2025 que estão evoluindo em um ritmo mais rápido.

Três tendências para observar em 2024 e 2025

Sequência principal de desenvolvimento de IA

Os grandes modelos de linguagem (LLMs) de IA transformaram a maneira como pensamos sobre IA generativa, expandindo suas capacidades além de saídas estreitas e específicas de tarefas para soluções mais dinâmicas e sensíveis ao contexto. Mas, assim como no mundo real, tudo, incluindo a IA, continuará a evoluir. Esses LLMs nos conquistaram quando cruzaram o vale da estranheza.

O vale da estranheza se refere ao sentimento inquietante que as pessoas experimentam quando a IA se torna quase, mas não totalmente, indistinguível dos humanos, criando uma sensação de desconforto devido à sua imitação quase perfeita.

A GenAI e o ChatGPT, em particular, cruzaram o vale da estranheza ao atingir 100 milhões de usuários em dois meses, o que é notável. Agora que cruzaram o vale da estranheza, há mais por vir, o que pode causar mais impacto do ponto de vista neurológico, da busca cognitiva, do que apenas a GenAI.

Ataques de ransomware sem criptografia

Anteriormente, a criptografia era usada para ataques de ransomware e dominava a pauta principal: roubar seus dados, exigir resgate pela operação e, se você não pagasse, não conseguiria manter seu negócio em funcionamento.

No entanto, com o tempo, os criminosos que realizam ataques de ransomware perceberam que, ao reduzir a quantia de dinheiro que se está buscando e não impedir a vítima de fazer negócios, obteriam um rendimento maior. Então, por exemplo, digamos que eles diminuam o valor do resgate US$ 10 milhões para US$ 2 milhões, e as chances de você pagar vão de 5% para 70–80%; isso torna-se um modelo de negócio de ransomware "melhor" em escala. Isso é o ransomware sem criptografia.

No ransomware sem criptografia, os criminosos pegam os dados, ameaçam você e, em muitos casos, permitem que você continue as operações porque não querem interromper seus negócios.

Ao não interromper os negócios, menos danos à reputação podem ocorrer. Os criminosos também podem tentar convencer a vítima a não revelar o resgate ao SEC ou regulador, alegando que o valor não é relevante o suficiente.

Ataques de ransomware com tecnologia de IA

Os ataques de ransomware com tecnologia de IA são mais eficazes em melhorar o rendimento, a penetração e a automação dos ataques. Nesse caso, os invasores utilizam a IA para automatizar e aumentar a sofisticação dos ataques cibernéticos, tornando-os mais rápidos, mais direcionados e mais difíceis de detectar.

Quatro maneiras de os serviços financeiros lidarem com o cenário em evolução da IA

O uso de IA por empresas está crescendo rapidamente, junto com os riscos. Os quatro níveis de consideração estratégica corporativa podem orientar organizações de serviços financeiros a navegar pelas complexidades de um mundo pós-IA em constante evolução.

Em 2024, o uso de ferramentas de IA/ML cresceu 594% e o uso do ChatGPT cresceu em 634% (Relatório de segurança de IA de 2024 da Zscaler ThreatLabz).

Política e ética

Os serviços financeiros devem desenvolver políticas abrangentes que regem o uso ético da IA, garantindo a conformidade com a regulamentação e fomentando a confiança dos clientes. Isso envolve a criação de uma estrutura que aborde a privacidade de dados, a transparência algorítmica e a mitigação de vieses, enfatizando práticas responsáveis de IA.

Atividade principal

Como a IA impacta o negócio principal? A Harvard Business Review realizou um estudo que mostrou uma diferença estatisticamente significativa no desempenho de empresas em um determinado setor que usam IA em comparação àquelas que não a usam, e que essa diferença continua aumentando.

Então, como trazer IA para a empresa? Você vai fazer isso com um parceiro ou de forma privada? Você vai ter seus próprios modelos? Você vai participar do uso de modelos maiores? E qual é o caso de uso envolvido?

As organizações devem avaliar como a IA pode aprimorar suas principais operações comerciais, como melhorar os serviços ao cliente, otimizar o processamento e permitir a tomada de decisões baseada em dados.

As organizações devem avaliar como a IA pode aprimorar suas principais operações de negócios, como aprimorar o atendimento ao cliente, otimizar o processamento e permitir a tomada de decisões baseada em dados. Ao identificar as principais áreas onde a IA pode agregar valor, as organizações de serviços financeiros podem criar vantagens competitivas e promover a inovação alinhada aos objetivos estratégicos

P&D e infraestrutura

Com a chegada das ferramentas de IA aos negócios, como lidar com elas? Investir em uma infraestrutura robusta que suporte recursos de IA, como computação na nuvem, análise de big data e aprendizado de máquina, permitirá que as organizações aproveitem tecnologias emergentes e desenvolvam novas soluções para atender às necessidades em constante mudança dos clientes.

Vantagens da cibersegurança

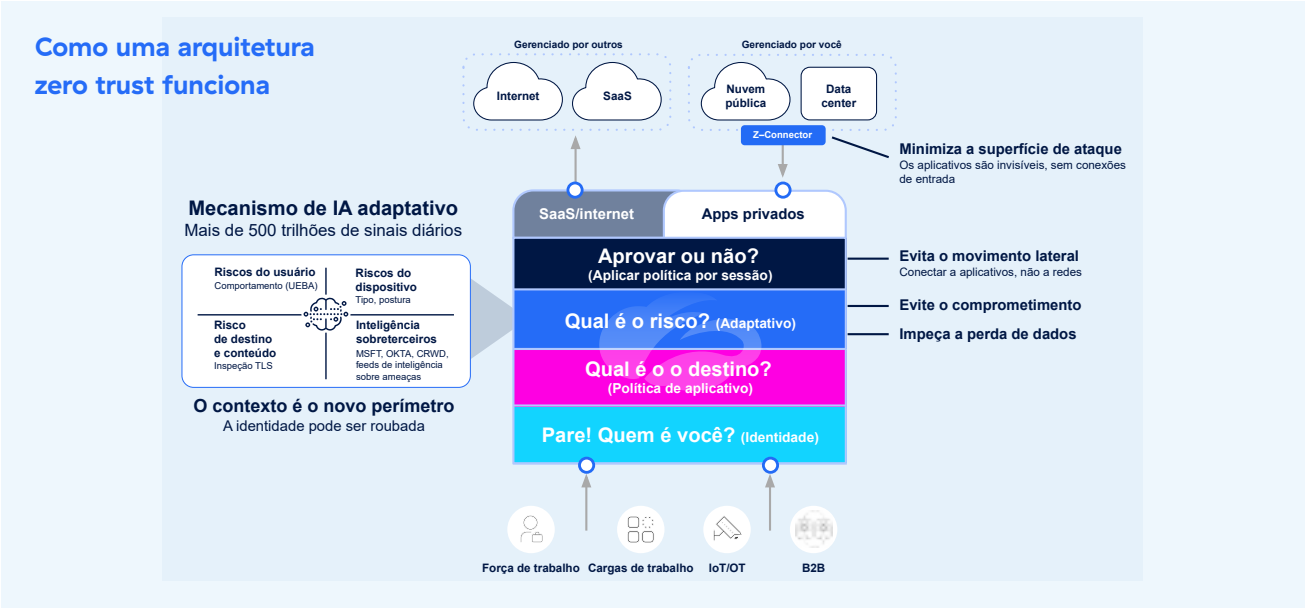
As instituições financeiras podem melhorar sua postura de cibersegurança utilizando soluções de segurança que aproveitam a IA para identificar e responder a ameaças em tempo real.

Você deve se perguntar: quais são as vantagens da IA e da cibersegurnaça ou quais são as potenciais ameaças? Como isso será usado contra você? Como você pode se preparar para isso? Ao implementar medidas de segurança orientadas por IA, as organizações podem proteger melhor dados e ativos sigilosos e garantir resiliência contra ameaças sofisticadas.

O papel do zero trust na redução do risco cibernético

Mesmo com a aceleração do uso da IA empresarial, as empresas bloqueiam **18,5%** de todas as transações de IA, um aumento de **577%**, sinalizando preocupações crescentes com a segurança (Relatório de segurança de IA de 2024 da Zscaler ThreatLabz). A melhor defesa neste ambiente de alto risco, onde nenhuma entidade, dentro ou fora da organização, pode ser considerada confiável, é o zero trust.

Zero trust é a estratégia que nos ajuda a navegar pela floresta sombria, permitindo apenas o que a empresa precisa, quando precisa. Implementar uma abordagem zero trust de não confiar em ninguém garante que, independentemente do usuário, carga de trabalho, dispositivo ou outra empresa, você pode reduzir significativamente o risco cibernético:



1. Autenticar identidade: pare. Quem é você?

a. Quem está se conectando?

b. Quais são os atributos?

c. Para onde vai a conexão?

2. Política de controle de aplicativos: onde você está tentando chegar?

a. Aonde você está tentando ir? Nesta etapa, o zero trust avalia o risco usando o contexto, evitando comprometimento e perda de dados.

3. Risco contextual adaptativo: qual é o risco?

a. Qual é o risco? Evite comprometimentos e interrompa a perda de dados avaliando o risco do usuário, o risco do dispositivo, o destino, o risco do conteúdo e informações de terceiros (Okta, CrowdStrike, etc.).

4. Aplicar políticas

a. Evite a movimentação lateral para que você se conecte a aplicativos, não a redes b. Aplique políticas para conexões de SaaS/internet com base na sessão e no usuário c. Aplicativos privados: minimize a superfície de ataque para que os aplicativos fiquem invisíveis e nenhuma conexão de entrada possa ocorrer.

Uma jornada zero trust

Para proteger sua empresa contra o crescente número de ameaças cibernéticas impulsionadas pela IA, embarcar em uma jornada zero trust é essencial. A implementação de uma jornada zero trust deve ser vista como um processo gradual, dividido em etapas gerenciáveis que se alinhem às prioridades de negócios e às metas de segurança, garantindo que sua segurança evolua de uma forma dimensionável e resiliente.

1. Proteja as equipes de trabalho

a. Fase 1A: sem alterações na rede

i. Proteção cibernética e de dados, experiência digital e quantificação de riscos

b. Fase 1B: simplificação da redei.

i. Filial ou escritório com zero trust, estratégia avançada de proteção cibernética e de dados e obtenção de insights de negócios

2. Proteja as cargas de trabalho

a. Proteção cibernética e de dados para cargas de trabalho

b. Rede de cargas de trabalho e segmentação zero trust

3. Acesso de terceiros

a. Acesso a aplicativos de terceiros com zero trust

b. Conectividade zero trust de sites de terceiros

4. Proteja os dispositivos (IoT/OT)

a. Proteção cibernética e de dados para IoT/OT

b. Conectividade zero trust de IoT/OT

Conclusão

O zero trust oferece a melhor defesa neste cenário em rápida evolução, onde nenhuma entidade, dentro ou fora da organização, pode ser considerada inerentemente confiável. À medida que a tecnologia e a IA continuam a evoluir e eventualmente convergem, adotar uma estratégia zero trust garante que apenas os usuários e processos certos acessem o que é necessário, quando é necessário, garantindo que você possa permanecer resiliente e preparar sua organização para o futuro.

Reduza seu risco cibernético, comece sua jornada zero trust aprendendo mais em zscaler.com/br

Conheça o autor

Com mais de três décadas de experiência como empreendedor, especialista em segurança da informação e executivo em empresas como RSA, Arbor Networks, CA, McAfee, Cbyereason e outras, Sam se dedica a capacitar defensores em conflitos cibernéticos e a cumprir a promessa de segurança, possibilitando um mundo seguro, confiável e conectado. Atualmente, Sam Curry é vice-presidente global e CISO da Zscaler e, em seu tempo livre, palestrante, apresentador de um podcast (On the Hook), membro de diversos conselhos e publicações e mentor de segurança da informação. Conecte-se comigo no LinkedIn.