GUARDIANKEY

Alta segurança de fácil utilização

Sobre

GuardianKey é uma solução para proteger sistemas contra acessos ilegítimos, tornando a autenticação mais segura. Ele usa técnicas de Inteligência Artificial para detectar se o acesso é realmente do usuário, podendo até mesmo bloquear o acesso ao sistema, mesmo que a senha utilizada seja válida. Por meio de bases de análise do comportamento do usuário, inteligência de ameaças, e psicometria (ou biometria comportamental), o GuardianKey fornece uma análise do risco de ataque em tempo real.

Além da segurança inteligente na autenticação, a solução GuardianKey provê boa experiência para o usuário, pois não requer o uso de informação extra ou tokens durante o login.

O analisador do GuardianKey provê uma análise de riscos de acesso em tempo real, o que pode ser usado na resposta a um ataque ou tomada de decisões de negócio. Os eventos e riscos podem ser visualizados no painel de administração da ferramenta.

GuardianKey

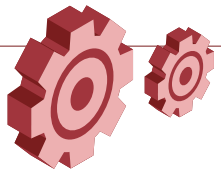
Como funciona

O método inovador de detecção do GuardianKey analisa os eventos enviados pelas aplicações protegidas. O GuardianKey pode funcionar como serviço, em nuvem, ou instalado no ambiente do cliente. É necessário apenas a instalação de um plugin ou pequenos ajustes no código da aplicação para possibilitar o envio e análise dos eventos.

A método de detecção de ataques faz uso de técnicas de Machine Learning e de uma fórmula matemática exclusiva para o cálculo do risco, que combinar três abordagens distintas: Inteligência de Ameaças, Análise Comportamental e Análise Psicométrica.

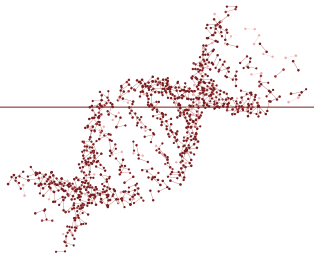
Inteligência de Ameaças

análise baseada na base de conhecimento do GuardianKey sobre ataques e atacantes da Internet



Análise Comportamental

usuários, no geral, interagem com sistemas a partir dos mesmos locais, usando mesmos dispositivos, em determinados horários do dia, etc. Essas informações são usadas pelo GuardianKey para criar um perfil comportamental para cada usuário. Tentativas de acesso ao sistema que desviam desses perfis são mensuradas para prover um risco de ataque.



Análise Psicométrica

a forma em que o usuário digita no teclado, move o mouse, segura o dispositivo móvel (ângulos, movimentos, etc.) é particular. O GuardianKey cria um perfil usando esse tipo de informação e usa esse perfil para obter uma métrica de identificação do usuário, que é processada para prover um risco de ataque.

Usando esses três pilares, o sistema de detecção calcula um risco para cada evento enviado pelos sistemas protegidos. Em tempo real, a tentativa de acesso pode ser bloqueada, mais informações podem ser requeridas ao usuário, ou uma notificação pode ser enviada ao usuário e/ou administrador do sistema.

Vantagens

- Efetivo contra as seguintes ameaças: roubo de identidade, ataques automatizados, ataques de força bruta, acesso por meio de sistemas anonimizadores, dentre outros ataques.
- Simplifica a experiência do usuário.
- Painel de administração de fácil utilização.
- Metodologia baseada em riscos, que permite integrar com framework corporativo de gestão de riscos.
- Disponível em nuvem ou no ambiente do cliente.
- Gratuito, em nuvem, para vários tipos de pequenos clientes.
- Baseado em tecnologias Big Data, que o torna apropriado para volumes de dados (realmente) grandes.
- Excelente Retorno de Investimento (ROI).

Quanto custa

O GuardianKey pode ser adquirido como serviço, em nuvem, ou para funcionamento dentro da infraestrutura do cliente (on-premise). Há três tipos de licenciamento: por transação, por usuário nominado (perpétuo), e por usuário nominado por ano (subscrição).

Os custos para o modelo em nuvem podem ser encontrados em https://guardiankey.io. Entre em contato para mais informações sobre o licenciamento on-premise.

Custos relacionados a fraudes, roubo de contas, marketing negativo e vazamento de informações podem ser muito prejudiciais ao qualquer negócio. Nesse caso, o GuardianKey provê um notável Retorno de Investimento (ROI)!

GUARDIANKEY

Usando o GuardianKey

Segurança inteligente com simplicidade é um dos nossos valores. Nesse sentido, o GuardianKey foi criado para prover uma integração simples com os sistemas a serem protegidos. São disponibilizados plugins para aplicações conhecidas e um código de referência para a API, em PHP e Python, para simplificar a implementação. Também é possível desenvolver integrações usando diretamente a API. Verifique a documentação para isso.

Verifique mais informações no site!

O GuardianKey é gerido por uma interface web de fácil utilização, onde é possível configurar políticas, criar grupos de autenticação, analisar eventos, usuários e riscos. Você pode criar um usuário agora mesmo, acessando o painel de administração do GuardianKey em nuvem. Entretanto, lembre-se que é necessário enviar alertas para possibilitar o processamento e visualização.

Entre em contato

Você tem alguma dúvida?
Envie-nos um e-mail que
retornaremos assim que possível!

contato@guardiankey.io

Ou visite: http://guardiankey.io