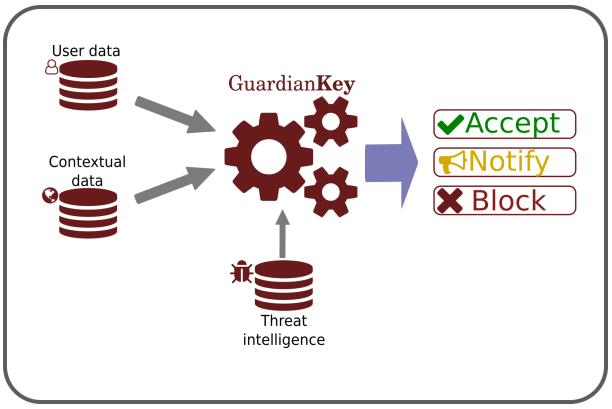
GuardianKey Auth Security Enterprise

O GuardianKey Auth Security Enterprise é uma solução para proteção contra acessos não autorizados e ataques.

Funcionamento



O mecanismo de detecção usa Inteligência artificial e uma fórmula matemática proprietária de cálculo de riscos para combinar inteligência de ameaças e perfil comportamental (ou contextual).

Usando esses pilares, o mecanismo calcula um risco para cada evento enviado pelos sistemas protegidos. Em tempo real, a tentativa de acesso pode ser bloqueada, um requisito extra pode ser solicitado ao usuário ou notificações podem ser acionadas.

Características

Sem Hardware Nenhum token, celular ou outro dispositivo é necessário.	**Implantação fácil** Apenas algumas linhas de código são necessárias. Também é possível usar um proxy reverso.	**Tempo Real** As tentativas de autenticação são tratadas e disponíveis para visualização em tempo real.
Transparente Menos dor de cabeça para os usuários! O usuário não precisa usar 2 fatores ou ações extras.	**Alto ROI** Melhore a segurança com baixos custos e baixos esforços.	**Alta Segurança** Abordagem de última geração baseada em Machine Learning e avaliação de risco para proteger o processo de autenticação.

Especificações gerais e recursos:

- O GuardianKey tem como foco a proteção de sistemas contra ataques de autenticação.
- O GuardianKey implementa técnicas de *Inteligência Artificial* para analisar o comportamento dos usuários e avaliar usando inteligência de ameaças.
- Para cada usuário o sistema mantém uma base de comportamento, para o cálculo de desvios comportamentais (ou contextuais) e mensuração de riscos.
- O GuardianKey processa eventos em tempo real, permitindo que a aplicação protegida bloqueie uma tentativa de acesso à aplicação baseado no risco de ataque identificado pelo GuardianKey, ainda que a senha tenha sido corretamente digitada.
- O sistema recebe eventos coletados em sistemas durante o processo de autenticação, processa e retorna um nível de risco e uma resposta baseada nas definições de política previamente configurada.
- O risco é calculado por meio de fórmula probabilística que combina o risco relacionado ao desvio do padrão contextual de cada usuário com o risco detectado pela reputação das origens dos acessos (inteligência de ameaças).
- O valor do risco é apresentado em uma escala de 0 a 100.
- O sistema pode notificar usuários por e-mail para que os mesmos respondam se o acesso foi legítimo ou não. Em caso afirmativo, o sistema aprende para evitar novos alertas semelhantes, em caso contrário, o sistema pode alertar a equipe de tratamento de incidentes.
- O GuardianKey permite a customização do e-mail enviado aos usuários e da tela de verificação de eventos, acessada pelos usuários.
- O sistema não exige *tokens*, dispositivos móveis, códigos, ou outras informações adicionais para o processamento de eventos.
- O sistema propõe os seguintes níveis de resposta às tentativas de acesso: “aceitar”, “notificar”, “notificar com ação”, e “bloquear”.
- As respostas propostas são baseadas no nível do risco e pode ser ajustada em política, mantida pelo sistema e configurada pelo administrador.
- O GuardianKey possui API HTTP/REST de comunicação para implementação de integração entre sistemas.
- A GuardianKey é parceira tecnológica da Red Hat, atual mantenedora do KeyCloak e fabricante do RH-SSO.

Captação de eventos

- Os eventos são coletados nas aplicações, onde o usuário executa a processo de autenticação, e enviados via API para o sistema de análise de eventos de autenticação.
- Os eventos podem ser cifrados com chave criptográfica simétrica (AES 256 bits), para assegurar a confidencialidade e autenticidade do evento.
- O GuardianKey não coleta senhas de usuários.
- Há implementações de referência para a API abertos em várias linguagens, dentre elas PHP, Python, NodeJS, LUA, ASP Clássico, Java, e Ruby.
- Dentre as informações do evento encontram-se as seguintes: timestamp da tentativa de acesso, “User-Agent” do navegador do usuário, sucesso ou falha na autenticação, e IP de origem do acesso.

Processamento

- O sistema permite a criação de unidades organizacionais para segmentar os acessos dos administradores aos eventos e configurações de políticas para tratamento baseado nos níveis dos riscos.
- O GuardianKey permite a criação de grupos de usuários para a implementação de políticas específicas para cada grupo.
- Mais de um sistema protegido pode enviar eventos para o mesmo grupo de usuários (authgroup), permitindo assim o compartilhamento da base comportamental entre sistemas. Também é possível

segmentar o processamento entre sistemas, neste caso, o processamento é realizado de forma distinta.
- O administrador pode configurar limites dos níveis de risco para a sugestão de resposta ao evento.
- Todos os eventos possuem uma identificação única e os eventos são georreferenciados a partir do endereço de IP de origem dos acessos. O georreferenciamento inclui as coordenadas geográficas (longitude e latitude), o país e a cidade.
- A análise contextual (do comportamento do usuário) inclui a análise das seguintes características típicas do usuário: navegador, dispositivo, localização geográfica, sistema operacional, ASN da origem do endereço de IP (ISP), entre outras. Uma mudança geográfica do acesso, por exemplo, pode elevar o risco do acesso.
- A análise do risco da inteligência e de ameaças é construída com informações próprias e públicas (OSINT), e detecta: Origens comprometidas ou infectadas por malware, tráfego saindo de proxy/TOR, origem anonimizada, IP utilizado para ataques, entre outros.
- O resultado do processamento inclui o risco contextual, risco de inteligência de ameaças, risco global, e sugestão de resposta ao evento, fornecendo o risco mesmo se a senha estiver incorreta.
- O sistema permite a identificação da aplicação que gerou o evento e do servidor (agente de coleta) que fez o envio do evento.
- O sistema possui detecção de ataques de força bruta próprio, que se baseia em reputação positiva e negativa das origens, reduzindo falsos positivos.
- Para ataques de força bruta, o sistema possui resposta com aumento progressivo do risco.
- A reputação de origens detectadas como geradores de ataques de força bruta decai após determinado tempo. O tempo de decaimento da reputação aumenta em função da recorrência de tentativas de ataques de força bruta. O que é efetivo para combater o ataque e reduz impactos em caso de falsos positivos.
- O sistema fornece uma classificação dos tipos de ataque ou ameaças.
- O sistema suporta eventos com endereços de IP de origens nas versões IPv4 e IPv6.

Implantação

- Todos os componentes do GuardianKey são executáveis no sistema operacional Linux.
- O console de administração pode operar em servidor de aplicações Apache ou NGINX.
- O processamento e armazenamento de dados contextuais são realizados por meio de tecnologias Big Data, que permitem escalabilidade.

Integração

- O envio de eventos pode ser feito por meio de API no protocolo HTTP/REST ou por pacote UDP.
- Não há necessidade de importação prévia de base de dados de usuários. O sistema identifica novos usuários a partir dos eventos enviados.
- A visualização de um evento para apresentação ao usuário e submissão da resposta do usuário sobre a legitimidade do acesso pode ser feita por meio da API no protocolo HTTP/REST.
- O GuardianKey pode enviar os eventos processados para ferramentas de logs externas via webhook HTTP/REST, podendo ser cifrados com uma chave simétrica.
- A notificação de usuários pode ser feita via webhook ou SMTP.
- Para envios via correio eletrônico (SMTP) é possível enviar: apenas para usuários; para usuários e administradores; ou apenas para administradores.
- O GuardianKey é acompanhado por implementações da API de referência nas linguagens PHP, Python, NodeJS, LUA, ASP Clássico, Java, e Ruby.
- O sistema possui extensão para KeyCloak, RH-SSO, WordPress, Moodle, RoundCube, entre outros. Lista completa disponível em https://guardiankey.io/pt-br/products/guardiankey-integrations/

Console de administração e visualização de eventos

- O GuardianKey possui console web para a administração de grupos de usuário e políticas e para a visualização de eventos.
- A console de administração e visualização dos eventos é em tecnologia WEB, responsiva, dispensando a instalação de qualquer software adicional para o acesso e uso. Compatível com os principais navegadores do mercado (Chrome, Edge, Firefox, Opera, Safari, dentre outros).
- O console web é disponibilizado exclusivamente para acesso com HTTPS.
- O console possui painéis (dashboards) para riscos e eventos, como por exemplo: Usuá
- O console apresenta gráficos com riscos acumulados de todos os usuários, podendo por exemplo ver o “top 10” dos usuários ou filtrar por um usuário específico.
- Os dashboards podem ser filtrados por tempo ou por grupo de usuários.
- A console permite a pesquisa de eventos ou usuários por meio de filtros, podendo ainda visualizar detalhes do evento, como por exemplo cidade, coordenadas geográficas, nome do navegador utilizado, nome do dispositivo utilizado no acesso, endereço ip de origem, score de risco e resultado da ação com base na política definida, código identificador do ISP (internet service provider) e detalhes do evento.
- A console permite a apresentação de informações de usuário, tais como estatísticas de sua base contextual (navegadores e sistemas operacionais utilizados; cidades e países de acesso) e linha do tempo dos eventos gerados. É possível também visualizar um gráfico dos eventos desse usuário.
- O console possúi um dashboard no formato de mapa geográfico para visualização dos eventos, que permite filtrar, por exemplo, por cidade, usuário, score de risco, data, entre outros.
- O console possui dashboard que permite a visualização do risco organizacional, podendo filtrar por janela de tempo ou segmentar por grupo de usuários, entre outros filtros possíveis.

Requisitos técnicos

Para o funcionamento adequado do GuardianKey Auth Security Enterprise, é necessário haver ao menos 1 (um) servidor dedicado para o serviço, podendo ainda ser um servidor virtual (VM), contendo as configurações abaixo, de acordo com a quantidade de usuários a serem atendidos:

De 1001 até 100.000 usuários e até 1000 eventos por segundo:

- 12 núcleos de CPU
- 128GB de memória RAM
- 250GB de armazenamento usando tecnologia SSD e/ou de latência inferior a 3ms para gravação e no mínimo 1000 IOPS
- Comunicação com a Internet
- IP público roteável para acesso externo, caso seja necessário.

Acima de 100.001 usuários ou 1001 eventos por segundo, necessário cluster para processamento. Consultar nossa área de negócios.