FORCEPOINT

Descritivo

Segurança da Informação

FORCEPOINT UEBA

PROTEGER PROPRIEDADE INTELECTUAL, DETECTAR CONTAS COMPROMETIDAS E REDUZIR O RISCO INTERNO

Forcepoint User and Entity Behavior Analytics (UEBA) habilita as equipes de segurança a monitorar proativamente comportamentos de alto risco dentro da empresa. Nossa plataforma de análises de segurança fornece contexto inigualável aos mesclar dados estruturados e não estruturados para identificar e impedir usuários maliciosos, comprometidos e negligentes. Nós descobrimos problemas críticos como contas comprometidas, espionagem corporativa, furto de propriedade intelectual e fraude.

POR QUE FORCEPOINT UEBA PARA SEGURANÇA

Nossos clientes confiam na Forcepoint para fornecer contexto sobre o comportamento humano nas empresas. Somente Forcepoint UEBA oferece análises configuráveis para ajudar os analistas de segurança a abordarem os problemas que mais importam para a empresa. Somos dimensionáveis e ajudamos as equipes de segurança a:

- Reduzir o tempo para detectar ataques internos
- Identificar os alertas relevantes quando as equipes de segurança estão se afogando em ruídos
- Granularidade sobre a atividade dos usuários, indo além de SIEM e outras ferramentas no seu ambiente
- Aprimorar a eficiência da investigação para resposta a incidentes e análise forense após violações

PILARES DA PLATAFORMA

Forcepoint UEBA fornece insight sobre comportamentos e pessoas de alto risco, e não apenas alertas anômalos. Ao avaliar as interações variáveis entre pessoas, dados, equipamentos e aplicativos, Forcepoint UEBA prioriza as linhas de tempo para as equipes de segurança. Nosso software apoia-se em quatro pilares:

Contexto rico › Associa fontes de dados diferentes em uma única narrativa, combinando o conteúdo de comunicações para decifrar a intenção nos feeds de enriquecimento de SIEM, endpoints e funcionários.

Análises comportamentais › Aplica diversos tipos de análises comportamentais e baseadas em conteúdo rigorosas, com foco em detecção de mudanças, padrões e anomalias para detectar melhor ataques sofisticados.

Pesquisa e descoberta › Expõe ferramentas potentes de pesquisa forense e descoberta com uma interface de usuário rica em contexto para monitoramento constante e investigações profundas.

Principais casos de uso

- **Atividades precursoras**
- **DLP com reconhecimento de conteúdo**
- **Detecção de contas comprometidas**
- **Reconhecimento de dados**
- **Abuso de usuários privilegiados**
- **Análises de segurança**

Fluxo de trabalho intuitivo › Entrega relatórios proativos que se integram totalmente com o fluxo de trabalho humano e a arquitetura existente de informações de clientes para dinamizar a eficiência operacional.

REDEFININDO AS ANÁLISES DE SEGURANÇA

Visibilidade orientada pelo contexto › Forcepoint UEBA entrega visibilidade única sobre as atividades, os comportamentos e os relacionamentos dos funcionários, integrando fluxos de dados não estruturados e ricos em contexto com dados estruturados. Nossos modelos analíticos permitem que entidades e eventos sejam pontuados e priorizados através de múltiplas lentes em todos os fluxos de dados — o que antes estava indisponível para as equipes de segurança. Também integramos com Active Directory, SIEM, EDRs e as fontes de dados principais para oferecer verdadeira consciência situacional, e uma plataforma forense potente que aprimora radicalmente as investigações internas.

Análises configuráveis › As ferramentas UBA tradicionais black-box com frequência limitam-se a fontes de dados estruturados, analisados em sistemas diferentes, com uma configuração fixa de análises. O Forcepoint UEBA, em contrapartida, entrega recursos analíticos potentes que permitem que as equipes de segurança abordem casos de uso de segurança em evolução, e façam análises ad hoc em tempo real, incluindo pesquisa avançada em todos os conjuntos de dados. Nossas análises podem ser ajustadas sem programação adicional, permitindo uma resposta mais ágil às ameaças de segurança.

Escalável › Somos fundamentalmente escaláveis. Somente Forcepoint UEBA usa ElasticSearch para habilitar o acesso instantâneo a quantidades massivas de dados. Nossa plataforma armazena de forma transparente os dados estruturados e não estruturados, e é horizontalmente escalável para crescer com os nossos clientes. Forcepoint UEBA também fornece níveis variáveis de controles de acesso e administrativos, para que você possa confiar em nossa tecnologia para trabalhar para a sua empresa em qualquer tipo de implementação.

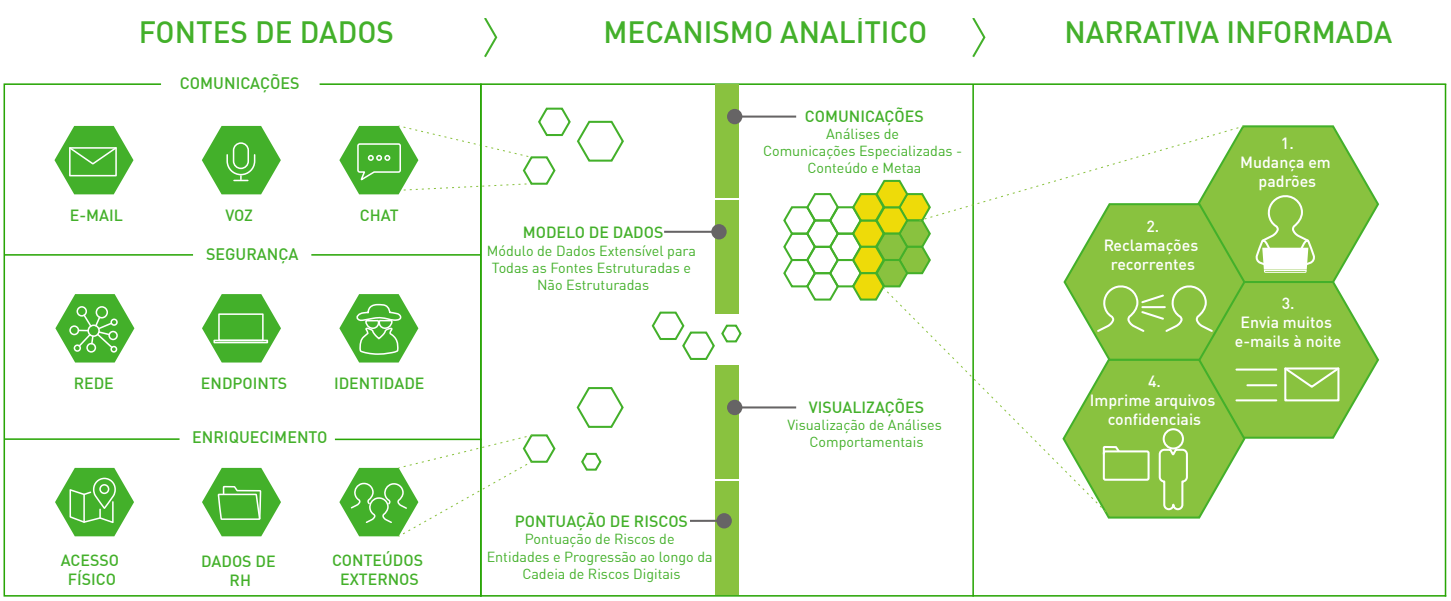
Capacidades

- **Painéis de controle e fluxos de dados com base em funções** Ative a revisão rápida de atividades não compatíveis por meio de uma interface de usuário intuitiva para que analistas e gerentes possam investigar, analisar, escalar e tomar medidas rapidamente..
- **Direitos de dados robustos** Suporte integral para direitos de dados complexos, requeridos por controles internos e preocupações de privacidade de dados impulsionadas externamente.
- **Plataforma extensível** Análises, painéis de controle e fluxos de trabalho configuráveis oferecem suporte para casos de uso de segurança out of the box, com capacidade integral para expandir para qualquer caso de uso de risco. Entrega modelos avançados de ciência de dados sem um compromisso rigoroso de serviços profissionais.
- **Opções de implementação flexíveis** Implemente prontamente Forcepoint UEBA no local, em uma nuvem privada virtual ou mesmo usando um appliance Forcepoint UEBA.

Dados analíticos avançados

- **Análises comportamentais** Identifique mudanças de comportamento que podem indicar atividade de funcionários ilegal, indesejada ou não conforme, atual ou potencial, usando análise de sentimento e conteúdo.
- **Priorização inteligente** Priorize eventos de interesse e alertas com base em análise de conteúdo e padrões de metadados.
- Processamento de Linguagem Natural **(NLP, Natural Language Processing)** Reduza os falsos positivos de forma significativa com uma aplicação inteligente e prática de léxicos complexos de NLP para qualquer idioma, e tecnologia de identificação de texto que reconhece isenções de responsabilidade e citações de textos de e-mails segmentados.
- **Visualizações** Visualizações personalizadas e desenvolvidas especificamente para desbloquear as capacidades de inferência dos analistas e entregar contexto máximo sobre atividades relevantes. Entenda rapidamente "quem", "o quê", "quando" e "como" das ações de funcionários.
- **Classificação de conteúdo** Turbine as implementações de DLP usando o mecanismo de classificação de conteúdo do Forcepoint UEBA para identificar e filtrar comunicações não relevantes, como correspondência em massa, malas diretas de terceiros e muito maiscomo propagandas (junk mail), campanhas com listas de e-mails e mais.

CONTATO
www.forcepoint.com/contact


FONTES DE DADOS
MECANISMO ANALÍTICO
NARRATIVA INFORMADA
COMUNICAÇÕES
E-MAIL
VOZ
CHAT
SEGURANÇA
REDE
ENDPOINTS
IDENTIDADE
ENRIQUECIMENTO
ACESSO FÍSICO
DADOS DE RH
CONTEÚDOS EXTERNOS
MODELO DE DADOS
Módulo de Dados Extensível para Todas as Fontes Estruturadas e Não Estruturadas
PONTUAÇÃO DE RISCOS
Pontuação de Riscos de Entidades e Progressão ao longo da Cadeia de Riscos Digitais
COMUNICAÇÕES
Análises de Comunicações Especializadas - Conteúdo e Metaa
VISUALIZAÇÕES
Visualização de Análises Comportamentais
1. Mudança em padrões
2. Reclamações recorrentes
3. Envia muitos e-mails à noite
4. Imprime arquivos confidenciais