Datasheet

Blockbit XDR

EXTENDED DETECTION & RESPONSE

Visibilidade Total | **Proteção Proativa** | **Resposta Automática**

Blockbit XDR:
O Futuro da Cibersegurança

O Blockbit XDR (eXtended Detection & Response) é uma solução avançada de cibersegurança projetada para oferecer visibilidade, proteção e resposta abrangentes a ameaças em múltiplos vetores, como endpoints, redes, e-mails e ambientes em nuvem.

A plataforma integra-se de forma fluida com as infraestruturas de TI existentes, automatizando respostas a incidentes e simplificando a gestão de segurança, tudo em uma interface unificada.

Integração com o Blockbit Cyber Threat Intelligence (CTI)

A integração nativa com o Blockbit Cyber Threat Intelligence (CTI) eleva a proteção do Blockbit XDR, permitindo acesso a informações atualizadas sobre ameaças emergentes, vulnerabilidades e táticas de ataque.

Essa correlação de dados de segurança com inteligência global melhora a precisão na detecção de ameaças, reduzindo falsos positivos e acelerando respostas. Além disso, antecipa e neutraliza ameaças antes que se concretizem, garantindo uma defesa mais robusta e adaptável ao panorama dinâmico da cibersegurança.

Proteção avançada contra ransomware, phishing e ataques “zero day”

Combinando inteligência artificial, machine learning e análise comportamental avançada, o Blockbit XDR permite identificar e bloquear ataques sofisticados em tempo real e automatizar respostas a incidentes.

99.9%
Taxa de detecção de ameaças

+95%
Incidentes resolvidos automaticamente

+150
Integrações com soluções de mercado

Sobre a Blockbit

A **Blockbit** é líder em produtos de cibersegurança, protegendo milhares de empresas e milhões de usuários de ataques e ameaças digitais.

+5M
clientes corporativos

+2MM
usuários protegidos

Por que “eXtended Detection & Response”?

O Blockbit XDR oferece uma abordagem de segurança mais holística e integrada do que as soluções tradicionais de Endpoint Detection & Response (EDR), proporcionando visibilidade abrangente e defesa contra ameaças em toda a infraestrutura de TI.

Ao correlacionar dados de múltiplas fontes, o XDR aprimora a detecção de ameaças multi-vetoriais e automatiza respostas coordenadas, reduzindo a complexidade operacional e os custos associados à gestão de múltiplas ferramentas de segurança.

Compliance	Cloud	Automação
Conformidade com LGPD, GDPR, PCI DSS, ISO 27001, NIST, entre outras.	Integração nativa com Azure, AWS, Google Cloud, Microsoft 365, GitHub, Docker, entre outras.	Resposta em tempo real com remediação imediata para bloquear ataques.

Plataformas suportadas:

Blockbit Cloud
Blockbit XDR Manager

Cloud
- AWS
- Azure
- Google Cloud
- Microsoft 365
- GitHub
- Docker

Endpoints: Workstations & Servers
- Windows
- macOS
- Linux
- Solaris
- HP-UX
- AIX

Multi-Vetorial
Desktops, servidores, redes, apps, e-mails e nuvem.

Multi-Etapas
Detecção mais precisa com correlação de eventos.

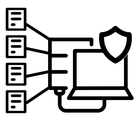
Integração
Interações holísticas para bloqueios e respostas precisas.

Automação
Orquestração e resposta automatizada.

Visibilidade
Compreensão mais ampla e contextualizada.

Descubra os principais módulos do Blockbit XDR:

Endpoint Threat & Attack Protection



Protege os endpoints contra malware, ameaças avançadas e ataques tanto através de assinaturas quanto através de comportamento para bloquear atividades maliciosas e processos suspeitos.

Compliance Management

Automatiza o monitoramento contínuo e a conformidade com leis, regulamentações e normas, como LGPD, PCI DSS, GDPR, ISO 27001 e NIST, garantindo uma gestão eficiente e contínua.

Active Response & Automated Remediation

Mitiga de forma automática as ameaças detectadas, como interrupção de processos maliciosos ou isolamento de um endpoint infectado, garantindo uma reação imediata e sem intervenção humana.

Application Allowlisting & Blocklisting

Configura e gerencia listas de permissões e restrições de aplicações, garantindo que apenas softwares autorizados sejam executados nos sistemas, prevenindo a execução de aplicações maliciosas.

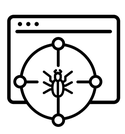
Behavioral Analysis

Detecta anomalias ou desvios de comportamento padrão que podem indicar uma ameaça, incluindo o monitoramento de comportamentos de usuários e aplicações para detectar atividades suspeitas.

File Integrity Monitoring (FIM)

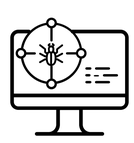
Monitora o sistema de arquivos detectando alterações no conteúdo, permissões, propriedade e atributos, e identifica os usuários e aplicativos usados para criar ou modificar arquivos.

Threat Hunting



Investigação e pesquisa avançada para identificar padrões de ataque e atividades suspeitas não detectadas por mecanismos de defesa tradicionais.

Host Intrusion Prevention System (HIPS)



Protege proativamente contra ameaças detectando comportamentos anômalos e bloqueando atividades maliciosas, como exploração de vulnerabilidades, ataques de força bruta e malware.

Asset Inventory & Visibility

Inventário e visibilidade em tempo real dos seus ativos, como aplicativos instalados, processos em execução, portas abertas, interfaces de rede, informações de hardware e sistema operacional.

Cloud Security

Visibilidade e proteção para workloads em ambientes de nuvem integrando com plataformas como Azure, AWS, Google Cloud, Microsoft 365, GitHub e Docker, monitorando serviços, máquinas virtuais e atividades.

Vulnerability Detection

Detecta automaticamente vulnerabilidades (CVE) nos ativos monitorados, identificando softwares desatualizados ou com falhas de segurança, para ações proativas e redução do risco de exposição.

Containers Security

Monitora e analisa atividades dentro de contêineres, como Docker e Kubernetes, para detectar e responder a ameaças como violações de contêineres ou vulnerabilidades de configuração.

Configuration Assessment

Avaliação contínua das configurações de segurança de sistemas, dispositivos e aplicativos, garantindo conformidade com normas internas, políticas de hardening e regulamentações de forma proativa.

Multi-Source Log Collection & Management

Avaliação contínua das configurações de segurança de sistemas, dispositivos e aplicativos, garantindo conformidade com normas internas, políticas de hardening e regulamentações de forma proativa.

Secure Internet Gateway

Filtra o conteúdo e controla o acesso dos endpoints à Internet, oferecendo também proteção avançada contra phishing e callbacks maliciosos, garantindo segurança proativa para workstations e servidores.

Malware Sandboxing

Integrado nativamente, emula e executa arquivos suspeitos na nuvem Blockbit, analisando comportamentos com IA e ML para identificar e examinar ameaças detectadas no ambiente.

Recursos	Itens	Blockbit XDR
Sensores	• Integrações com mais de 150 soluções de mercado	✓
Management	• Disponibilizada na Nuvem da Blockbit • Acessível via navegador web, sem a necessidade de instalação de software adicional • Permite um acesso unificado ou distribuído • Arquitetura de administração centralizada • Dashboard Mitre Basic • Dashboard Mitre Attack Framework (por estágio e técnicas) • Dashboard Mitre Radar (por applications, files, OS e network) • Dashboard Attack Map (origem dos ataques) • Custom Dashboards • Relatórios • API • CLI • Interface gráfica para configuração do manager • Interface gráfica para configuração do agente • Visibilidade de acesso à Internet • Integração SSO (Single Sign-On): LDAP • Integração SSO (Single Sign-On): Microsoft Active Directory • Integração SSO (Single Sign-On): SAML • Syslog Remoto para envio dos logs e auditoria • Multifator Authentication • Busca e detecção de IOCs (Indicators of Compromise) • Exportação de relatórios em CSV/XLS, texto e PDF • Notificações por E-mail, Remote Syslog, Webhook (HTTP/S), Mensageria (RabbitMQ, Kafka), Amazon SNS, Google Cloud Pub/Sub, Azure Event Hub	✓
Extended Security	• SIEM • Integração nativa com Threat Intelligence • Análise Comportamental de Usuários (UEBA) • Mecanismos para detecção, proteção e resposta à ameaças internas (Insider Threats) • Monitoramento de IoT/IIoT • Integração com NDR	✓
Compliance	• LGPD • PCI DSS • GDPR • HIPAA • NIST • TSC • ISO 27001	✓
Threat Intelligence	• Detecção de Anomalias com Blockbit Threat AI • Detecção de Anomalias com Machine Learning • Integração nativa com CTI de mercado • Integração nativa com Blockbit CTI • Integração nativa com Blockbit Sandbox • Integração com VirusTotal • Visualização da árvore de processos • Respostas a incidentes baseadas nos frameworks: MITRE ATT&CK, OWASP, CVSS ou NIST	✓

Recursos	Itens	Blockbit XDR
Endpoint Protection	• Sistemas Operacionais suportados (Windows, Linux, MacOs e Unix) • EPP/EDR Integrado • Orquestração de EPP/EDR • Host IPS • Configuration Assessment • Malware Detection - Hash • Malware Detection - Behavior • Malware Detection - YARA (manager) • Malware Detections - YARA (endpoint) • Rootkit Detection • Proteção contra Exploits • File Integrity Monitoring • Threat Hunting • Vulnerability Detection • Filtro de conteúdo web • Controle de acesso à Internet • Proteção avançada contra phishing • Proteção avançada contra callbacks maliciosos • Controle de Aplicações (Application Control) • Automação de Resposta a Incidentes (SOAR) • Proteção de manipulações (Anti-Tamper) • Senha para desinstalar o agente no Endpoint • Backup de Segurança e Recuperação de Incidentes • Bloqueio de mídia USB e Bluetooth • Modo apenas leitura para USB e Bluetooth • Exceções para USB e Bluetooth (nome, fornecedor, número de série, combinação) • Proteção específica para ataque de Ransomware • Proteção específica para ataque de Phishing • Proteção específica para ataque de Zero Day • Proteção e detecção de Programas Potencialmente Indesejados (PUPs) • Proteção contra malwares e ataques desconhecidos • Proteção contra Scripts Powershell maliciosos • Proteção contra Scripts CScript maliciosos • Proteção contra exfiltração de dados • Orquestração de regras de Firewall local • Proteção contra movimentação lateral • Proteção contra Vírus, trojans, worms, spyware, exploits, fileless, "Side Load DLL", adwares e outros tipos de códigos maliciosos • Proteção contra ataques de Overflow • Proteção contra alterações em “Live Memory (RAM)” • Proteção contra ataques de “drive-by download” • Proteção contra exploração de macro em arquivos do Microsoft Office • Proteção e Detecção contra mineradores de criptomoedas • Proteção contra escalação de privilégios • Proteção do Shadow Copy • Backups Regulares	✓
Cloud Security	• Monitoramento de Contêineres • Cloud Workload Protection • AWS • Azure • Microsoft 365 (proteção de e-mail, proteção de contas e proteção de arquivos - One Drive e SharePoint) • Data Loss Prevention - DLP (proteção para Microsoft 365) • Google Cloud (proteção de e-mail e proteção de contas) • GitHub • Docker	✓

Recursos	Itens	Blockbit XDR
Infraestrutura	• Redundância • Backup • Escalabilidade Automática • Proteção do ambiente	✓
Serviços	• Monitoramento 24×7 por SOC • Suporte Dedicado 24×7 • Resposta Proativa a Incidentes • Relatórios Detalhados e Personalizados • Automação Avançada de Resposta (via SOAR) • Investigação de Incidentes por Especialistas • Redução de Falsos Positivos (refinamento SOC) • Acompanhamento de Conformidade Regulamentar • Gestão e Ajuste Contínuo de Regras • Acesso a Inteligência de Ameaças Proprietária	✓