Produto de ponta para segurança e avaliação de risco: gerencia e monitora mudanças em configurações, hardening, patches, vulnerabilidades e políticas de conformidade dos ativos de TI e aplicações web.

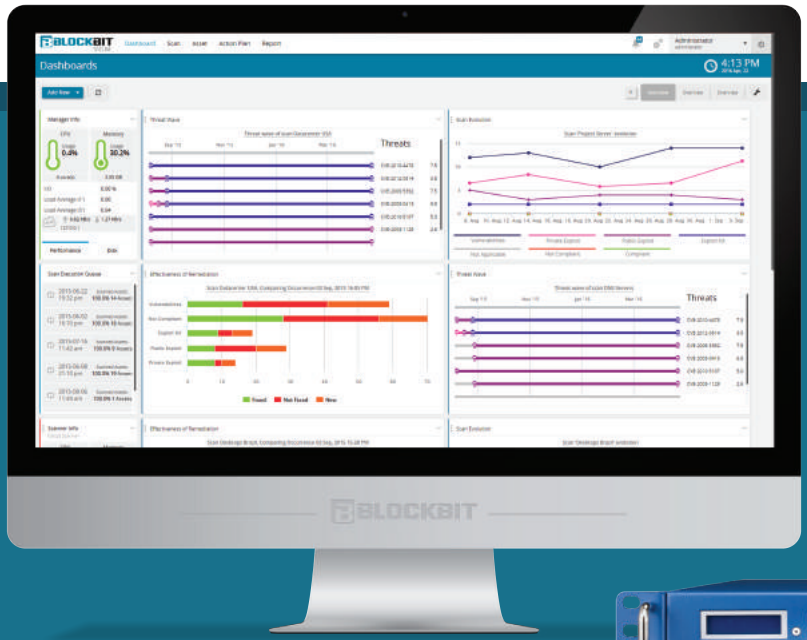
Gerenciamento de Vulnerabilidade e Conformidade

VCM | BLOCKBIT

Gerenciamento de Vulnerabilidade e Conformidade

Escalável, Eficaz e Fácil de usar.

Enquanto ataques online estão se tornando cada vez mais sofisticados e mais bem-sucedidos, e as obrigações regulamentares continuam aumentando, as organizações são confrontadas com o desafio de combater a constante evolução de ameaças avançadas ao mesmo tempo que precisam garantir a conformidade com as políticas. Para mitigar o risco neste ambiente de ameaças e obrigações de conformidade em constante mudança, as organizações precisam de um produto de vulnerabilidades e conformidades através de políticas que consigam abranger todos os tipos de ativos, ir além das ferramentas de avaliação de vulnerabilidades e gerenciamento de patches tradicionais, ser capaz de detectar ameaças avançadas e ter a capacidade de priorizar o processo de remediação, considerando as chances reais de exploração.



Destaques

- **Threat Wave:** Sistema de visualização revolucionário e único, onde é possível verificar as ameaças reais existentes na rede.
- **Action Plan:** Fluxo de trabalho de remediação avançado que permite atribuir a mitigação de problemas de segurança distribuindo corretamente para os profissionais responsáveis.
- **Effectiveness of Remediation:** Recurso inovador que fornece uma maneira simples de visualizar o progresso das remediações, comparando o estado entre duas varreduras (scans).
- **Asset Discovery:** Módulo avançado que detecta os ativos de sua rede, cria recorrência das pesquisas e identifica novos ativos adicionados à rede.
- **Distributed Architecture:** É possível multiplicar o número de ativos que serão analisados em paralelo reduzindo significativamente o tempo de execução dos scans, ou em diferentes unidades organizacionais com segmentos de rede não interligados.

Opções de Implantação: Hardware Appliance ou Virtual Appliance

BLOCKBIT

VCM | Descrição do Produto

O BLOCKBIT VCM é um produto de segurança e avaliação de riscos abrangente e escalável, que gerencia e monitora as alterações de configuração, vulnerabilidades, reforço e conformidades das políticas dos equipamentos, aplicações e ativos de TI, incluindo uma biblioteca de assinaturas, padrões industriais e regulamentações governamentais.

O BLOCKBIT VCM tem um recurso inovador que prioriza o processo de remediação baseado não só no grau de risco, mas também na disponibilidade de ferramentas para automatizar a exploração em diferentes estágios.

O BLOCKBIT VCM oferece facilidade de gerenciamento automatizado para criar métricas de base de segurança e medir de forma contínua a conformidade das políticas e regulamentações. Com painéis interativos e relatórios fáceis de gerar, BLOCKBIT VCM demonstra de forma simples, como os níveis de segurança e conformidade estão evoluindo. A solução também ajuda a reduzir os seus custos operacionais de TI ao automatizar os processos de avaliação, através de uma implantação distribuída, estruturada, reduzindo assim as necessidades de recursos adicionais.

Destaques

- **Threat Wave:** Sistema de visualização revolucionário e único, onde é possível verificar as ameaças reais existentes na rede.
- **Action Plan:** Fluxo de trabalho de remediação avançado que permite atribuir a mitigação de problemas de segurança distribuindo corretamente para os profissionais responsáveis.
- **Effectiveness of Remediation:** Recurso inovador que fornece uma maneira simples de visualizar o progresso das remediações, comparando o estado entre duas varreduras (scans).
- **Asset Discovery:** Módulo avançado que detecta os ativos de sua rede, cria recorrência das pesquisas e identifica novos ativos adicionados à rede.
- **Distributed Architecture:** É possível multiplicar o número de ativos que serão analisados em paralelo reduzindo significativamente o tempo de execução dos scans, ou em diferentes unidades organizacionais com segmentos de rede não interligados.

Fale conosco hoje mesmo ou visite nosso website para mais informações

+55 11 2165 8888

www.blockbit.com/pt-br/

VCM | **BLOCKBIT** Gerenciamento de Vulnerabilidade e Conformidade

Escalável, Eficaz

e

Fácil de usar

BLOCKBIT

VCM | Modelos de Equipamentos

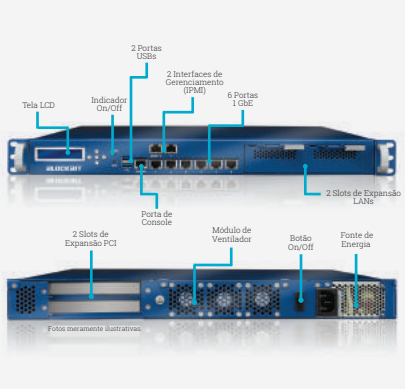
Virtual Appliance

Requisitos Mínimos	Manager / Scanner	Scanner
Memória RAM	8GB	4GB
Armazenamento	120GB	32GB
Processador	8 Core x86_64	4 Core x86_64

Hardware Appliance

BB 1000

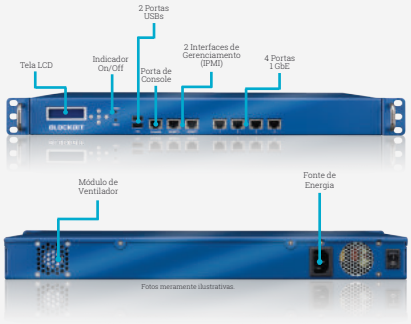
Manager / Scanner



16GB RAM
240GB SSD
8 LAN
2 Slots LAN *(opcional)*
8x 1GbE RJ45 ou 4x 10GbE Fiber *(opcional)*

BB 100

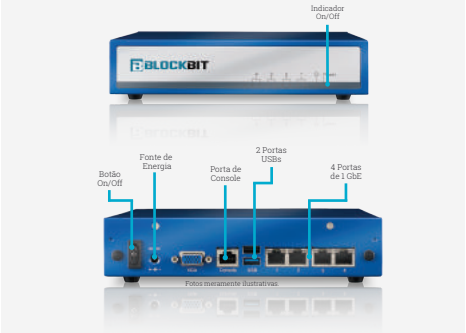
Manager / Scanner



16GB RAM
120GB SSD
6 LAN

BB 10

Scanner



4GB RAM
32GB SSD
4 LAN

- *Requisitos podem variar de acordo com a configuração dos scans (periodicidade, simultaneidade, número de IPs/ Web Applications)*

Implantação Flexível

BLOCKBIT VCM tem opções flexíveis de implantação:
Hardware Appliance ou Virtual Appliance.

Hardware Appliance

- Desempenho máximo
- Estabilidade garantida
- Instalação rápida

Virtual Appliance

- Maior escalabilidade
- Recuperação de desastres mais rápida
- Otimização da infraestrutura

BLOCKBIT

VCM | Diferenciais

Threat Wave

Threat Wave é o sistema de visualização revolucionário do BLOCKBIT VCM onde você pode verificar as ameaças reais existentes na rede, exibindo uma linha do tempo com os hosts afetados por falhas de segurança que contém qualquer exploit conhecido. Threat Wave permite que você visualize a progressão do risco através de circuitos e redes complexas, quando, onde e como um risco ou uma ameaça real estiver se espalhando dentro do ambiente, além de alertas de momentos críticos como a exposição a diferentes estágios de exploits.

Action Plan

Action Plan é um módulo do BLOCKBIT VCM que contém um fluxo de trabalho de reparação avançado e inovador e permite atribuir a mitigação de problemas de segurança distribuindo corretamente para os profissionais responsáveis de acordo com os níveis de (SLA), monitorando em seguida todo o progresso. A pessoa responsável pela mitigação dos problemas de segurança pode verificar se a correção foi aplicada com sucesso ou não, executar uma função de "Auto Auditoria", e o gerente de sistemas pode controlar a resolução dos problemas de segurança por meio de painéis gráficos.

Asset Discovery

BLOCKBIT VCM possui o módulo Asset Discovery, onde você pode encontrar os ativos de sua rede, criar recorrência das pesquisas e identificar novos ativos adicionados à rede. Com esse módulo, você pode importar os ativos encontrados em seu inventário BLOCKBIT VCM e também importar sua lista de ativos do Active Directory, ganhando velocidade e eficiência em seus scans.

Distributed Architecture

Um único Appliance Manager pode concentrar e correlacionar dados recolhidos por vários scanners, atendendo às necessidades de diferentes avaliações de segurança por tipo de scan, escopo, local ou unidade de negócio. Além disso, você pode multiplicar o número de ativos que serão analisados em paralelo, reduzindo significativamente o tempo de execução dos scans. Tudo a partir de um único ponto.

Effectiveness of Remediation

Effectiveness of Remediation é um recurso inovador do BLOCKBIT VCM que fornece uma maneira simples de visualizar o progresso das reparações, comparando o status entre dois scans, mostrando a eficácia do trabalho da equipe para mitigar o risco. A eficácia da reparação pode ser visualizada em um painel ou através da geração de um relatório específico mostrando o que foi corrigido, o que não foi corrigido e o que é um novo problema de segurança.

Multi-User Dashboard

Cada usuário do sistema pode criar seu próprio painel, adicionando os widgets que desejar e separando-os em diferentes abas.

Data Protection

O sistema inteiro é criptografado, garantindo que nenhum agente externo possa ter acesso aos dados de vulnerabilidades coletados pelo sistema, seja no Manager, no Scanner ou nos dados das credenciais dos sistemas para os scans autenticados.

BLOCKBIT

VCM | Outros Recursos

Policy Compliance

Monitore mudanças em configurações, reforçando a conformidade com as políticas de segurança dos ativos. Você pode criar modelos conforme a política da sua empresa, definir regras de conformidade baseadas em regulamentações e normas, gerenciar as políticas de segurança da sua organização e analisar se elas estão sendo aplicadas nos ativos, evitando possíveis violações da política de segurança. Além disso, você pode criar recorrência do sistema e identificar quando uma política não está sendo aplicada.

Non-Authenticated Vulnerability Scan

Com o Non-Authenticated Vulnerability Scan BLOCKBIT VCM (Scan Não-Autenticado de Vulnerabilidade) você pode encontrar as vulnerabilidades em sua rede de uma forma transparente e rápida. BLOCKBIT VCM usa mecanismos de scan avançados para identificar os serviços vulneráveis que colocam sua empresa em risco. Você pode detectar softwares sem patches, backdoors, certificados vencidos, protocolos de criptografia inseguros (como SSLv2), senhas fracas, protocolos de autenticação sem criptografia, serviços não autenticados (como FTP anônimo) e muitas outras vulnerabilidades.

Authenticated Vulnerability Scan

É possível realizar a avaliação detalhada de vulnerabilidades através do Authenticated Vulnerability Scan BLOCKBIT VCM (Scan Autenticado de Vulnerabilidade) para evitar falsos positivos e obter total visibilidade de todas as vulnerabilidades em seus ativos, incluindo softwares sem patches, configurações inseguras, plug-ins maliciosos, programas desatualizados, entradas de registros inseguras e muitas outras vulnerabilidades. Com o Scan Autenticado você não precisa confiar em serviços ou portas abertas para detectar vulnerabilidades. O sistema funciona sem a instalação de client. Os dados das credenciais dos sistemas para o Scan Autenticado estão seguros em sua Carteira de Credenciais BLOCKBIT VCM, protegida por criptografia.

Web Application Vulnerability Scan

Detecte vulnerabilidades em todas as camadas de aplicação web com um mecanismo capaz de rastrear e autenticar várias páginas com credenciais diferentes, incluir exceções e analisar respostas. O sistema é capaz de alertá-lo sobre os riscos em sua aplicação web simulando scans originados por dispositivos distintos, como smartphones e tablets, para testar aplicações web responsivas. O Web Application Security é indicado para DAST (Dynamic Application Security Testing) que avaliam aplicações web, como SQL Injection, Blind SQL Injection, XSS (Cross-Site Scripting), Execução de Comandos, Injeção de Código, Cross Site Request Forgery, Inclusão de Arquivos, Cookies Inseguros, entre outras vulnerabilidades.

Destaques

- **Threat Wave:** Sistema de visualização revolucionário e único, onde é possível verificar as ameaças reais existentes na rede.
- **Action Plan:** Fluxo de trabalho de remediação avançado que permite atribuir a mitigação de problemas de segurança distribuindo corretamente para os profissionais responsáveis.
- **Effectiveness of Remediation:** Recurso inovador que fornece uma maneira simples de visualizar o progresso das remediações, comparando o estado entre duas varreduras (scans).
- **Asset Discovery:** Módulo avançado que detecta os ativos de sua rede, cria recorrência das pesquisas e identifica novos ativos adicionados à rede.
- **Distributed Architecture:** É possível multiplicar o número de ativos que serão analisados em paralelo reduzindo significativamente o tempo de execução dos scans, ou em diferentes unidades organizacionais com segmentos de rede não interligados.

Fale conosco hoje mesmo ou visite nosso website para mais informações

+55 11 2165 8888

www.blockbit.com/pt-br/

VCM | BLOCKBIT Gerenciamento de Vulnerabilidade e Conformidade

Escalável, Eficaz

e

Fácil de usar

BLOCKBIT

BLOCKBIT VCM | Especificações Técnicas

Asset Management

- Descoberta de ativos no ambiente
- Descoberta de ativos recorrente a agendado
- Definição do escopo da rede para descoberta de ativos (IPv4)
- Registro de ativos
- Agrupamento de ativos por plataforma
- Agrupamento de ativos por unidades organizacionais
- Classificação de ativos por nível de criticidade (Low, Medium Low, Medium High, High)
- Importação de ativos registrados em domínio Windows
- Carteira para gerenciamento de credenciais
- Mapa para visualização de topologia da rede

Vulnerability Management

- Scan autenticado em plataforma Windows (SMB)
- Scan autenticado em plataforma Linux (SSH)
- Scan não autenticado
- Scan em múltiplas redes (IPv4)
- Scan recorrente e agendado
- Scan history
- Scan evolution
  - Visualização por Ativo
  - Visualização por Vulnerabilidade
  - Threat Wave
  - Effectiveness of Remediation
- Políticas de scan personalizadas
- SSL Scanning (HTTPS)
- Ajustes de desempenho do scan (velocidade, delay, timeout, número de conexões)
- Sistemas Linux suportados
  - Canonical Ubuntu Linux 12.04 LTS
  - Canonical Ubuntu Linux 14.04 LTS
  - CentOS-3
  - CentOS-4
  - CentOS-5
  - CentOS-6
  - CentOS-7
  - Red Hat Enterprise Linux 3
  - Red Hat Enterprise Linux 4
  - Red Hat Enterprise Linux 5
  - Red Hat Enterprise Linux 6
  - Red Hat Enterprise Linux 7
  - SUSE Linux Enterprise Server 10
  - SUSE Linux Enterprise Server 11
  - SUSE Linux Enterprise Server 12
- Sistemas Windows suportados
  - Microsoft Windows Vista
  - Microsoft Windows 7
  - Microsoft Windows 8
  - Microsoft Windows 8.1
  - Microsoft Windows 10
  - Microsoft Windows Server 2003
  - Microsoft Windows Server 2008
  - Microsoft Windows Server 2008 R2
  - Microsoft Windows Server 2012
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2016

Policy Compliance

- Policy Compliance em plataforma Windows (SMB)
- Policy Compliance em plataforma Linux (SSH)
- Scan em múltiplas redes (IPv4)
- Scan recorrente e agendado
- Scan history
- Scan evolution
  - Visualização por Ativo
  - Visualização por Compliance
  - Effectiveness of Remediation
- Políticas de scan personalizadas
- Sistemas Linux suportados
  - Red Hat Enterprise Linux 5
  - Red Hat Enterprise Linux 6
- Sistemas Windows suportados
  - Microsoft Windows Vista
  - Microsoft Windows 7
  - Microsoft Windows 8
  - Microsoft Windows 8.1
  - Microsoft Windows 10
  - Microsoft Windows Server 2003
  - Microsoft Windows Server 2008
  - Microsoft Windows Server 2008 R2
  - Microsoft Windows Server 2012
  - Microsoft Windows Server 2012 R2

Web Application Scanning

- Scan recorrente e agendado
- Scan history
- Scan evolution
  - Visualização Ativo
  - Visualização por Ameaça
  - Effectiveness of Remediation
- Políticas de scan personalizadas
- Personalização de User-Agent
- Ajustes de desempenho do scan (requisições simultâneas, timeout, profundidade)
- Módulos suportados
  - Common Backdoors Detection
  - Backup Files
  - Captcha Detection
  - Code Injection
  - Common Directories
  - Credit Card number disclosure
  - Cross-site request forgery
  - Directory Listing
  - File Inclusion
  - .htaccess LIMIT misconfiguration
  - Insecure Coockies
  - LDAP Injection
  - ASP Localstart
  - Command Injection
  - Auto-complete for password from fields
  - Path Transversal
  - Private IP address disclosure
  - Response splitting
  - Remote File Inclusion
  - Session Fixation
  - Source code disclosure
  - SQL Injection
  - Blind SQL Injection
  - Insecure Transport Layer Protection for password forms
  - Unvalidated Redirect
  - WebDAV Detection
  - Xpath Injectino
  - Cross-Site Scripting (XSS)
  - HTTP TRACE detection

Action Plan

- Gerenciamento de múltiplos planos de ação
- Acompanhamento de solução de problemas (Action Board)
- Auditoria de resolução no plano de ação (Audit View e Self Audit)
- Definição personalizada de SLA
- Arquivamento

Gerenciamento

- Interface de gerenciamento Web
- Interface de gerenciamento em linha de comando (CLI)
- Ferramenta de backup e recuperação de configurações
- Arquitetura distribuída e gerenciamento de múltiplos scanners
- Múltiplos Dashboards personalizados
  - Widget de monitoramento do sistema
  - Widget de monitoramento dos scans
  - Widget de status e consumo da licença
  - Widget de alertas do sistema
  - Widget de Top 10
  - Widget de Security Issues
  - Widget de Security Indicators
  - Widget de Scan Evolution
  - Widget de Effectiveness of Remediation
  - Widget de Threat Wave
- Redirecionamento de logs via Syslog
- Relatórios flexíveis
  - Security Issues by Assets
  - Security Issues by Vulnerabilities
  - Effectiveness of Remediation
  - Top 10 unique vulnerabilities by host
  - Top 10 unique vulnerabilities by risk
- Exportação de relatórios em múltiplos formato (PDF, XLSX)
- Monitor de tráfego de rede
- Monitor de serviços e status do sistema
- Monitor de eventos do sistema
- Notificações e alertas do sistema por E-mail
- Múltiplos administradores com controles de acesso
- Controle de mudanças e logs de auditoria

20190320 - v1.4rev00

AMÉRICA LATINA
Rua Eng. Francisco Pitta Brito 779 – 3º andar
São Paulo – SP 04753-080 – Brasil
Tel.: +55 11 2165 8888

AMÉRICA DO NORTE
703 Waterford Way – 4th floor
Miami – FL 33126 – United States
Tel.: +1 305 373 4660

EUROPA
2 Kingdom Street – 6th floor
London – W2 6BD – England
Tel.: +44 203 580 4321

www.blockbit.com