BLOCKBIT

Cutting edge security and risk assessment product to manage and monitor configuration changes, hardening, vulnerabilities and policy compliance of IT assets and web applications.

Vulnerability and Compliance Management

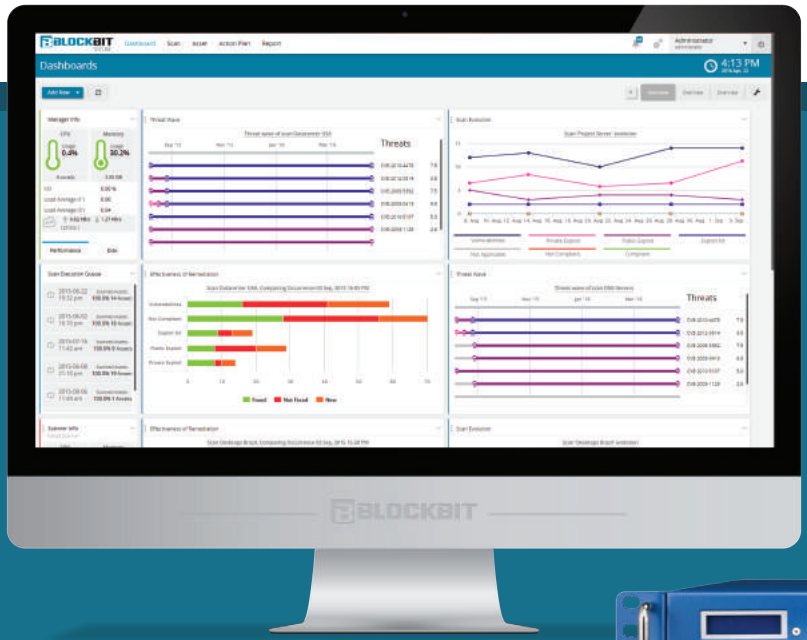
VCM | BLOCKBIT
Vulnerability and Compliance Management

Scalable, Effective and User-Friendly.

As online attacks become more sophisticated and successful, and regulatory obligations are continually increasing, organizations face the challenge to combat ever-evolving advanced threats as well as to achieve policy compliance. In order to mitigate risk in the constantly changing threat and compliance landscape, organizations need a vulnerability management and policy compliance product that can cover all kinds of assets, go beyond traditional vulnerability assessment and patch management tools, be able to detect advanced threats and to prioritize the remediation process considering the real chances of exploitation.

Highlights

- **Threat Wave:** The revolutionary and unique viewing system where you can check the real threats within your network.
- **Action Plan:** The advanced remediation workflow that allows you to assign the mitigation of security issues to appropriate staff members.
- **Effectiveness of Remediation:** The innovative feature that grants you with a simple way to visualize the progress of the remediations by comparing the status of two scans.
- **Asset Discovery:** The advanced module where you can find the assets of your network, create recurrence of the searches and identify new assets added to the network.
- **Distributed Architecture:** You can multiply the number of assets scanned in parallel and significantly reduce the scan time.



Deployment Options: Hardware Appliances or Virtual Appliances

BLOCKBIT

VCM | Product Description

BLOCKBIT VCM is a comprehensive, scalable security and risk assessment product, that manages and monitors configuration changes, vulnerabilities, hardening and policy compliance of IT assets, devices and applications, including a signature library, industry standards and government regulations.

BLOCKBIT VCM has an innovative feature that prioritizes the remediation process, based not only on the risk classification, but on the availability of tools to automate the exploitation in different stages.

BLOCKBIT VCM offers you ease, automated management to create security baseline metrics and to continuously measure compliance with policies and regulations. With interactive dashboards and easy-to-generate reports, BLOCKBIT VCM effortlessly shows the evolution of security and compliance. It also helps to reduce your IT operational costs by automating assessment processes through a structured, distributed deployment, therefore reducing the need for additional resources.

Highlights

- **Threat Wave:** The revolutionary and unique viewing system where you can check the real threats within your network.
- **Action Plan:** The advanced remediation workflow that allows you to assign the mitigation of security issues to appropriate staff members.
- **Effectiveness of Remediation:** The innovative feature that grants you with a simple way to visualize the progress of the remediations by comparing the status of two scans.
- **Asset Discovery:** The advanced module where you can find the assets of your network, create recurrence of the searches and identify new assets added to the network.
- **Distributed Architecture:** You can multiply the number of assets scanned in parallel and significantly reduce the scan time.

Call us today or visit our website for more information

+1-305-373-4660
www.blockbit.com

VCM | **BLOCKBIT** Vulnerability and Compliance Management

Scalable, Effective and User-Friendly.

BLOCKBIT

VCM | Appliances Models

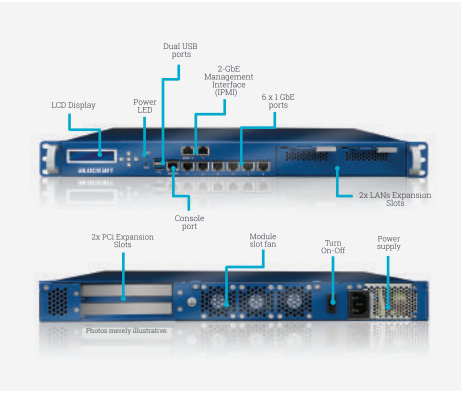
Virtual Appliance

Minimum requirements	Manager / Scanner	Scanner
RAM	8GB	4GB
Storage	120GB	32GB
Processor	8 Core x86_64	4 Core x86_64

Hardware Appliance

BB 1000

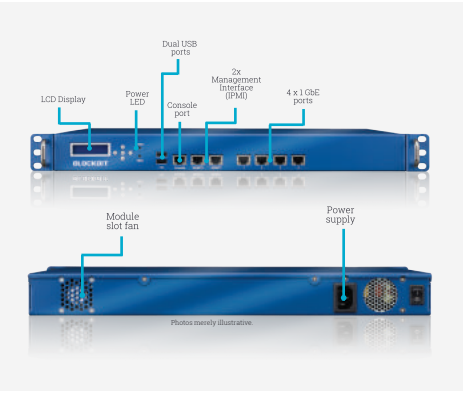
Manager / Scanner



16GB RAM
240GB SSD
8 LAN
2 Slots LANs *(optional)*
8x 1GbE RJ45 or 4x 10GbE Fiber *(optional)*

BB 100

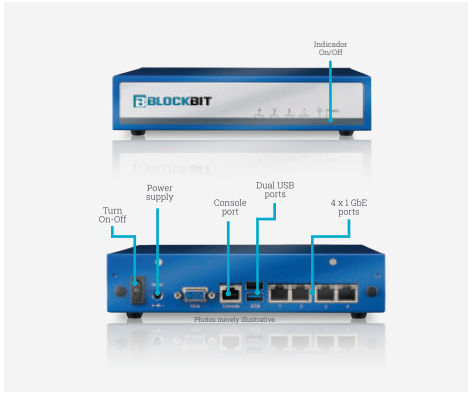
Manager / Scanner



16GB AM
120GB SSD
6 LAN

BB 10

Scanner



4GB RAM
32GB SSD
4 LAN

- *Requirements may vary depending on the configuration of scans (periodicity, concurrency, number of IPs / Web Applications)*

Flexible Deployment

BLOCKBIT VCM has flexible deployment options:
Hardware Appliance or Virtual Appliance.

Hardware Appliance

- Maximum performance
- Stability Guaranteed
- Fast installation

Virtual Appliance

- Greater scalability
- Faster disaster recovery
- Infrastructure optimization

BLOCKBIT

VCM | Differentiators

Threat Wave

Threat Wave is BLOCKBIT VCM's revolutionary viewing system, where you can check the real threats within your network, displaying a timeline with hosts affected by security flaws that contain any known exploit. Threat Wave allows you to visualize risk progression across complex networks and tracks when, where and how a risk or a real threat is spreading within the environment. It alerts critical moments such as exposure to different stages of exploits.

Action Plan

Action Plan is a module that contains an advanced and innovative remediation workflow that allows you to assign the mitigation of security issues to the appropriate staff. Just set an owner and service level agreement (SLA) for the task and monitor its progress. The person responsible for the security issues mitigation can check whether the correction was applied successfully or not by running a "Self Audit" function, and the system manager can track the resolution of the security issues through graphic dashboards.

Asset Discovery

BLOCKBIT VCM's Asset Discovery module allows you to find the assets of your network, create recurrence of the searches and identify new assets added to the network. With the system, you can import the assets found into BLOCKBIT VCM inventory and also import your Active Directory assets list, gaining speed and efficiency in your scan.

Distributed Architecture

A single Manager Appliance can concentrate and correlate data collected by several Scanner Appliances, meeting the needs of different security assessments by type of scan, scope, location or business unit. Also, you can multiply the number of assets being scanned in parallel and reduce significantly the scan time allowing you to perform fast scans in large environments. All managed by a single point.

Effectiveness of Remediation

Effectiveness of Remediation is an innovative BLOCKBIT VCM feature that gives you a simple way to visualize the progress of the remediations by comparing the status of two scans. It shows how effective is your team working to mitigate risks. Progress can be visualized on a dashboard or by generating a specific report that shows what was fixed, not fixed and new security issues.

Multi-User Dashboard

Each system user can tailor their own dashboard by adding widgets they want and separating it into different tabs.

Data Protection

The whole system is encrypted, assuring that no external agent can get access to the vulnerability data collected by the system, whether in the Manager, Scanner or on the system's credentials data for the authenticated scans.

BLOCKBIT

BLOCKBIT VCM | Other Features

Policy Compliance

You can monitor configuration changes, hardening and policy compliance of IT assets. Create templates according to your company policy, define compliance rules based in regulations and standards, manage your organization's security policies and analyze if they are being applied to corporate assets, avoiding non-compliance and/or possible security breaches. Your policies can be automatically verified on different platforms, ensuring a wide coverage on corporate security controls. In addition, you can create system recurrence and have visibility of the exact moment when a policy is no longer been enforced.

Non-Authenticated Vulnerability Scan

With BLOCKBIT VCM Non-Authenticated Vulnerability Scan you can find vulnerabilities in your network in an invisible and fast way. BLOCKBIT VCM uses advanced scan engines to identify vulnerable services that put your business at risk. You can detect unpatched software, backdoors, expired certificates, unsafe cryptographic protocols (such as SSLv2), weak passwords, unencrypted authentication protocols, unauthenticated services (such as anonymous FTP) and many other vulnerabilities.

Authenticated Vulnerability Scan

You can perform deep vulnerability assessment through BLOCKBIT VCM Authenticated Vulnerability Scan. Avoid false positives and have full visibility of all the vulnerabilities within your assets including unpatched software, insecure configurations, malicious plug-ins, outdated software, insecure registry entries and many other vulnerabilities. The system is clientless, and it doesn't affect the performance of the analyzed asset. BLOCKBIT VCM Scanner does all the processing job. The system's credentials data for the Authenticated Scan are safe in your BLOCKBIT VCM Credential Wallet, protected by two strong encryption layers.

Web Application Vulnerability Scan

BLOCKBIT VCM Web Application Vulnerability Scan is able to detect vulnerabilities on every layer of web application, using an advanced engine to track, authenticate in various pages using different credentials, with the capability to include exceptions and understand responses. It is also able to alert you about the security risks in your web application simulating scans originated by distinct devices such as Smartphones and Tablets to test responsive web applications. This feature is indicated for Dynamic Application Security Testing (DAST), assessing web applications such as SQL Injection, Blind SQL Injection, XSS (Cross-Site Scripting), Command Execution, Code Injection, Cross Site Request Forgery, File Inclusion, Insecure Cookies, among other vulnerabilities.

Highlights

- **Threat Wave:** The revolutionary and unique viewing system where you can check the real threats within your network.
- **Action Plan:** The advanced remediation workflow that allows you to assign the mitigation of security issues to appropriate staff members.
- **Effectiveness of Remediation:** The innovative feature that grants you with a simple way to visualize the progress of the remediations by comparing the status of two scans.
- **Asset Discovery:** The advanced module where you can find the assets of your network, create recurrence of the searches and identify new assets added to the network.
- **Distributed Architecture:** You can multiply the number of assets scanned in parallel and significantly reduce the scan time.

Call us today or visit our website for more information

+1-305-373-4660

www.blockbit.com

VCM | **BLOCKBIT** Vulnerability and Compliance Management

Scalable, Effective and User-Friendly.

BLOCKBIT

BLOCKBIT VCM | Technical Specifications

Asset Management

- Asset Discovery of in the environment
- Recurring and Scheduled Asset Discovery
- Network Scope Definition for Asset Discovery (IPv4)
- Asset Registration
- Asset grouping by platform
- Asset grouping by organizational units
- Asset classification by criticality level (Low, Medium Low, Medium High, High)
- Import assets registered in Windows domain
- Portfolio for credential management
- Network topology visualization map

Vulnerability Management

- Authenticated Scan on Windows Platform (SMB)
- Authenticated Scan on Linux Platform (SSH)
- Non-authenticated Scan
- Scan on multiple networks (IPv4)
- Recurring and Scheduled Scan
- Scan history
- Scan evolution
  - View per asset
  - View per Vulnerability
  - Threat Wave
  - Effectiveness of Remediation
- Custom Scan Policies
- SSL Scanning (HTTPS)
- Scan performance settings (speed, delay, timeout, number of connections)
- Supported Linux systems
  - 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
- Supported Windows Systems
  - 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 on Windows platform (SMB)
- Policy Compliance on Linux platform (SSH)
- Scan on multiple networks (IPv4)
- Recurring and Scheduled Scan
- Scan history
- Scan evolution
  - View per asset
  - View per Compliance
  - Effectiveness of Remediation
- Custom Scan Policies
- Supported Linux systems
  - Red Hat Enterprise Linux 5
  - Red Hat Enterprise Linux 6
- Supported Windows Systems
  - 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

- Recurring and Scheduled Scan
- Scan history
- Scan evolution
  - View per Asset
  - View per Threat
  - Effectiveness of Remediation
- Custom Scan Policies
- User-Agent Customization
- Scan performance settings (simultaneous requests, timeout, depth)
- Supported Modules
  - 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

- Management of multiple Action Plans
- Troubleshooting (Action Board)
- Audit of resolution in the action plan (Audit View and Self Audit)
- Custom SLA
- Archiving

Management

- Web Management Interface
- Command Line Interface Management (CLI)
- Backup and configuration recovery tool
- Distributed architecture and management of multiple scanners
- Multiple Custom Dashboards
  - System Monitoring Widget
  - Scans Monitoring Widget
  - Status and License Consumption Widget
  - System Alert Widget
  - Top 10 Widget
  - Security Issues Widget
  - Security Indicators Widget
  - Scan Evolution Widget
  - Effectiveness of Remediation Widget
  - Threat Wave Widget
- Redirecting logs via Syslog
- Flexible reports
  - Security Issues by Assets
  - Security Issues by Vulnerabilities
  - Effectiveness of Remediation
  - Top 10 unique vulnerabilities by host
  - Top 10 unique vulnerabilities by risk
- Reports Exported in multiple formats (PDF, XLSX)
- Network traffic Monitor
- Services and system status Monitor
- System events Monitor
- System notifications and alerts by E-mail
- Multiple administrators with access controls
- Change control and audit logs

NORTH AMERICA
703 Waterford Way – 4th floor
Miami – FL 33126 – United States
Phone: +1 305 373 4660

LATIN AMERICA
Rua Eng. Francisco Pitta Brito 779 – 3º andar
São Paulo – SP 04753-080 – Brazil
Phone: +55 11 2165 8888

EUROPE
2 Kingdom Street – 6th floor
London – W2 6BD – England
Phone: +44 203 580 4321

www.blockbit.com

BLOCKBIT
It´s easy to be secure