



Total Visibility



Proactive Protection



Automated Response

Blockbit XDR: The Future of Cybersecurity

Blockbit XDR (eXtended Detection & Response) is an advanced cybersecurity solution designed to provide comprehensive visibility, protection, and response to threats across multiple vectors, including endpoints, networks, emails, and cloud environments.

The platform integrates seamlessly with existing IT infrastructures, automating incident responses and simplifying security management, all within a unified interface.

Integration with Blockbit Cyber Threat Intelligence (CTI)

Native integration with Blockbit Cyber Threat Intelligence (CTI) enhances the protection of Blockbit XDR, providing access to up-to-date information on emerging threats, vulnerabilities, and attack tactics.

This correlation of security data with global intelligence improves threat detection accuracy, reduces false positives, and speeds up response times. Additionally, it anticipates and neutralizes threats before they materialize, ensuring a more robust and adaptive defense in the dynamic cybersecurity landscape.

Advanced protection against ransomware, phishing and “zero day” attacks

Combining artificial intelligence, machine learning and advanced behavioral analytics, Blockbit XDR enables you to identify and block sophisticated attacks in real time and automate incident responses.

99.9%

Threat detection rate

+95%

Incidents resolved
automatically

+150

Integrations with
market solutions

About Blockbit

Blockbit is a leader in cybersecurity products, protecting thousands of companies and millions of users from digital attacks and threats.



+5M
corporate
clients



+2MM
protected
users

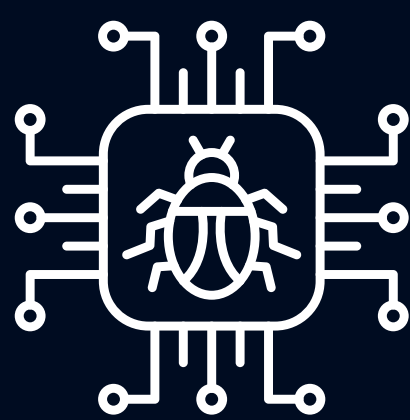
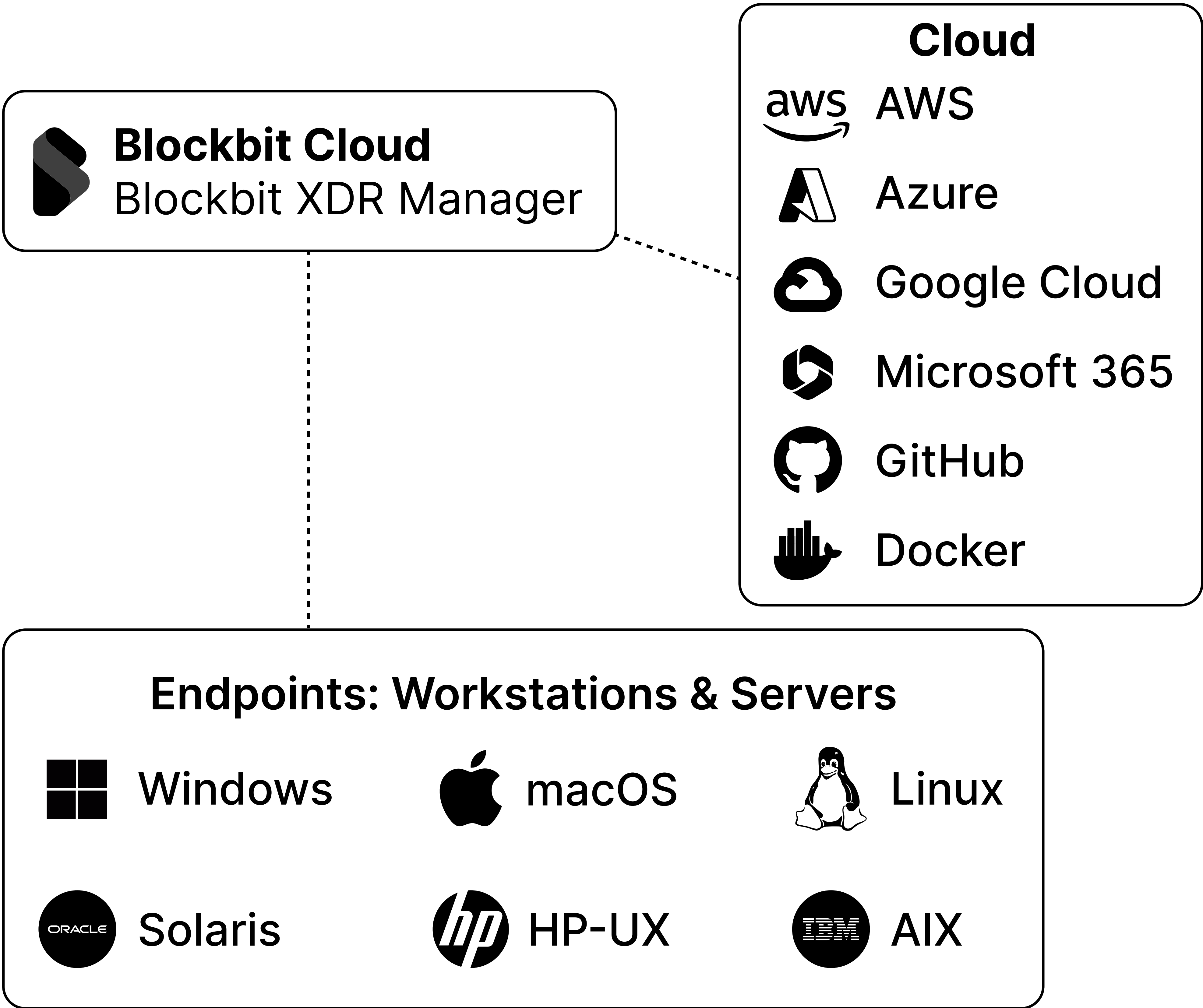
Why “eXtended Detection & Response”?

Blockbit XDR offers a more holistic and integrated approach to security than traditional Endpoint Detection & Response (EDR) solutions, providing comprehensive visibility and threat defense across the entire IT infrastructure.

By correlating data from multiple sources, XDR enhances multi-vector threat detection and automates coordinated responses, reducing the operational complexity and costs associated with managing multiple security tools.

Compliance	Cloud	Automation
Compliance with LGPD, GDPR, PCI DSS, ISO 27001, NIST, among others.	Native integration with Azure, AWS, Google Cloud, Microsoft 365, GitHub, Docker, among others.	Real-time response with immediate remediation to block attacks.

Supported platforms:



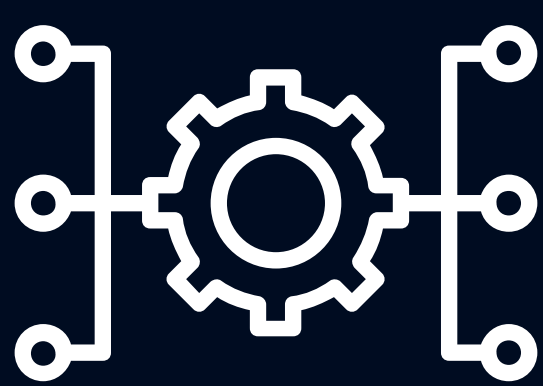
Multi-Vector

Desktops, servers, networks, apps, emails and cloud.



Multi-Stage

More accurate detection with event correlation.



Integration

Holistic interactions for accurate blocks and responses.



Automation

Orchestration and automated response.



Visibility


Broader and more contextualized understanding.

Discover the main modules of **Blockbit XDR**:



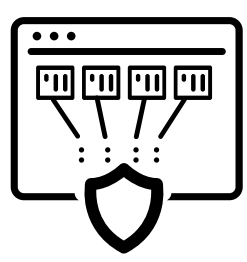
Endpoint Threat & Attack Protection

Protects endpoints against malware, advanced threats, and attacks through both signatures and behavior to block malicious activity and suspicious processes.



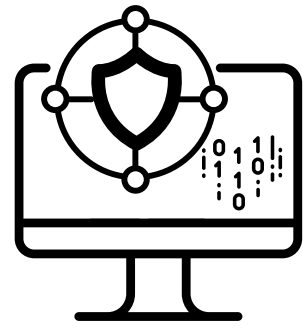
Compliance Management

Automates continuous monitoring and compliance with laws, regulations, and standards such as LGPD, PCI DSS, GDPR, ISO 27001, and NIST, ensuring efficient and ongoing management.




Active Response & Automated Remediation

Automatically mitigates detected threats, such as interrupting malicious processes or isolating an infected endpoint, ensuring an immediate reaction without human intervention.




Application Allowlisting & Blocklisting

Configures and manages application permissions and restrictions lists, ensuring that only authorized software runs on systems, preventing malicious applications from running.



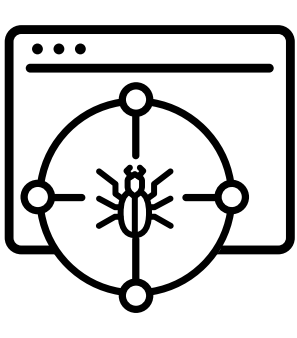
Behavioral Analysis

Detects anomalies or deviations from standard behavior that may indicate a threat, including monitoring user and application behaviors to detect suspicious activity.



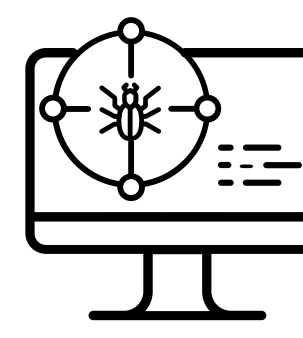
File Integrity Monitoring (FIM)

Monitors the file system for changes in content, permissions, ownership, and attributes, and identifies the users and applications used to create or modify files.




Threat Hunting

Advanced investigation and research to identify attack patterns and suspicious activities not detected by traditional defense mechanisms.




Host Intrusion Prevention System (HIPS)

Proactively protects against threats by detecting anomalous behavior and blocking malicious activities such as vulnerability exploits, brute force attacks, and malware.




Asset Inventory & Visibility

Real-time inventory and visibility into your assets, such as installed applications, running processes, open ports, network interfaces, hardware and operating system information.



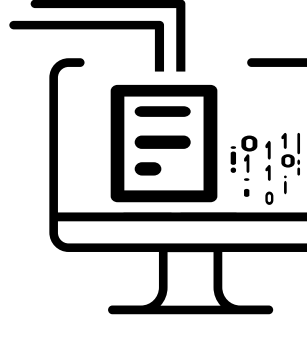
Cloud Security

Visibility and protection for workloads in cloud environments integrating with platforms such as Azure, AWS, Google Cloud, Microsoft 365, GitHub and Docker, monitoring services, virtual machines and activities.




Vulnerability Detection

Automatically detects vulnerabilities (CVE) in monitored assets, identifying outdated software or software with security flaws, for proactive actions and reducing the risk of exposure.




Containers Security

Monitors and analyzes activity within containers, such as Docker and Kubernetes, to detect and respond to threats such as container breaches or configuration vulnerabilities.




Configuration Assessment

Continuous assessment of the security configurations of systems, devices and applications, ensuring compliance with internal standards, hardening policies and regulations in a proactive manner.



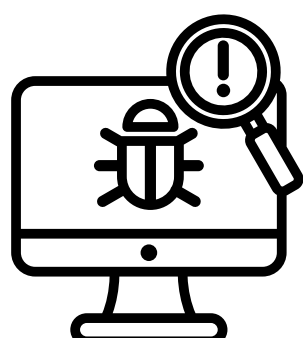
Multi-Source Log Collection & Management

Continuous assessment of the security configurations of systems, devices and applications, ensuring compliance with internal standards, hardening policies and regulations in a proactive manner.








Secure Internet Gateway


Filters content and controls endpoint access to the Internet, also offering advanced protection against phishing and malicious callbacks, ensuring proactive security for workstations and servers.




Malware Sandboxing

Natively integrated, it emulates and executes suspicious files in the Blockbit cloud, analyzing behaviors with AI and ML to identify and examine threats detected in the environment.

Resources	Items	Blockbit XDR
Sensors	<ul style="list-style-type: none">Integrations with over 150 market solutions	
Management	<ul style="list-style-type: none">Available on the Blockbit CloudAccessible via web browser, without the need to install additional softwareAllows unified or distributed accessCentralized administration architectureMitre Basic DashboardMitre Attack Framework Dashboard (by stage and techniques)Mitre Radar Dashboard (by applications, files, OS and network)Attack Map Dashboard (origin of attacks)Custom DashboardsReportsAPICLIGraphical interface for configuring the managerGraphical interface for configuring the agentVisibility of Internet accessSSO (Single Sign-On) integration: LDAPSSO (Single Sign-On) integration: Microsoft Active DirectorySSO (Single Sign-On) integration: SAMLRemote Syslog for sending logs and auditingMultifactor AuthenticationSearch and detection of IOCs (Indicators of Compromise)Export of reports in CSV/XLS, text and PDFEmail Notifications, Remote Syslog, Webhook (HTTP/S), Messaging (RabbitMQ, Kafka), Amazon SNS, Google Cloud Pub/Sub, Azure Event Hub	
Extended Security	<ul style="list-style-type: none">SIEMNative integration with Threat IntelligenceUser Behavior Analytics (UEBA)Mechanisms for detecting, protecting, and responding to insider threats (Insider Threats)IoT/IIoT monitoringIntegration with NDR	
Compliance	<ul style="list-style-type: none">LGPDPCI DSSGDPRHIPAANISTTSCISO 27001	
Threat Intelligence	<ul style="list-style-type: none">Anomaly Detection with Blockbit Threat AIAnomaly Detection with Machine LearningNative integration with market CTINative integration with Blockbit CTINative integration with Blockbit SandboxIntegration with VirusTotalProcess tree visualizationIncident response based on frameworks: MITRE ATT&CK, OWASP, CVSS, or NIST	

Resources	Items	Blockbit XDR
Endpoint Protection	<ul style="list-style-type: none">• Supported Operating Systems (Windows, Linux, MacOS and Unix)• Integrated EPP/EDR• EPP/EDR Orchestration• Host IPS• Configuration Assessment• Malware Detection - Hash• Malware Detection - Behavior• Malware Detection - YARA (manager)• Malware Detections - YARA (endpoint)• Rootkit Detection• Exploit Protection• File Integrity Monitoring• Threat Hunting• Vulnerability Detection• Web Content Filter• Internet Access Control• Advanced Phishing Protection• Advanced Malicious Callback Protection• Application Control• Incident Response Automation (SOAR)• Anti-Tamper Protection• Agent Uninstall Password on Endpoint• Security Backup and Incident Recovery• USB and Bluetooth Media Blocking• Read-only Mode for USB and Bluetooth• Exceptions for USB and Bluetooth (name, vendor, serial number, combination)• Specific Protection Against Ransomware Attacks• Specific Protection Against Phishing Attacks• Specific Protection Against Zero Day Attacks• Detection and Protection Against Potentially Unwanted Programs (PUPs)• Protection Against Unknown Malware and Attacks• Protection Against Malicious PowerShell Scripts• Protection Against Malicious CScript Scripts• Protection Against Data Exfiltration• Local Firewall Rule Orchestration• Protection Against Lateral Movement• Protection Against Viruses, Trojans, Worms, Spyware, Exploits, fileless, "Side Load DLL", Adware and Other Malicious Code Types• Protection Against Overflow Attacks• Protection Against "Live Memory (RAM)" Changes• Protection Against "Drive-by Download" Attacks• Protection Against Microsoft Office File Macro Exploitation• Detection and Protection Against Cryptocurrency Miners• Protection Against Privilege Escalation• Shadow Copy Protection• Regular Backups	
	<ul style="list-style-type: none">• Container Monitoring• Cloud Workload Protection• AWS• Azure• Microsoft 365 (Email Protection, Account Protection, and File Protection - OneDrive and SharePoint)• Data Loss Prevention - DLP (Protection for Microsoft 365)• Google Cloud (Email Protection and Account Protection)• GitHub• Docker	

Resources		Items	Blockbit XDR
Infrastructure		<ul style="list-style-type: none">• Redundancy• Backup• Auto-Scaling• Environment Protection	
		<ul style="list-style-type: none">• 24/7 Monitoring by SOC• 24/7 Dedicated Support• Proactive Incident Response• Detailed and Customized Reports• Advanced Response Automation (via SOAR)• Incident Investigation by Experts• False Positive Reduction (SOC Tuning)• Regulatory Compliance Tracking• Continuous Rule Management and Fine-Tuning• Access to Proprietary Threat Intelligence	