BLOCKBIT

Innovative secure email gateway product that has an Anti-Spam with state-of-the-art heuristic analysis, a built-in Antivirus, sophisticated Anti-Phishing and an advanced Data Loss Prevention

Secure eMail eXchange

SMX | BLOCKBIT
Secure eMail eXchange

Powerful and Simple-to-Manage.

Email is the most common form of communication used in the corporate world. With 80% of emails containing spam and over 10% of these emails including malicious content, protecting your email service with a good secure email gateway solution including Anti-Spam and Antivirus capabilities is crucial to maintaining the entire security of your systems and data.

Highlights

- SmartFolder: Innovative feature to handle messages that were delivered as SPAM and also folders that help them manage their listings (Whitelist / Blacklist).
- Advanced Heuristic Analysis: Advanced module that can receive feedback from users through the SmartFolders, achieving an accuracy rate of over 99%.
- Multi-Conditional Policies: Infinite combinations for conditions can be created on SMX to determine whether or not a message should be sent or received.
- Unique Instance Storage: The UIS does not allow the same message sent to a group of users to be duplicated, saving on storage and backup costs.
- Storage Encryption: Stored messages are encrypted and protected against non-authorized access.

Deployment Options:
Hardware Appliances, Virtual Appliances & Cloud Appliances

Data Sheet

SMX | Product Description

BLOCKBIT SMX (Secure eMail eXchange) is an Email Firewall system, a complete secure Email Gateway, and has all the features of an Email Server. The Email Firewall allows you to create thousands of conditions to determine if a message can be delivered to or sent by your company. It also has an Anti-Spam feature with heuristic analysis, a built-in Antivirus, a sophisticated Anti-Phishing and an advanced Data Loss Prevention (DLP) capability.

In addition, BLOCKBIT SMX can integrate with other email systems such as Exchange, or act alone playing the role of a MTA (Mail Transfer Protocol – SMTP/S) and a MRA (Mail Retrieval Agent - IMAP/S) with flexible deployment options.

Flexible Implementation

BLOCKBIT SMX has flexible deployment options:
Hardware Appliance, Virtual Appliance or Cloud Appliance.

Hardware Appliance

- Maximum performance at all times
- Guaranteed stability
- Fast installation

Virtual Appliance

- Greater scalability
- Faster disaster recovery
- Infrastructure optimization

Cloud Appliance

- Ready and available environment
- Quick implementation
- Accessible everywhere

Highlights

- SmartFolder: Innovative feature to handle messages that were delivered as SPAM and also folders that help them manage their listings (Whitelist / Blacklist)
- Advanced Heuristic Analysis: Advanced module that can receive feedback from users through the SmartFolders, achieving an accuracy rate of over 99%.
- Multi-Conditional Policies: Infinite combinations for conditions can be created on SMX to determine whether or not a message should be sent or received.
- Unique Instance Storage: The UIS does not allow the same message sent to a group of users to be duplicated, saving on storage and backup costs.
- Storage Encryption: Stored messages are encrypted and protected against non-authorized access.

Call us today or visit our website for more information

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

SMX | BLOCKBIT Secure eMail eXchange

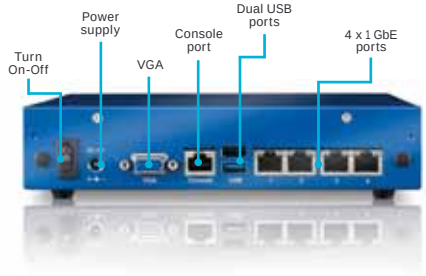
Powerful and Simple-to-Manage

Data Sheet

SMX | Appliances Models

Model BB 10

Small Business

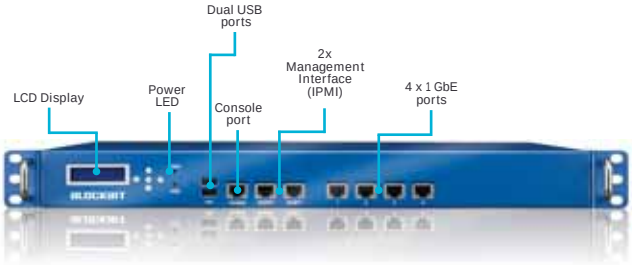


Specification

- Appliance model BB 10
- Quad-core processor 1.9Ghz
- 4GB Memory
- 120GB SSD
- 4 LANs (2 Bypass) + 1 Cons

Model BB 100

Mid-Size Business

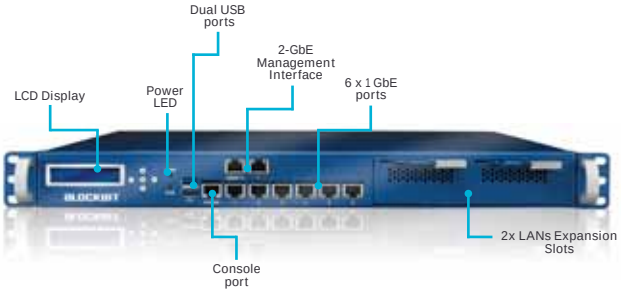


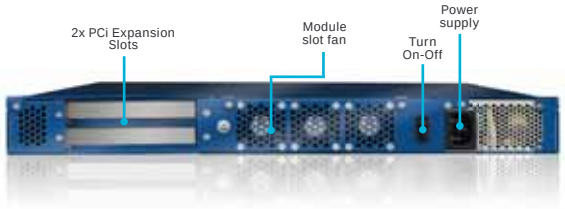
Specification

- Appliance model BB 100
- Octa-core processor 2.4Ghz
- 8GB Memory
- 120GB SSD
- 4 LANs (2 Bypass) + 2 Mgt + 1 Cons

Model BB 1000

Large Business



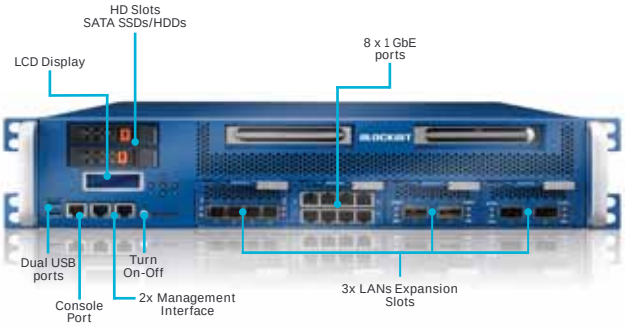


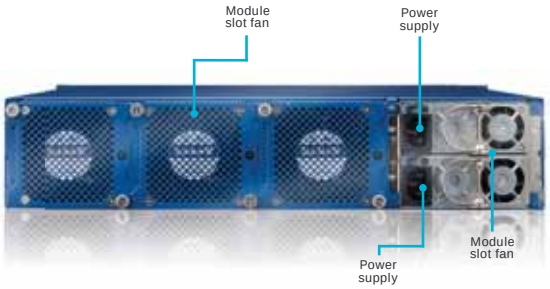
Specification

- Appliance model BB 1000
- Quad-core processor 4 threads 3.5Ghz
- 16GB Memory
- 240GB SSD
- 6 LANs (3 Bypass) + 2 Mgt + 1 Cons
- 2x LANs expansion slots
- LAN expansion per slot (optional)
  8x 1GbE RJ45 or 4x 10GbE Fiber

Model BB 10000

Enterprise & Datacenter





Specification

- Appliance model BB 10000
- 2x Octa-core processors 16 threads 2.6 Ghz
- 32GB Memory
- 480GB SSD
- 8 LANs (4 Bypass) + 2 Mgt + 1 Cons
- 3x LANs expansion slots
- LAN expansion per slots (optional)
  8x 1GbE RJ45 or 4x 10GbE Fiber

Hardware Appliances, Virtual Appliances or Cloud Appliances

SMX

	BB 10	BB 100	BB 1000	BB 10000
Accounts for Mail Firewall	100	500	2,000	10,000
Accounts for Mail Firewall and Mail Server	50	250	650	6,500
Max Cluster (Require an Extra Appliance)	2	3	5	20
Max Accounts for Mail Firewall with Max Cluster	200	1,500	10,000	200,000
Max Accounts for Mail Firewall and Mail Server with Max Cluster	100	750	3,250	130,000
Min Required LANs per Appliance	1	1	1	1
Max Allowed LANs per Appliance	2	2	2	2
Email Storage for Mail Server (Only for Cloud Appliance)	**60 GB** (included)	**240 GB** (included)	**600 GB** (optional)	**1.8 TB** (optional)

BLOCKBIT

Data Sheet

SMX | Differentiators

SmartFolder

BLOCKBIT SMX users get SmartFolder in their mailboxes to handle messages that were delivered as SPAM and also folders that help them manage their listings (Whitelist / Blacklist), without the need to leave the comfort of their email client, such as Outlook for desktop or a mobile email client.

Advanced Heuristic Analysis

BLOCKBIT SMX is a complete Anti-Spam that meets the various RFCs for SPAM controlling and combating. It also includes a heuristic analysis module that can receive feedback from users through the SmartFolder, achieving an accuracy rate of over 99%.

Multi-Conditional Policies (Email Firewall)

Infinite combinations for conditions can be created on SMX to determine whether or not a message should be sent or received. With this flexibility, it is practically impossible not to meet the diverse demands for control that you may have.

Unique Instance Storage

The UIS (Unique Instance Storage) is a feature that does not allow the same message sent to a group of users to be duplicated, saving on storage and backup costs. Crucial for cloud systems and larger environments.

Queue-less

All compliance, Anti-Spam and malware analyses are made during the message transport time, eliminating the need for a message processing queue in parallel. Thus, eliminating the delays on sending and receiving messages.

Storage Encryption

With this feature enabled messages stored by BLOCKBIT SMX are not violated even when intercepted. Even a “sysadmin” with unrestricted access to the stored messages will not have access to the information.

Native Archiving

BLOCKBIT SMX has a native email archiving system, without the need to purchase any additional system or module. The archiving is done through policies based on the company’s needs and can be accessed by any email client via the SmartFolder.

Native Cluster

BLOCKBIT SMX offers a native cluster of email services to meet the different sizes of companies and numbers of mailboxes. The system can operate in GRID mode providing high availability and service balancing.

Data Sheet

SMX | Key Features

Anti-Spam

BLOCKBIT SMX has a powerful Anti-Spam tool. In addition to conventional Anti-Spam features, our appliance also offers the self learning feature through validation algorithms and has several security bases that are generated and maintained by our Intelligence Lab. The Anti-Spam tool also includes the analysis of Mail Compliance, based on a set of actions and conditions for content filtering and policies to receive and send messages with a maximum level of prevention against a variety of violations in message handling. In addition to RFCs, Blacklist, Whitelist and Mail Reputation, maintained by our Intelligence Lab, our Anti-Spam offers the SmartFolder feature that captures the messages reclassification actions that is available on email clients from IMAP connections.

Antivirus/Anti-Malware

BLOCKBIT SMX includes an internal Antivirus/Anti-Malware feature that is updated several times a day searching for new threats that can infect your network. BLOCKBIT SMX scans the file, separates the items by content type (e.g. HTML, Doc, Flash, Zip, Exe, BATS, VBS, OCTET STREAM, JPEG, GIF, MPEG, PNG, TIF, etc) and analyzes the compliance rules even before delivering the email into the user's mailbox. In addition, BLOCKBIT Anti-Malware detects and blocks incoming or outgoing messages infected by known and unknown viruses, trojans, worms, rootkits, adware, spyware, in real-time which dramatically reduces the number of false positives.

Anti-Phishing

BLOCKBIT SMX has a sophisticated Anti-Phishing technology in multiple layers to combat and stop phishing attacks that bypass many security systems. BLOCKBIT SMX detects links that induces the users to mistakes, allows you to implement conditional policies to block messages containing links, blocks messages from malicious senders and has a heuristic learning system that blocks emails based in messages previously blocked for being a phishing.

DLP - Data Loss Prevention

BLOCKBIT SMX takes care of both your inbound and outbound emails, protecting you from external and also internal threats. Through the DLP (Data Loss Prevention) capability BLOCKBIT SMX helps you to protect your confidential information from data-leak incidents. You can configure policies using regular expressions to identify sensitive information inside any message (such as SSN - Social Security Number - credit card data, source code, etc) and define an action: block, alert, send a copy, reroute, or even sending a captcha. These rules can be applied to everyone or only to specific Active Directory groups, users, email accounts, etc. This capability helps you also to comply with the PCI DSS, HIPAA, SOX (Sarbanes-Oxley), and many other regulations.

Email Firewall

BLOCKBIT SMX uses Email Firewall technology with the concept of Multi-Conditional Policies. Through its actions and conditions BLOCKBIT SMX can reach millions of rule combinations in order to meet the specific compliance needs of your company. Issues with emails that were impossible to solve, now are easily resolved using a friendly and intuitive interfaced powered by sophisticated BLOCKBIT SMX engines.

Data Sheet

SMX | Key Features

Email Server

BLOCKBIT SMX has a powerful Email Server that can act as your single messaging solution, without the need for additional investments. It includes both sending and receiving email protocols (SMTP/S, IMAP/S). Our email server has a set of folders (SmartFolder) that allows the user to interact with their Quarantine, Whitelist and Blacklist through your favorite mail client, without the need to use portals or other tools. Another key differentiator is the UIS (Unique Instance Storage) technology that consolidates emails with the same content, providing storage and backup savings, performance gains and agility in data maintenance.

Email Archive

Many organizations are required to keep records of email communications in order to comply with standards and regulations. BLOCKBIT SMX can create Email Archiving policies that allow you to read archived emails directly from your email client (e.g. Outlook) even on smartphones. Unlike other Email Archive tools in the market, BLOCKBIT SMX Email Archive feature is already included as part of the solution and not sold separately.

Encrypted Email

BLOCKBIT SMX Email Server enables end-to-end encryption. This means all messages stored on the server are secure. Even with physical access to the server it is impossible to have access to the information stored ensuring the integrity and confidentiality.

Email Reputation

BLOCKBIT SMX Email Reputation is a feature with a database maintained by our Intelligence Lab with thousands of signatures to verify the qualification of the email senders. This source of reputation is also powered by its own millions of BLOCKBIT SMX users worldwide. When a user receives an email, they can choose to mark it as good or bad and this information, after correlated and analyzed, feeds the reputation base. This database is replicated to all BLOCKBIT SMX Email Servers and is an effective method to protect your organization against unwanted SPAMMERS and emails.

Other Features

- Email quota by Account, Group and General. Includes Notifications
- Mail Retrieval. Email Search on Other Servers (Pop / Imap / Pops and Imaps)
- SmartFolder (Quarantine, Blacklist, Whitelist). The Users Themselves Manage and Control Their Preferences
- Address List Sync by LDAP (MS Exchange)
- Address Sync by LDAP
- Customization of Automatic Responses
- Customization of Block Messages
- Support for Multiple Domains
- Integration with RBL
- Integration with TLD (Top Level Domain)
- Email Forwarding by Condition
- Captcha by Condition
- Action to Reject Messages for a Limited Time
- Condition by Reputation
- Condition by Period
- Filter by Regular Expression in the Message Body
- Service Certificate Issuance
- Third-Party Certificate Import
- Several Types of Reports
- Load Balancing
- High Availability
- Attachment Filter by MiME-Type
- Queue-Less, Incoming Messages are Analyzed and Delivered in Real Time

BLOCKBIT

Data Sheet

SMX | Technical Specification

Mail Server

- Protocols (IMAP, IMAPs, POP, POPs, SMTP and SMTPs)
- End-to-End Encryption (TLS / SSL)
- Authentication Methods (PLAIN and LOGIN)
- Relay Control
- Multiple Domain Support
- Support to UIS (Unique Instance Storage) Systems
- Mailbox Encryption (64 Bits; 128 Bits and 192 Bits)
- User Accounts (Local and Integration AD/Ldap Base)
- Control of Number of Messages
- Quota by User
- SmartFolder
- SmartAction
- Archiving
- Maintenance of Mailboxes by User and Group
- Balancing of IMAP / POP Connections
- RBL Queries
- Mail Retriever for Connections to Other Email Servers

Anti-Spam

- Heuristic Learning
- SmartFolder
- Blacklist / Whitelist
- RFC's (822, 2822)
- Learning Through Lists and Number of Occurrences on Blacklist / Whitelist
- Reputation Database

Policy Sensors

- Anti-Spam Exception Policies
- Anti-Malware Exception Policies
- RBL (Real-Time Blocking List) Exception Policies

Firewall Local (Security)

- Configurable Policy
  - Grouping by Network Zones
  - Exclusive for Services (SMTP, SMTPS, SMTP Submission, IMAP, IMAPS POP3, POP3S and HTTPS -Webmail-)
- Packet Filter
  - Entry Policies
- Security
  - DoS (Denied of Service) Protection
  - PortScan Protection
  - Protection for Invalid Packets
  - SYN Flood Protection
  - ICMP Flood Protection
  - ICMP Controls
    - Echo/Request PING
    - ICMP Redirect
    - ICMP Broadcast
  - Source Routing
  - Checksum
  - Invalids Logs
  - TCP_Be_Liberal
- TCP / UDP connection controls

Anti-Malware

- Message Split by Content Type. (HTML, DOC, FLASH, ZIP, EXE, BATS, VBS, OCTET STREAM, JPG, GIF, MPEG, PNG, TIF, Etc)
- Block List for URLs and Domains
- List of Malicious Files (Trojans, Worms, Rootkits, Adware, Spywares, Etc)
- Automatic and Periodic Updates of the Malware Base
- Heuristic Analysis
- Block Encrypted Files
- Detect Malicious Applications (PUA)

Mail Compliance

- + 4 Million Possibilities
- Filter by Content. (Header, Attachments, Mime Type, Message Text, Links, Attachment Size and Among Others, Etc)
- Mail Reputation
- Anti-Phishing
- Anti-Malware
- Anti-Spam
- Antivirus
- RBL (Real-Time Blocking List)
- Operating Method
  - Groups by Purpose
  - Sorting by Priority
- First-Match-Wins by Final Type Action
  - Receive
  - Block
  - Reject
  - Discard
  - Move to Quarantine
  - Send Captcha
  - Send Captcha and Add on Whitelist
  - Divert to Another SMTP Server
- DLP – by Compliance
- Size of the Recipient List

Webmail

- Protocols (SMTP/ SMTPS / IMAP / IMAPS)
- Secure Connection (TLS / SSL)
- Access to External Catalog (LDAP)
- Automatic Response Support (User-Configurable)
- Support When Accessing SmartFolder (Whitelist, Blacklist, Quarantine)

General Resources

- Kernel SMP x86 64 Bits
- Interfaces
  - Ethernet
  - MACVLAN
  - VLAN
  - DSL
- Support SNMP Protocol
- H.A. (High Availability)
- Update Date and Time with Support for NTP Servers (Network Time Protocol)
- Automatic and Periodic System Updates for Corrections and Releases
- HTTPS WEB Administration
- Management Dashboard
- Disaster Recovery (Backup / Restore)
- Storage
  - NFS
  - DISK (HDD)
- Synchronization of Users and Groups with Windows AD Servers and LDAP Servers
- Authentication
  - Local
  - Windows
  - AD/LDAP
- Support to Multiple Authentication Domains
- SSL Certificates
- Resource Objects
  - IP Address
  - Timetable
  - Periods and Dates Table
  - Keywords (Set of Words and/or Regular Expressions)
  - Content Types

NORTH AMERICA (Headquarters)
1450 Brickell Avenue – 14th floor
Miami – FL – 33131
UNITED STATES
Phone: +1 305 373 4660

EUROPE (Main Office)
2 Kingdom Street – 6th floor
Paddington – London – W2 6JP
UNITED KINGDOM
Phone: +44 203 580 4320

LATIN AMERICA (Main Office)
Alameda dos Tupinás 33 – 5º Andar
São Paulo – SP – 04069-000
BRAZIL
Phone: +55 11 2165 8888

BLOCKBIT

It´s easy to be secure.