Blockbit

Datasheet

Blockbit GSM
Global Security Management

blockbit.com

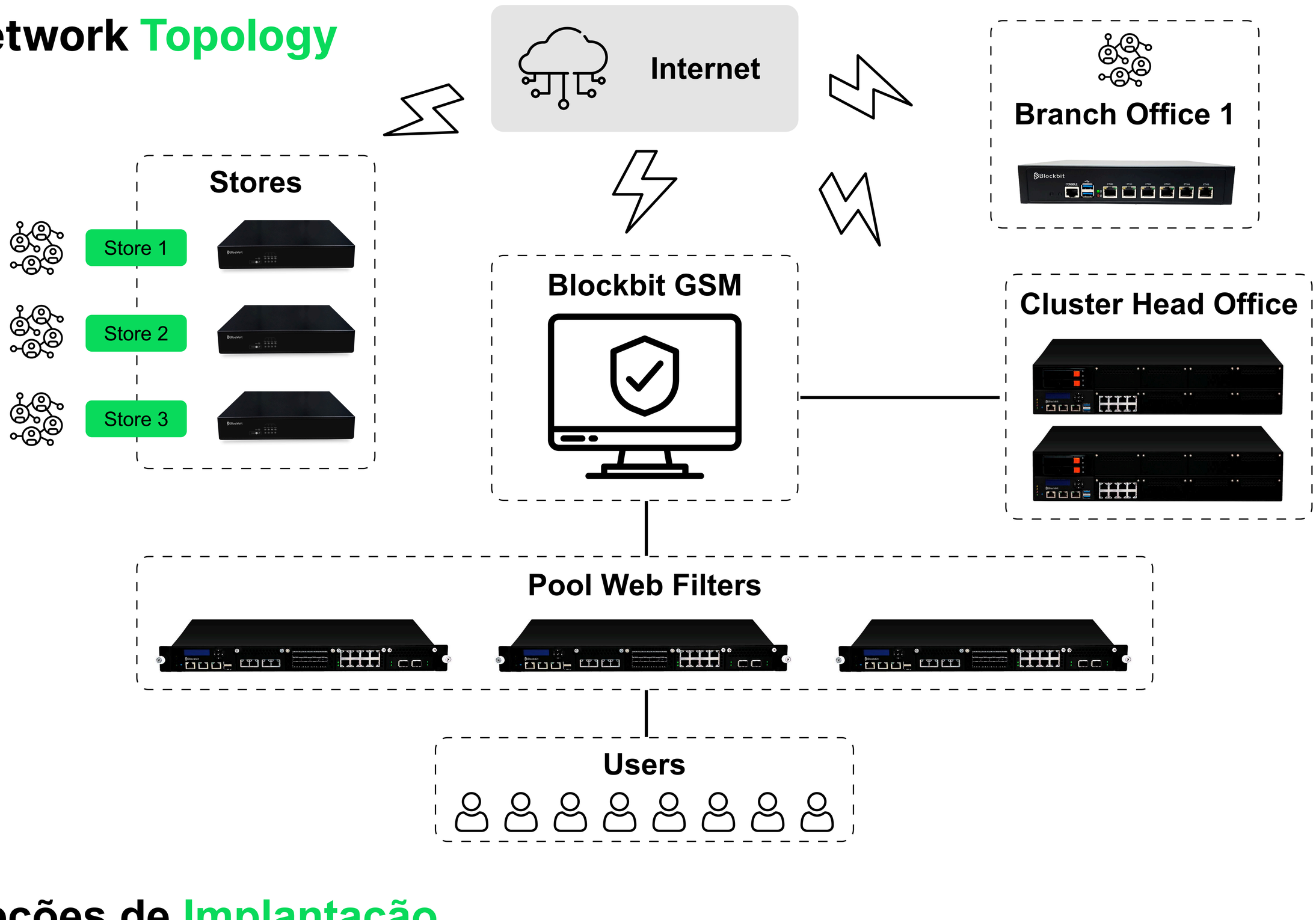
Sobre o Blockbit GSM

O Blockbit GSM (Global Security Management) é a solução responsável pelo gerenciamento centralizado da plataforma Blockbit, permitindo administrar de forma unificada múltiplos dispositivos e recursos de segurança distribuídos na infraestrutura. Integrado ao ecossistema da Blockbit Platform, o GSM atua como o ponto de controle que simplifica operações, consolida políticas e garante maior eficiência na gestão de ambientes complexos.

A solução combina funções de gerenciamento (Manager) e análise (Analyzer), possibilitando a criação e distribuição de configurações padronizadas, além da coleta e correlação de logs e eventos de tráfego em tempo real. Com isso, os administradores conseguem ter visibilidade completa do ambiente e responder de forma mais eficiente a incidentes de segurança.

Além disso, o Blockbit GSM foi projetado para oferecer uma operação intuitiva e escalável, com recursos como provisionamento automatizado, inventário de dispositivos, gestão de políticas e análise avançada de dados.

Network Topology



Opções de Implantação

Hardware Appliance

Appliance físico dedicado para alto desempenho com controle total do hardware e suporte a redundância.

Virtual Appliance

VM compatível com VMware ESXi, XenServer, KVM e ProxMox. Implantável em nuvens públicas (AWS, Azure, Oracle, Google, IBM).

Plataformas suportadas

Virtualização:
VMware ESXi | XenServer | KVM | ProxMox

Cloud Pública:
AWS | Azure | Oracle | Google | IBM

Interface:
Português BR e English US

Gerenciamento Centralizado

Recursos	Itens	Blockbit GSM
Dispositivos, Inventário e Deploy	• Gerenciamento centralizado de múltiplos NGFWs (físicos e virtuais) • Inventário com nome, modelo, versão, licença e status em tempo real • Organização por grupos e communities (multi-tenant) • Visualização em mapas online de geolocalização (Geomap) • Device Templates com presets: UTM, IPS, ATP, SWG ou Custom • Módulos configuráveis: Firewall, Proxy, Web Cache, Web Filter, Threat, IPS, SD-WAN, DHCP, DNS • Zero Touch Provisioning (ZTP) individual e em lote (Batch Provisioning) • Configuração automática de rede: hostname, DNS, NTP, gateway, interfaces e zonas • Aplicação automática de templates e políticas no primeiro boot do NGFW • Backup centralizado com restore dos equipamentos gerenciados • Reboot, desligamento remoto e atualização centralizada com rollback • Automações de gestão: sincronismo de regras e orquestração centralizada	✓
Políticas, Perfis e Objetos	• Pacotes de políticas IPv4 e IPv6 com versionamento e controle de versão • Ordenamento Pre Rules / Local Rules / Post Rules para priorização • Validação automática de conflitos e redundâncias entre políticas (IPv4) • Contagem de utilização (hit count) por regra para otimização de performance • Regras com data de expiração e ativação por horário/período (Schedules) • Perfis centralizados: Web Filter, App Control, Threat, IPS, SSL Inspection, SD-WAN • Objetos: Addresses, Services, Time, Schedules, Dictionaries, Contents • Usuários e Grupos centralizados com autenticação por zona • Deploy com fluxo de aprovação, auditoria, agendamento e rollback • Clonagem de perfis e políticas para replicação rápida • Suporte a QoS integrado nas políticas com Traffic Shaping • Suporte a grupos para servidores de autenticação (AD, LDAP, Radius)	✓
SD-WAN Orchestration	• Orquestração centralizada de perfis SD-WAN em múltiplos NGFWs • Tipos de perfil: Load Balance, Failover, Spillover e Dynamic Selection • Monitoring Interval configurável (em segundos) e Fail Ratio (1-100%) • Monitoring Targets com IPs virtuais e testes de conectividade • Métricas SLA por circuito: Jitter (ms), Latency (ms) e Packet Loss (%) • Monitoramento de Inbound/Outbound (bits RX/TX) por circuito WAN com histórico • Estatísticas por interface: entrada/saída de pacotes, descartes e erros • Services SD-WAN com priorização por porta, protocolo e aplicação • Application-Aware Routing (AAR) com seleção dinâmica do melhor link • WAN Aggregation e Link Failover com detecção automática de falha • Orquestração de VPNs site-to-site, Full Mesh e Star (HUB-Spoke) • Visualização de jitter, latência e packet loss por link e por circuito no Analyzer	✓
Observabilidade por Aplicação	• Identificação de tráfego por aplicação, independente de porta/protocolo • Classificação automática de aplicações em tempo real • Métricas por aplicação: latência, jitter e perda de pacotes • Correlação aplicação x link (WAN/SD-WAN) para análise de performance • Análise de experiência do usuário (QoE) por aplicação • Detecção de degradação de aplicações em tempo real • Flow analysis com drill-down até nível de fluxo individual • Monitoramento de performance e comportamento de tráfego por aplicação • Correlação entre consumo de banda e performance por aplicação • Visão unificada: rede, segurança e performance aplicacional	✓

Analyzer e Relatórios

Recursos	Itens	Blockbit GSM
Analyzer, Correlação e Dashboards	• +90 visões pré-construídas distribuídas em 6 módulos de análise • Firewall: Geolocation, Zone Traffic, Top User, Top Service, Top Source, Top Policy • Web Filter: Allowed/Denied Sites, History Categories, Domains, Profiles, Content Types • Application Control: Top Allowed/Denied Apps, Top Allowed/Denied Categories, History • IPS: Alerted/Blocked, Geolocation, Impact High/Medium/Low, Layer 3 Protection • Threat Protection: Threats/Malwares History, Malicious IP Classification, Top Threat Types • User Behavior: Network Traffic, Policy/App/Web Usage, Threat/IPS por usuário • Dashboards customizados para visibilidade personalizada do tráfego • Correlação multi-device com filtros combinados (src, dst, protocol, user, threat) • Correlação temporal: Today, Yesterday, Last 7/30 days, This/Last Month, By Date/Period • Drill-down com redirecionamento automático para Events detalhados	✓
Monitoramento e Performance	• Monitoramento em tempo real de status e desempenho dos equipamentos • Status de túneis VPN site-to-site e client-to-site (Up/Down/Connected) • Visualização de usuários remotos conectados via VPN com detalhes de sessão • Performance por aplicação com jitter, latência e packet loss • Performance por link WAN/SD-WAN com comparativo entre conexões • Monitoramento de CPU, memória, disco e storage por dispositivo • Monitoramento de HA: Cluster Status, Uptime, Connection e Sync Status • Captura de pacotes (PCAP) por regra de IPS para análise forense • Integração com ferramentas de monitoramento externo via SNMP • Geomap para visualização geográfica dos dispositivos e alertas • Redução de MTTR com troubleshooting avançado e correlação	✓
Relatórios e Business Intelligence	• Tipos Analysis: Network Traffic, Policy Usage, Web Filter, App Control • Tipos Analysis: Intrusion Prevention, Threat Protection, User Behavior • Tipo Log: queries personalizadas com exportação CSV • Custom Reports integrado com ferramentas de Discover, Visualize e Dashboard • Fontes de dados: logs gerais, tráfego por aplicação e métricas de SD-WAN • Campos BI: jitter, latency, packet_loss, bandwidth, protocol, timestamp • Relatórios de qualidade por aplicação e por link (SD-WAN aware) • Histórico de performance: latência, jitter e perda por período • Duplicação de relatórios existentes para personalização rápida • Agendamento: única vez, semanal e mensal com envio automático por e-mail • Exportação em HTML, PDF e CSV; gráficos em SVG e PNG • Personalização de logo e rodapé por relatório (Custom Branding)	✓

Loggers, Eventos e Diferenciais

Recursos	Itens	Blockbit GSM
Loggers e Armazenamento	• Múltiplos Loggers: Standalone e Integrated • Cluster de Loggers com HA, failover automático e replicação em tempo real • IP Virtual, Heartbeat, sincronismo configurável e Virtual MAC • Capacidade escalável de armazenamento de logs indexados (dimensionável por ambiente) • Rotação automática de logs por porcentagem de disco e período (dias/meses/anos) • Backup automático em storages remotos: SMB, NFS e SFTP • Retenção configurável por quantidade de backups e porcentagem de uso de disco • Indexação de logs para busca acelerada sem abertura de arquivos antigos • Logs consolidados por Device ou grupo de Devices • Visualização gráfica do total de logs gerados por período • Monitoramento de CPU, memória, disco e storage por Logger • Histórico centralizado de backups com restore e status de execução	✓
Eventos e Busca Avançada	• Events com visualização próximo ao tempo real por logger ou grupo • Query Editor com +30 filtros: logtype, src, dst, sport, dport, protocol, service • Filtros: devin/devout, zonein/zoneout, client_mac/user/ip, geoip_src/dst • Filtros: rule_name/action, web_category/site/method/mime, app_name/category • Filtros: ips_profile, malware_file/md5/status/name, threat_class/category/sid/impact • Operadores: Contain, Not Contain, Equals, Not Equals com string editável • Salvar e reutilizar queries personalizadas (Save Query) • Análise de desempenho e detecção de problemas com base nos logs • Top Hits, History (gráfico de barras) e Log Events com Event View detalhado	✓
Diferenciais Técnicos	• Observabilidade orientada à aplicação com métricas de performance • Correlação entre rede, segurança e performance em uma única plataforma • Visão unificada de ambiente distribuído (filiais, data center, cloud) • Conformidade regulatória alinhada ao Marco Civil da Internet • Redução de MTTR com troubleshooting avançado e drill-down por fluxo • Business Intelligence integrado para análises avançadas e relatórios customizados • Posicionamento como plataforma de observabilidade além de segurança • Diminuição do TCO com gerenciamento centralizado de milhares de NGFWs • Maximização do ROI em ambientes multi-site de grande capilaridade	✓

Administração, HA e Integrações

Recursos	Itens	Blockbit GSM
Administração e Segurança	• Acesso simultâneo por múltiplos administradores com bloqueio de alterações • Perfis Read-Only e Read-Write por administrador • Autenticação via LDAP, AD, SAML e Radius com SSO e MFA/2FA • Certificados X509v3 e suporte a certificados revogados (LCR) • Identity Provider: Service Provider e Identity Provider (SAML) • Controle de acesso granular e Access Control • Audit Log com rastreamento completo e Audit View detalhado • Visualização e comparação de configurações com suporte de IA • Upgrade de firmware e patches via interface de gerenciamento com rollback • Login Disclaimer configurável na página de autenticação do GSM • Ambiente multi-tenant com communities • Custom Branding do GSM (logo, cores, favicon, background, page title)	✓
Alta Disponibilidade (HA)	• Cluster HA do GSM Manager: Primary + Secondary (standby) • Cluster HA de Loggers: Primary + Replica com IP Virtual • Failover automático com heartbeat configurável (intervalo em segundos) • Até 3 Peer IPs redundantes com Virtual MAC e Sync Interval • Sincronismo resiliente com validação de integridade antes da replicação • Reaplicação automática de deploys interrompidos após failover • Notificação por e-mail em eventos de failover e sincronismo • Ativação manual (Sync Now / Active Now) e automática (Auto Activation) • Cluster Status com Local/Peer State, Uptime, Connection e Sync Status	✓
CLI, API e Integrações	• CLI com +70 comandos: ping, traceroute, tcpdump, netstat, arping, telnet • CLI rede: set-network-interface/dns/gateway/hostname/timezone • CLI gerenciamento: reboot, shutdown, reset, passwd, rewizard, enable-root • CLI logger: logger-config, logger-enable, logger-key, logger-devices-add/list • CLI debug: debug-backup, debug-ha, debug-sync, debug-deployer, debug-rotation • CLI SNMP: enable-snmp, disable-snmp; CLI update: update-gsm, upgrade-blockbit • API RESTful com autenticação JWT (bearer token) na porta 3002 (JSON) • Endpoints: /auth/login, /api/appliances, /api/policies, /api/ips, /api/traffic • Filtros API: interval_type (hour/min/d/m/y), init_date/end_date, device_id • Alertas por e-mail (SMTP), SNMP e Syslog com integração com monitoramento externo e Geomap • VPN SSL e IPSec (client-to-site) com Blockbit Client para Windows	✓