



## BlockAPT Platform

---

Your automated, intelligent  
cyber defence solution

## Adding value across your business

BlockAPT protects your digital assets by unifying operational technologies against advanced persistent threats. We have deeply integrated our BlockAPT platform with leading edge solution providers so whether you are an SME or a Large Enterprise, you can benefit from cutting edge automation and intelligent response management. BlockAPT brings you a fully integrated solution through a single security management portal.



### Key features

- ✔ Deeply integrated APIs with leading network and security providers
- ✔ Automated migration/transfer between different solutions providers
- ✔ Import and export configuration
- ✔ Backup and restore schedules, on a daily, weekly, or monthly plan
- ✔ Threat detection including alert notifications
- ✔ Fully automated, non-intrusive, cloud based vulnerability scans 24/7 all year round

### Business benefits

- ✔ **90%+** reduction in routine tasks
- ✔ **80%** reduction - MTTD / MTTR
- ✔ **70%+** increase in operational efficiency and productivity
- ✔ **1** hour deployment - minimal disruption to business
- ✔ **2** hours – realised tangible ROI
- ✔ **95%** reduction on time, resource and costs for digital transformation projects (automated configuration migration)

#### Monitor

Our BlockAPT platform offers deep integration throughout multiple layers of security enabling a single pane of glass view across all your applications.

#### Manage

Integrated with leading vendors, you can benefit from having threat intelligence, vulnerability management, and incident response management all on one platform.

#### Automate

Single command & control of your assets with automated responses enables vulnerability scans, threat intrusion monitoring and modelling prevention – 24/7.

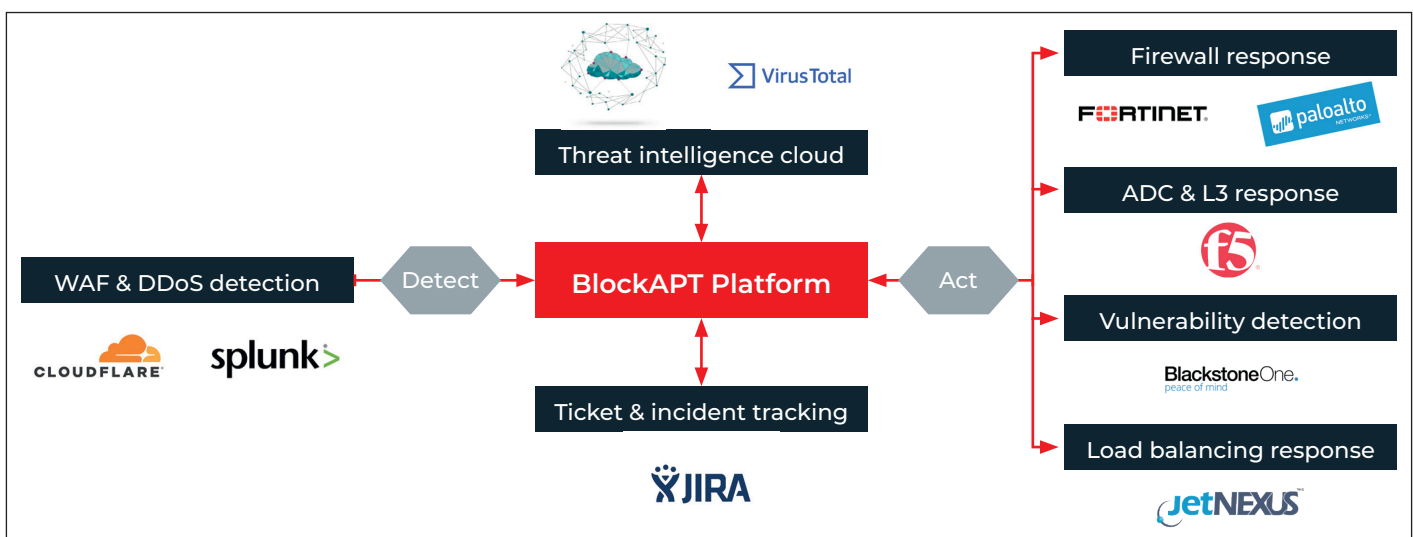
#### Respond

Incident responses can be integrated into your change control applications and communication processes to ensure compliance across your ecosystem.

# Our solutions

Whether you are an SME looking at centralised control with reduced costs through an affordable managed security service or a Large Enterprise looking to unify your existing technologies and disparate/legacy systems, BlockAPT can provide you with a range of core solutions.

<p><b>Automated Migration</b></p> <p>Shift between your digital assets in a more seamless and intelligent way. Take advantage of our automated migration reducing time and costs.</p>	<p><b>Threat Prevention</b></p> <p>Protect your websites, e-commerce sites, web portals, and business critical online applications against advanced targeted cyber attacks.</p>	<p><b>Vulnerability Scanning</b></p> <p>Automate threat vulnerability checks in a non-intrusive and seamless way with continuous scans that run 24/7 all year round.</p>	<p><b>Backup &amp; Restore</b></p> <p>Automatically backup your entire network and security infrastructure with the ability to restore configurations on demand to ensure business continuity – 24/7.</p>
---	---	--	---



### Audits and tests

- ✓ Vulnerability scanning
- ✓ Security compliance testing
- ✓ Security audits

### Risk analysis

- ✓ Security analytics
- ✓ Threat landscape
- ✓ Business impact

### Security architecture

- ✓ Reference architectures
- ✓ Technology selection
- ✓ Design principles

### Security reviews

- ✓ Applications & infrastructure visibility
- ✓ Security audit & reporting
- ✓ Holistic view

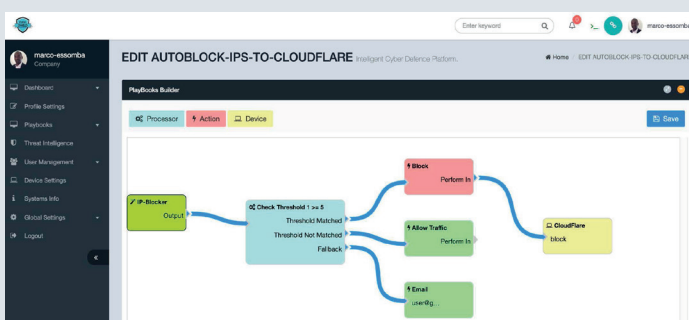
### Security control

- ✓ Risk mitigation
- ✓ Controls & processes
- ✓ Security policy formulation

### Implementation and support

- ✓ Technical delivery
- ✓ Bespoke training
- ✓ Cyber response


























## Automation – at your fingertips



Create automated playbooks – a drag and drop approach to support workflow processes.

- ✓ Reduce manual intervention of repeatable and predictable tasks - free up your resources.
- ✓ One playbook - multiple products integrated automatically providing a holistic view across the entire stack.
- ✓ Real time alerts - notifications automatically tied into your communication processes and escalation protocols.
- ✓ Advanced data analytics – develop a library of playbooks to protect your business 24/7.

## Integration – leading solutions providers

ADC & Load Balancing	
   	
Blockchain	Cyber Threat Intelligence
	
DDOS & Web App Security	Encryption & Endpoint Security
 	
Penetration Testing	Security Incidents Management
 	
Perimeter Security	
       	
Secure Remote Access	SIEM
 	 
Web & Email Security	
	

# Deep integration (push & pull)

## Remote device management

- ✔ SOAP & REST API
- ✔ Native plugins (SSH, SCP)

## High availability

- ✔ High Availability mode (Active – Standby)
- ✔ Redundancy with fast configuration restore

## Connectivity methods

- ✔ Push & pull commands via HTTPS/API
- ✔ TCP connect
- ✔ SSH connect

## Networking

- ✔ IPV4 & IPV6 support
- ✔ Single or multi interface configuration choice of interfaces (from 4x1GbE up to 4x10GbE or 8x1GbE)
- ✔ Unrestricted interfaces (virtual)
- ✔ High performance virtual network drives (virtual)

## Monitoring & alerting

- ✔ Selectable SSL certificate
- ✔ SNMP native support
- ✔ Controlled Command Line Interface (CLI)
- ✔ SMTP configurable email alerts

## Default security analytics

- ✔ Device CPU monitoring
- ✔ Device RAM monitoring
- ✔ Top attacking IPs
- ✔ Top cyber threats
- ✔ Top attacking IP sources
- ✔ Top attacking IP distribution

## Automated migration:

- ✔ Migrate/transfer from one solution provider to another in a few clicks
- ✔ Analyse a device configuration at source and destination before migration
- ✔ Test and verify migrated configuration plans
- ✔ Support for multiple network and security vendor APIs & plugins.

## Automated vulnerability scans (subscription required)

- ✔ Automated notifications and crowdsourced remediation solutions
- ✔ Innovative dashboards for access on smartphones, PCs and TVs
- ✔ Agile task management feeding remediation tasks to the BlockAPT platform

## Automated playbooks/workflows

- ✔ Pre-programmed playbooks for ease of use
- ✔ Customisable playbooks - simple drag & drop functionality
- ✔ Integrated into your existing change control processes
- ✔ Integrated into your existing email communications with an audit/tracking trail

## Audit & device transaction logs

- ✔ Remote Syslog server
- ✔ Local logging

## Backup & restore

- ✔ Automated device backups
- ✔ Seamless backup of your entire security infrastructure for disaster recovery and compliance

## Device security

- ✔ Secure connection to devices on cloud or on premise
- ✔ Adaptive SSL negotiation
- ✔ Local credential encryption

## Supported cloud infrastructures

- ✔ Amazon Web Services (AWS)
- ✔ Microsoft Azure
- ✔ Google

## SSL certificates management

- ✔ Manage all your SSL certificates across your entire security infrastructure

## Supported blockchains

- ✔ Stellar

## Technical specification

The BlockAPT platform can be deployed **in the cloud** (including AWS, Azure or Google Cloud) or **on-premise**.



Physical appliance tech specs	ICS-P1	ICS-P2	ICS-P3	ICS-P4
Chassis	1U half depth	1U full depth	1U full depth	1U full depth
CPU cores – Hyper threading – Threads – Processor base frequency – Max turbo frequency – Cache	4 Yes 8 3 GHz 3.50 GHz 15 MB SmartCache	6 Yes 12 3.40 GHz 3.70 GHz 20 MB SmartCache	8 Yes 16 3.20 GHz 3.60 GHz 25 MB SmartCache	12 Yes 24 3.00 GHz 3.50 GHz 30 MB SmartCache
Memory	8 GB	16 GB	32 GB	64 GB
Network interface	2 x 1 GbE	4 x 1 GbE Optional 2 x 10GbE	4 x 1 GbE & 2 x 10 GbE	4 x 1 GbE & 2 x 10 GbE
Storage	80 GB SSD	120 GB SSD	120 GB SSD	180 GB SSD
Power consumption	70W peak	148W peak	148W peak	148W peak
Power redundancy	No	Yes	Yes	Yes
Monitoring max throughput	3 Gbps	6 Gbps	10 Gbps	20 Gbps
Max secure connections to devices	Up to 1000 devices	Up to 2000 devices	Up to 4000 devices	From 8000 devices*
SSL transactions per second*	Up to 2500 tps	Up to 5000 tps	5000+ tps	5000+ tps*

\*Not limited by licence