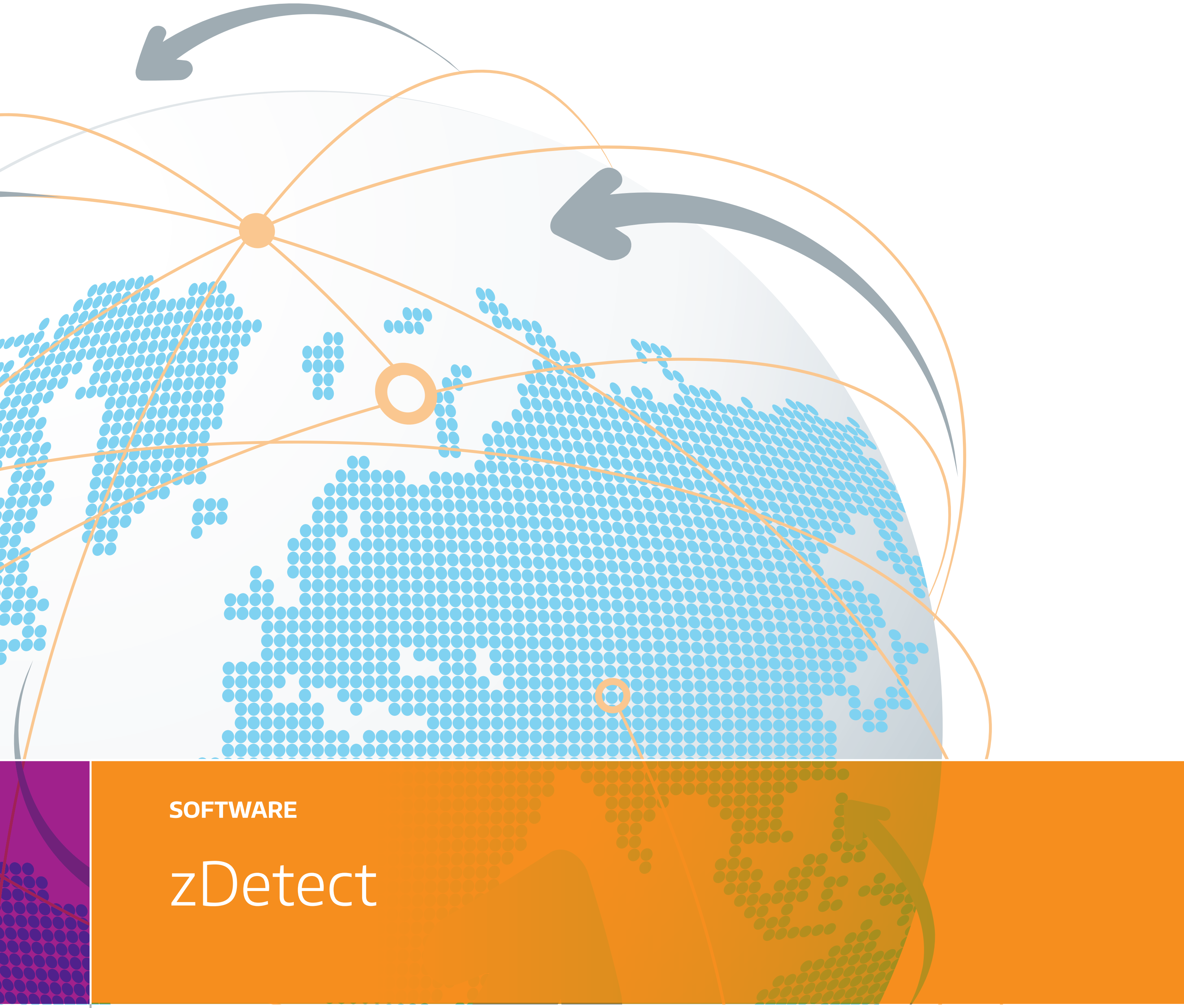
RSM PARTNERS

MAINFRAME



SOFTWARE

zDetect

Real-time security threat detection
and alerts for your mainframe systems

Threat detection and intelligent security analysis made easy

zDetect is a powerful z/OS mainframe security monitoring tool, specifically designed to detect actual and potential security issues in real time.

Making a difference

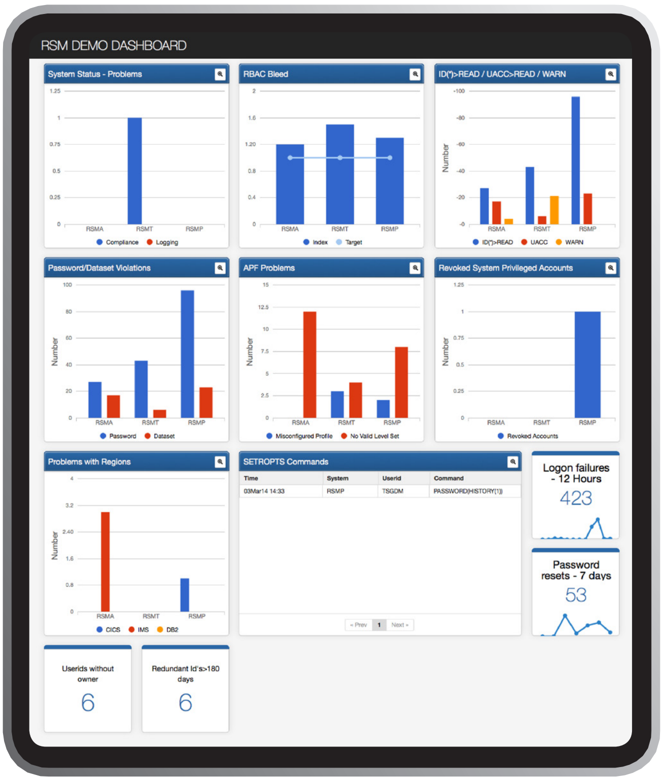
Collecting data is the easy part: the real value lies in transforming your data into insight. Unlike other security monitors, **zDetect** doesn't simply collect information to send to a SIEM. It uses sophisticated internal security algorithms for intelligent analysis, detecting suspicious events that can threaten your organisation's security posture. These events are visualised through an easy-to-use yet comprehensive mainframe security dashboard.

- Better protect your organisation, systems and confidential data
- Identify security threats as soon as they occur
- Reduce the risk of security breaches occurring
- Runs in the environment it's monitoring, minimising any risk of data/information loss
- Architected to consume minimal system resources: keeps system overheads to a minimum
- Complements the IBM zSecure security suite

How zDetect works

- Collects data in real time from the z/OS environment, loads it into its repository and continually processes the information, identifying threats using intelligent algorithms
- Runs on z/OS, so the software is as close as possible to the environment being monitored
- Data comes from various sources including SMF data, logs and zDetect specific processes
- Threats are displayed on a dashboard interface via a standard web browser; events can also be sent to your organisation's SIEM

zDetect works closely with the IBM zSecure product suite so that security engineering processes can be co-ordinated across the organisation. Future releases will work with other vendor security suites.



RSM DEMO DASHBOARD

SETROPTS Commands

Time	System	Userid	Command
03Mar14 14:33	RSMP	TSGDM	PASSWORD(HISTORY(1))

Logon failures - 12 Hours
423

Password resets - 7 days
53

Userids without owner
6

Redundant Id's>180 days
6

Key features

- Real-time threat detection
- Intelligent security analysis
- Drill-down capability for detailed threat analysis
- Dashboard for security teams to see threats and risks in real time
- Interfaces to SIEMs
- Identifies RACF threats and vulnerabilities including:
  - Poorly defined user controls
  - Poorly defined resource controls
  - Privilege elevation
  - Continual log-in failures
- Identifies RACF weaknesses including
  - Missing or weakly defined classes
  -Poorly defined sensitive resource controls
- Identifies z/OS threats and vulnerabilities to:
  - Sensitive resources
  - Sensitive commands
  - System console
- Identifies if known system vulnerabilities to z/OS are exploitable
- Identifies z/OS subsystem threats and vulnerabilities
- Provides detailed reporting capabilities

Why RSM?

We are a unique provider of mainframe expertise, software and services - 100% focused on the System z marketplace. Working for many world-leading companies – spanning financial, retail, utility, government and service organisations – no other partner can offer you the same mix of z knowledge, hands-on experience, reliability, flexibility and agility. We are proven to add value.

In 2016 RSM Partners received Ready for IBM Security Intelligence Validation as a leader in z Systems Security Consulting.

Business Partner IBM

Business Partner IBM
Ready for
Security Intelligence

zDetect specification

Platforms Supported

- zDetect runs on IBM z/OS Mainframe only
- Currently supports only RACF managed environments - not ACF/2 or Top Secret

Technical Requirements

PC/Mac supporting web browser IE, Firefox, Chrome, Safari, etc.

Installation & Maintenance

Necessary maintenance is SMP/e packaged and delivered as either an upgrade or PTF.

Licensing

By annual rental fee based on number of LPARs monitored. Licence fees payable in advance and are inclusive of maintenance and support.

Manuals

The software is supplied with Installation, Operation and User Manuals.

To find out more about these and other RSM Partners services, call **+44 (0) 1527 837767** or visit **www.rsmpartners.com**

RSM PARTNERS
z MAINFRAME

T +44 (0) 1527 837767
E info@rsmpartners.com
www.rsmpartners.com

The Courtyard, Buntsford Dr, Stoke Pound, Bromsgrove, B60 3DJ, UK