



# Verisys<sup>®</sup>

**File Integrity Monitoring System**

## Ionx Verisys<sup>®</sup> Console and Agents

File Integrity Monitoring System

Overview

<http://www.ionx.co.uk>



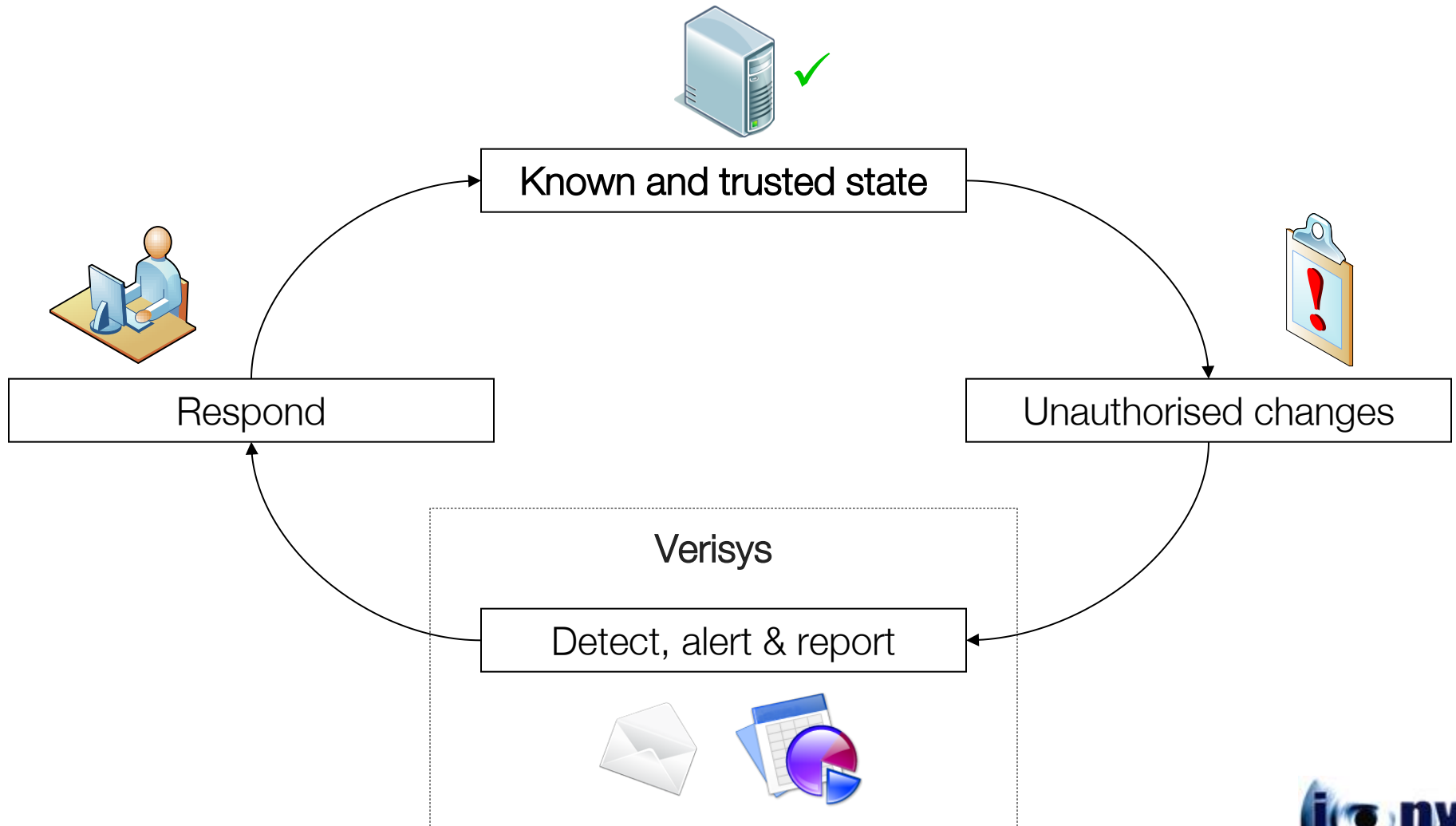
# What is Verisys?

- File integrity monitoring software
  - Detects unauthorised changes to files and Windows registry objects
  - Allows you to maintain integrity of data, ensuring your systems are in a known and trusted state
  - Sends alerts when discrepancies are detected, allowing a rapid response
  - Includes reporting tools
  - Agents available for Windows and Linux systems

# Main Usage Scenarios

- Enhance security
  - Good business practice as part of a comprehensive data security policy
  - Detect unauthorised changes
  - Allow rapid response
- PCI DSS (Payment Card Industry Data Security Standard) Compliance
  - Use of file integrity monitoring software is mandated by the PCI DSS to satisfy requirement 10.5.5 and 11.5
- SOX (Sarbanes-Oxley) Compliance
  - Must be able to demonstrate that your systems remain in a known and trusted state
- Change auditing
  - Provide an audit trail of what was changed, and when
  - Detect changes made outside of formal change/maintenance windows

# How it Works



# How it Works

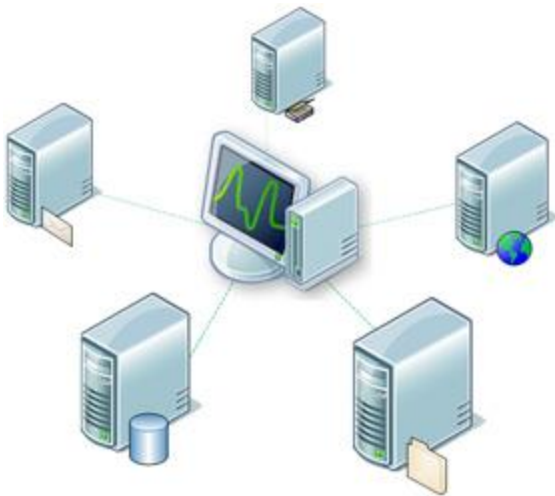
- Takes baseline snapshot of current system state
- Periodically compares current system state to stored baseline and detects any changes
- Checks a number of properties, as well as performing a complex cryptographic hashing algorithm on the actual data
  - Object name
  - Creation time
  - Last modified time
  - Last accessed time
  - Index node
  - Size
  - Flags
  - CRC-32
  - SHA-256 hash
  - Symlink target
  - Owner
  - Primary group
  - Access permissions
  - Audit rules
  - Extended attributes
- If files are altered in any way, Verisys will detect it

# Key Features

- Detects unauthorised changes
- Meets PCI DSS requirements 10.5.5 & 11.5
- Centralised administration
- Schedule automated integrity checks
- Wide range of alerting options
- Comprehensive reporting tools
- Templates for common system configurations

# Centralised Administration

- Manage many file integrity monitoring Agents from a single, central location
- Simplifies management of large or distributed deployments
- Easy to use GUI



The screenshot shows the Verisys Console GUI. The main window displays a table of agents with columns for Display Name, Host, Port, Ruleset, Job, and Status. The table lists various server types such as Application Servers, Email Servers, File Servers, MSSQL Database Servers, Oracle Database Servers, Payment Processing Servers, Print Servers, Web Servers, and File Servers, all with their respective hostnames, ports, rulesets, and job names. The status for all listed agents is 'OK'.

Display Name	Host	Port	Ruleset	Job	Status
Application Server A01	asa01.ionx.co.uk	3313	Windows 2008 Application Servers	Daily Integrity Check	OK
Application Server A02	asa02.ionx.co.uk	3313	Windows 2008 Application Servers	Daily Integrity Check	OK
Application Server A03	asa03.ionx.co.uk	3313	Windows 2008 Application Servers	Daily Integrity Check	OK
Email Server A01	esa01.ionx.co.uk	3313	Windows 2003 Email Servers	Daily Integrity Check	OK
Email Server A02	esa02.ionx.co.uk	3313	Windows 2003 Email Servers	Daily Integrity Check	OK
Email Server A03	esa03.ionx.co.uk	3313	Windows 2003 Email Servers	Daily Integrity Check	OK
File Server A01	fsa01.ionx.co.uk	3313	Windows 2008 File Servers	Daily Integrity Check	OK
File Server A02	fsa02.ionx.co.uk	3313	Windows 2008 File Servers	Daily Integrity Check	OK
File Server A03	fsa03.ionx.co.uk	3313	Windows 2008 File Servers	Daily Integrity Check	OK
File Server A04	fsa04.ionx.co.uk	3313	Windows 2008 File Servers	Daily Integrity Check	OK
File Server A05	fsa05.ionx.co.uk	3313	Windows 2008 File Servers	Daily Integrity Check	OK
MSSQL Database Server A01	dba01.ionx.co.uk	3313	Windows 2003 MSSQL Servers	Daily Integrity Check	OK
MSSQL Database Server A02	dba02.ionx.co.uk	3313	Windows 2003 MSSQL Servers	Daily Integrity Check	OK
Oracle Database Server A03	dba03.ionx.co.uk	3313	Windows 2003 Oracle Servers	Daily Integrity Check	OK
Oracle Database Server A04	dba04.ionx.co.uk	3313	Windows 2003 Oracle Servers	Daily Integrity Check	OK
Payment Processing Server A01	ppa01.ionx.co.uk	3313	Windows 2008 E-Commerce Servers	Hourly Integrity Check	OK
Print Server A01	psa01.ionx.co.uk	3313	Windows 2008 Print Servers	Daily Integrity Check	OK
Print Server A02	psa02.ionx.co.uk	3313	Windows 2008 Print Servers	Daily Integrity Check	OK
Web Server A01	wsa01.ionx.co.uk	3313	Windows 2008 Web Servers	Daily Integrity Check	OK
Web Server A02	wsa02.ionx.co.uk	3313	Windows 2008 Web Servers	Daily Integrity Check	OK
Web Server B01	wsb01.ionx.co.uk	3113	Windows 2008 Web Servers	Daily Integrity Check	OK
Web Server B02	wsb02.ionx.co.uk	3313	Windows 2008 Web Servers	Daily Integrity Check	OK

# Automated Alerting

- Send email
- Windows event log
- Syslog
- Save discrepancy report
- Execute any command

