Data Classification meets Security Analytics

Enhanced monitoring and protection of sensitive data assets

Benefits

Security monitoring focussed on data accesses to detect abuse

Increased protection by correlating Data Classification metadata and security events to reduce losses

Reduced risk with rapid investigation and recovery from attack

Efficient operations with unified views of data, events and sources

The importance of data protection

Data protection is becoming ever more important as public expectations of the secure collection and use of information increase.

Integration of Boldon James and Huntsman® Security technologies enables the proactive classification of data to protect it from access or loss and to detect abuse throughout the lifecycle.

Boldon James Classifier applies clear classification to data as it is created or updated. This combines with Huntsman's® ability to monitor and identify anomalous behaviour of users, devices and attacks from outside or inside the enterprise.

The outcome is rapid detection of attack and misuse of data, followed by immediate investigation and resolution.

How the integration works

Boldon James Classifier is a data classification solution that extends the capabilities of productivity tools, such as Microsoft Office, and other applications to allow users to apply relevant classification metadata and visual protection to documents, messages and data.

Huntsman® uses this source of rich intelligence on data sensitivity to automatically correlate and analyse access, use and transfers in conjunction with other enterprise security and event sources such as behavioural data from networks, security devices, applications, databases and 3rd party threat intelligence.

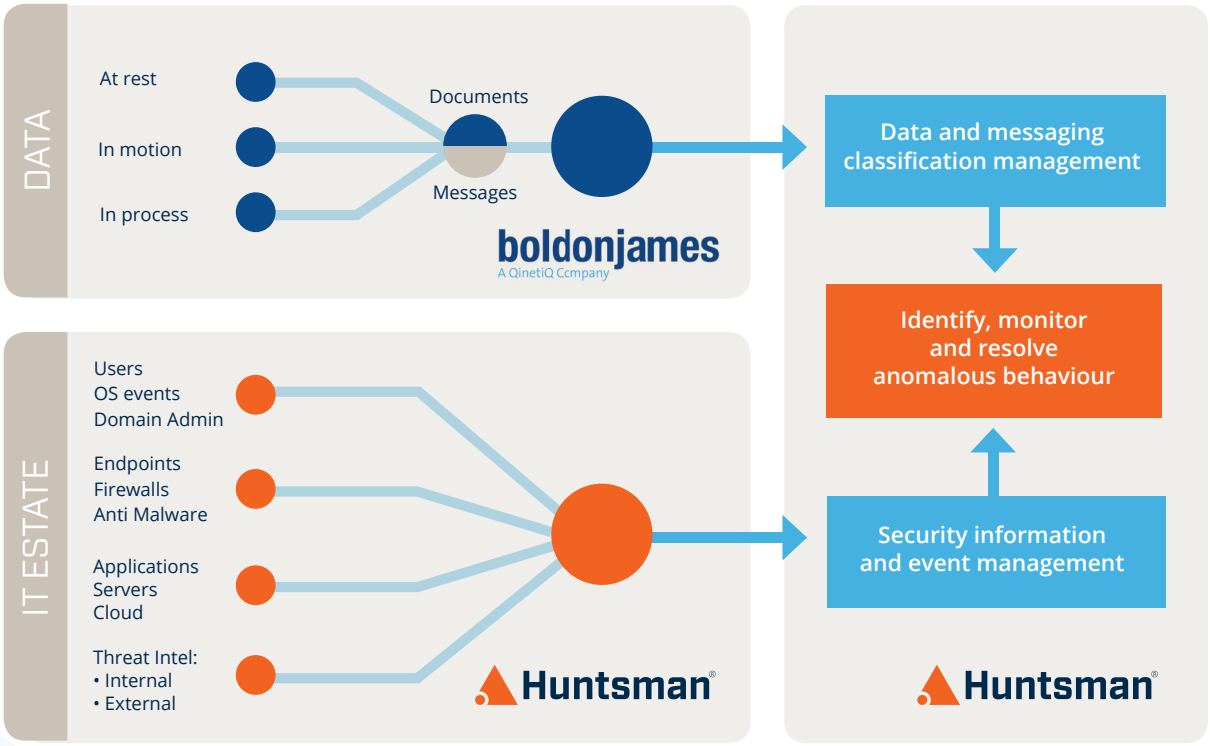
When an attack or misuse is detected the response can include prompting the end user, alerting security personnel or automating the containment of accounts, targeted devices and malicious processes.

This unique combination provides comprehensive analysis and protection to reduce data loss and thwart attacks.

boldonjames
A QinetiQ Company

Huntsman®
Defence-Grade Cyber Security

Enabling proactive protection of sensitive data and prevention of attacks



USE CASE: An unexpected large scale change in data classifications

Activity: Data classification events are correlated with user and device behaviour to determine whether the de-classification is authorised and normal for that user considering factors such as time, geographic location and business role.

Outcome: The user behaving unusually with sensitive data is detected and Huntsman® automatically instructs the OS to suspend/disable their account, access right or relevant network devices until investigations are complete.

Why: Personnel can be subverted or their have their credentials stolen. Having the ability to automatically detect irregular behaviours "at scale" and take action to protect enterprise data is critical.

USE CASE: Intelligence is received regarding malware designed to defeat classification controls and steal personal data

Activity: Workstations and users that access sensitive data are added to a Huntsman® watch list and endpoints are routinely examined to determine malware infection. Boldon James classification metadata is correlated with user and workstation authentication events to determine unauthorised data modifications.

Outcome: Any potential compromises are detected and presented to the security team for automatic or manual remote disabling of user accounts or quarantining of infected workstations to prevent the spread of malware and safeguard data.

Why: Malware statistically remains the biggest challenge to cyber security. Malware that is designed to steal or encrypt enterprise data must be prevented.

USE CASE: A user de-classifies Personally Identifiable Information (PII) to circumvent controls and export data to a USB stick

Activity: Boldon James provides classification metadata that Huntsman® correlates with file system "read" and "write" events and the insertion of USB devices to endpoints. This will identify malicious users by correlating classification changes with data export events and identification of anomalous behaviours, even over longer time periods and with low activity volumes.

Outcome: Identified malicious users can be added to a security watch list or have their account or workstation automatically quarantined to enable compliance, security or anti-fraud personnel to be automatically informed of relevant activity by email or alert.

Why: Insiders already have access privileges to compromise data deliberately, accidentally or if their authentication credentials are stolen.