Intelligent ID

Federal Information Security and Intelligent ID

It is no surprise that with the continuing advancements in data mobility, increasing demands of regulatory compliance, and sharing amongst the global community, that securing our nation's sensitive information becomes more difficult each day. It is with this mobile and ever-changing environment in mind that Intelligent ID was created.

Intelligent ID Overview

Intelligent ID is a comprehensive Endpoint Monitoring and Protection (EMaP) tool that reduces an organization's employee liability landscape by protecting its most valuable data. Intelligent ID accomplishes this by continuously monitoring endpoint and user behavior for policy violations, compliance infractions, and anomalous activity or file usage that could be signs of an impending breach. Intelligent ID's four modules: Data Loss Prevention, Identity Activity, Productivity Monitoring, and Infrastructure Monitoring, collect and analyze data to provide instant insight and alerts when an incident arises.

Why Endpoint Monitoring?

When dealing with sensitive data loss, waiting for an incident to be detected crossing the network may mean it's already too late. Other incidents will, intentionally or unintentionally, bypass all network monitoring appliances. Residing as a lightweight client on the endpoint, Intelligent ID can analyze behaviors as they take place in real time, view data as it is created, and display productivity data in accurate detail, all to help identify potential incidents before a breach occurs. Should a potential incident be detected, incident response can be notified immediately. By utilizing Intelligent ID's sophisticated investigation tools and replay capabilities, the incident can quickly be quarantined as it is happening, preventing the breach from occurring.

Key Benefits:

- Provides holistic continuous monitoring solution as required by FISMA 2.0 and NIST's RMF
- Helps to reduce your employee liability landscape
- Log-free analysis saves time and overhead
- Locates insecure sensitive data even when it has been reformatted or changed
- Provides real time forensics of endpoint activity
- Policies remain active regardless of the physical location or connectivity of the endpoint
- Highly customizable policy configuration preserve personal privacies while upholding strict security standards

Intelligent ID

Next Level of Data Loss Prevention

Intelligent ID's DLP tools not only provide comprehensive coverage for every channel of egress from an endpoint, but also track activities taking place on the endpoint itself that could be putting your data at risk. Intelligent ID can scan outgoing or incoming emails and their attachments, emails saved to a draft folder for later retrieval, files being moved to cloud storage or external media, and files printed, even if the printer is not on the network. We can even make you aware when suspicious behaviors are observed such as a user taking a screen capture of a sensitive data, reformatting the image and attempting to email it to a personal account.

Tracking of Sensitive Documents

Intelligent ID gives you detailed knowledge as to how many copies of a sensitive document exist, where they reside, and how they are being accessed and used. By utilizing our Sensitive Data Crawler, we allow you to identify every endpoint and file share where a document exists, even if the document has been renamed, reformatted, or if only a portion of the document exists in that location. In addition, alerts can be sent when a document is copied, duplicated, renamed, or moved from its secure location regardless of where or how it travels or if it ever touches the network layer.

Instant, Log-Free Compliance Audit

With our simple compliance mapping process, Intelligent ID can provide a real-time report on the status of your compliance initiatives including alerts detailing when, where, how, and why a violation occurred. View gaps in compliance by individual endpoint, group, department or organization as a whole to accurately target training and improve secure workflow.

Security of Off-site and Transient Employees

Intelligent ID makes it as easy to protect off-site workers, field employees, and travelling laptops as it is to protect those right in front of you. Because Intelligent ID runs on the endpoint, our monitoring and protection policies continue regardless of where the endpoint is located or whether it is currently online. In addition, our one-of-kind Productivity Analysis tools continuously collects and reports endpoint, application, and internet usage statistics to ensure time and resources are being used effectively, budgets maintained, and only secure applications run.

We See What the Network Misses

- Documents removed from fixed disk to removable media
- Documents encrypted/ unencrypted at the endpoint
- Unauthorized processes running
- Screen captures of sensitive databases or web applications
- Printing to local devices
- Altering, reformatting, or removing portions of sensitive documents
- Activity taking place off-network or in the field

For More Information:

Jim Mazotas
jim.mazotas@onguardsystems.com
614.325.0551

1275 Kinnear Road
Columbus, OH 43212

www.IntelligentID.com