Autonomy ICE
Compliance and Risk Management

As corporations promote information access and collaboration, the broad availability of this information lends an unprecedented level of risk to both enterprise and client data. The increasingly diverse set of channel vehicles being used for customer and client communication—websites, blogs, email, chat, social networking sites, phone, CRM applications, and collaboration tools—only increase the risk of insider theft, fraud, and data loss by providing easier access to highly sensitive information and generating data that resides outside of corporate compliance and governance strategies.

To keep data secure and compliant, Autonomy delivers the industry’s first complete realtime policy-based solution for information security and compliance. Autonomy Interaction Control Element (ICE) simplifies compliance with industry regulations, data privacy laws, and litigation requirements by understanding the meaning of employee interactions with customers, websites, or desktop applications and enabling organizations to effectively monitor and control sensitive corporate and client data. With Autonomy ICE, businesses can ensure customers, clients, and regulatory and legal agencies that they are operating ethically and responsibly.

Data Privacy
Data privacy is an already immense issue that continues to grow as individuals increasingly exchange personal and financial information with companies through various channels. Information collected and held within the enterprise is constantly at risk of being compromised, and watchdogs continue to report increases in insider theft and data leaks.

Autonomy ICE monitors server, desktop, and system events and forms a conceptual understanding of employee activity, whether they are speaking with a customer or accessing a helpdesk application. A combination of policy-based triggers and intelligent Meaning Based Computing technology allows ICE to identify any fraudulent or suspicious activities taking place within the organization such as:

- Copying of files onto mobile media (CDs or flash drives)
- Excessive time on screens containing personal data
- Transmission of files or information to addresses beyond the firewall
- Discussion of a customer’s personal information over the phone without the customer present
- Accessing restricted or unauthorized applications
- Transferring of information from one application to another (Copy/Paste)

The ability to interpret the meaning of all interactions also enables Autonomy ICE to recognize potential data leaks that may not have been defined by the end-user. Autonomy ICE is completely application independent, allowing the solution to trigger alerts from any application, including CRM and helpdesk suites, email and instant messaging systems, and browser-based applications.

Automatic Alerts
Autonomy ICE can be configured to automatically alert business managers, IT personnel, or compliance officers to potential data breaches or violations within the defined parameters. It can also

Highlights
- Minimizes information theft, fraud, and data risk by proactively managing all interactions, including voice, desktop, email, IM, and web
- Delivers real-time monitoring of desktop, server, and online events based on user-defined policies and built in Meaning Based Computing technology
- Identifies and alerts personnel to potential compliance violations or data leaks based on employee interactions
- Masks and mutes sensitive data from interactions for risk management or compliance with Payment Card Industry and HIPAA regulations
- Records and archives interactions containing suspicious or potentially fraudulent activity
- Applies information governance policies, including retention and disposition schedules or legal holds, to interactions in real time
- Seamlessly integrates with Autonomy Information Governance and eDiscovery solutions to offer the industry’s most comprehensive information risk management platform
- Application independent technology works with all recording systems, email clients, IT systems, and browser-based and software applications

“285 million data records were compromised in 2008 alone.”
—Verizon Business

“Each breached record cost a company between $90 and $350.”
—informationweek.com
send alerts on undefined activities by forming an understanding of what constitutes suspicious activity and identifying those characteristics in future interactions.

**Action Archiving**

Business and compliance managers may want Autonomy ICE to record suspicious interactions so that they can be reviewed in the event of an audit or investigation. When an event occurs, Autonomy ICE can trigger the recording system to capture a portion of the employee's voice or screen activity for a set period of time (or until the closing trigger happens) and save the recording to a server or archive. Autonomy ICE can additionally capture and archive any related metadata, CTI information, or structured data entered into a website or application.

**Realtime Data Masking and Muting**

To further secure sensitive customer data and enforce regulations such as the Payment Card Industry (PCI) Data Security Standards or Health Insurance Portability and Accountability Act (HIPAA), Autonomy ICE works in realtime to mask or mute out sensitive materials from audio and desktop applications that are recorded and stored. Administrators can define specific events, screens, fields, actions, or key words or numbers that “trigger” the masking or muting feature to ensure that all captured customer data within those parameters is redacted. These events can include the starting or stopping of a recording, an email system being accessed, or agent typing into a specific field in a desktop application, among others.

Autonomy ICE intelligently identifies which parts of which interactions require masking or muting for enterprise risk management or compliance, which strictly limit access to data such as credit card numbers and medical information. Autonomy ICE automatically redacts appropriate portions of the interaction that contains sensitive data. The masking and muting functionality is linked to employees’ permission settings, allowing the data to only be accessed by appropriately authorized individuals.

**Information Governance**

Autonomy ICE delivers an unprecedented level of governance to web interactions, desktop activity, email, instant messages, and audio recordings to ensure sensitive data is managed within corporate regulatory and corporate policies. By synchronizing desktop and web usage with live interactions, Autonomy ICE can identify interactions that are subject to compliance or corporate criteria and apply defined enterprise information governance policies, such as retention schedules, disposition management, and legal holds. This solution combines with Autonomy eDiscovery solutions to provide a single meaning-based platform for information access.

**Enterprise Architecture**

Autonomy ICE operates via a centralized policy server, with customization and definition available directly from any browser-based interface. Autonomy ICE is built on Autonomy’s Intelligent Data Operating Layer (IDOL) to offer businesses unique Meaning Based Computing functionality that understands the meaning of all enterprise information, no matter its language or format. With IDOL, businesses have access to a single enterprise platform for compliance, risk management, information governance, and eDiscovery. Autonomy ICE works with any enterprise information system, enabling policy definition, monitoring, and recording across all servers and email, web, and desktop applications.

**About Autonomy**

Autonomy Corporation plc (LSE: AU. or AU.L), a global leader in infrastructure software for the enterprise, spearheads the Meaning Based Computing movement. It was recently ranked by IDC as the clear leader in enterprise search revenues, with market share nearly double that of its nearest competitor. Autonomy’s technology allows computers to harness the full richness of human information, forming a conceptual and contextual understanding of any piece of electronic data, including unstructured information, such as text, email, web pages, voice, or video. Autonomy's software powers the full spectrum of mission-critical enterprise applications including pan-enterprise search, customer interaction solutions, information governance, end-to-end eDiscovery, records management, archiving, business process management, web content management, web optimization, rich media management and video and audio analysis.

Autonomy’s customer base is comprised of more than 20,000 global companies, law firms and federal agencies including: ADL, BAE Systems, BBC, Bloomberg, Boeing, Citigroup, Coca Cola, Daimler AG, Deutsche Bank, DLA Piper, Ericsson, FedEx, Ford, GlaxoSmithKline, Lloyds TSB, NASA, Nestlé, the New York Stock Exchange, Reuters, Shell, Tesco, T-Mobile, the U.S. Department of Energy, the U.S. Department of Homeland Security and the U.S. Securities and Exchange Commission. More than 400 companies OEM Autonomy technology, including Symantec, Citrix, HP, Novell, Oracle, Sybase and TIBCO. The company has offices worldwide. Please visit www.autonomy.com to find out more.