VERDASYS®

# STRATEGIES FOR PROTECTING INTELLECTUAL PROPERTY

WHITE PAPER

## Introduction

A company's Intellectual Property (IP) often represents both a significant portion of its assets, and a critical component of its market differentiation. Digitized IP comes in many different forms and can include "structured" types — like spreadsheets, documents, emails — that have content recognizable by scanning technology using keywords and regular expressions, or "unstructured" types — like vector drawings, images, formulae or software code — whose content is more difficult to predict with typical automated approaches. Regardless of how it is identified, the challenge for a company is how to protect IP without limiting its ability to create value.

The competitive advantages businesses gain by increasing the acceptable uses of IP manifests itself through more efficient decision support, execution, and innovation. For example, a chemical company can accelerate the ROI of its offshoring strategy by assuring the security and integrity of proprietary plant and machinery designs it is required to share with foreign partners and government agencies. Or when a fabless mobile chip designer can confirm its highly sensitive designs are contained between third party foundries and cell phone manufacturers, it can deliver more creative products in less time. In highly collaborative environments, putting your IP to work without undue risk clearly increases its value.

The benefits of collaboration are well understood by successful companies in all industries. Whether adopting distributed business processes or outsourcing critical deliverables, the ability to seamlessly integrate their collaborative processes is the key to business efficiency, agility, and market differentiation. The irony, of course, is the more IP is shared to create value, the more likely it is to be misused by a malicious insider. Securing collaborations requires enforcing policies that allow privileged users to productively share IP while ensuring it cannot be compromised.

## The Challenge

Protecting IP often forces companies to make risky and potentially costly trade-offs when enforcing acceptable use that either make collaboration safer or more productive — but usually not both. Obviously, too little oversight leaves IP exposed, and too much security can decrease employee productivity. Ironically, too many security gates in a business process can actually *increase* risks when well-meaning users bypass burdensome controls for the sake of performance. For example, an employee on a tight project deadline may send large sensitive files to a partner through their Gmail account because their corporate mail system limits attachment size as a security control — and although a procedure may be defined to request an exception to this policy, the time delay could justify the user to intentionally violate acceptable use policies. To avoid unproductive security measures (and decrease Help Desk costs), many companies with the inability to apply intelligent policy enforcement end up loosening usage restrictions and increasing the risk to IP in return for a better user experience.

Protecting IP includes two unique challenges beyond what is required for other types of sensitive data:

1. Privileged users with legitimate access to intellectual property are among the most trusted employees in an organization. IT security technologies such as disk encryption, firewalls, intrusion prevention, and access management systems are designed primarily to defend against unauthorized users, but are by definition ineffective against those with proper access credentials. But clearly, privileged users must be afforded the freedom to be productive within creative and collaborative environments; enforcing undue usage restrictions risks stifling the competitive advantages those employees bring to the business.
2. IP comes in multiple forms, file types, and data structures. It is therefore very difficult to automatically detect IP in unknown or irregular formats using content scanning and discovery tools reliant upon keywords or patterns (What is the pattern of a restricted formula?). Unlike predictable content like personal identifiable information (PII), the unstructured nature of most IP makes it much easier for potential thieves to evade standard data security technologies.

The challenge of protecting IP with network and perimeter-based security solutions is a legitimate concern for organizations known for innovation and secrecy. For example, over the last several years data thefts at LG, Motorola, and the Department of Defense have exposed a pattern of vulnerability within common data security models: despite large investments in firewalls, content monitoring systems, anti-malware, or identity and access control platforms, none of these solutions were able to protect IP compromise from malicious insider.

## The Limits of Data Loss Prevention Technology for IP Protection

Many companies have deployed network-based data loss prevention (DLP) solutions in the hope that they can offer some level of protection against IP theft. Although these solutions do offer some value in blocking structured data from leaving via corporate email, they are unable to consistently protect most types of IP for a variety of reasons including:

- DLP solutions limited to structured content scanning cannot recognize unstructured IP types saved in a non-standard format (e.g. CAD drawing saved as an MP3), or embedded within another file (e.g. image of text pasted within a text file).
- Once IP is encrypted in place or uploaded via secure tunnel (e.g. social media account), network sensors tools are blind to its content.
- DLP appliances cannot scale for networks with large amounts of IP due to computationally intensive and inaccurate data recognition models that rely on hashing, pattern recognition, or machine learning approaches.
- Most data compromises occur when a privileged user offloads it from their local system (e.g. to USB drives, Local Printers, or CD burns) to circumvent detection by network DLP appliances, or defeat endpoint DLP solutions that rely on a network component to enforce data policies.

- Without risk-based control options, network DLP either blocks or allows all data traffic, which makes productive policy enforcement impractical due to the likely disruption of legitimate business processes.

The most scalable and cost-effective approach to mitigate the liability of IP compromise requires a data-centric security model that enforces policy with risk-appropriate controls equally whether sensitive data is accessed online, offline, or in a virtual environment. The solution must also identify all structured or unstructured IP content, regardless how it may be altered or hidden to avoid detection, and ensure privileged users may only use data in authorized ways.

## Intellectual Property Protection by Digital Guardian

The Digital Guardian technology platform was designed specifically to protect IP from misuse by privileged users. Unlike typical DLP tools which can only scan network traffic to see and block structured files with easily definable text, Digital Guardian enables the safe and productive sharing of any IP type – even without scan-able content – while still protecting it from abuse by privileged users.

Digital Guardian assures the secure collaboration of IP, including files embedded within other files or obfuscated as unreadable formats, by permanently tagging and enforcing policy for virtually any sensitive content, including from sources where unstructured IP likely originates:

- CAD models
- Drawing files
- Image files
- Data files
- Document files
- Source code
- Equations
- Application databases

Verdasys Digital Guardian is a scalable, comprehensive, and proven enterprise information protection technology platform for protecting and tracking the use of critical IP by privileged users within network sessions, endpoints, and servers. It autonomously monitors and enforces data-level policies online, offline, and within virtual environments regardless of user privileges, and is designed especially for large enterprise deployments across highly-distributed and secure business processes over private or public infrastructure. Digital Guardian supports localization for most languages (including Sanskrit and double-byte characters), and also provides anonymous reporting to comply with works council laws around the world.

Digital Guardian delivers policy-based IP identification, classification, monitoring, and security controls across the data lifecycle using a combination of root-level endpoint agents and session-aware network agents. Digital Guardian endpoint agents forensically log all system, user, application, and data activities out of the box; its network agents deconstruct each layer of a network session across all ports and protocols to monitor and enforce policies at line speeds. Capable of classifying data using context, content, or user-determined rules, Digital Guardian enforces risk-aware file access and usage policies using a variety of identity-based controls, including integrated media, file, network, and email encryption. Most importantly for IP protection use cases, the Digital Guardian system is hardened and tamper resistant to prevent disablement by privileged administrators and targeted cyber attackers.

Digital Guardian endpoint and network agents are managed by the Digital Guardian Management Console (DGMC), a highly-scalable Web-based reporting and management server. The DGMC manages all aspects of the Digital Guardian platform: it captures, aggregates, and stores forensic event logs; drives the data classification framework; and creates and distributes policy definitions to all Digital Guardian agents for endpoint and network-based enforcement. The DGMC also defines and triggers security alerts, and includes a wizard-based rules engine for executive, forensic, and custom report creation. With its secure architecture and forensic visibility into all endpoint and network data activities, Digital Guardian continuously monitors and regulates how privileged users interact with IP, including "super" users like system administrators and IT security managers.

Digital Guardian is the only data security solution proven at large enterprise scale (>100,000 users) that allows companies to:

- Securely log where and how sensitive data is being accessed and used by privileged users internally, offline, or on virtual sessions.
- Securely manage the entire business process by combining usage rules for system, application, and network activity with data classification and evidentiary-quality event forensics.
- Enforce risk-appropriate responses to potentially dangerous activity using warnings, justifications, and blocking.
- Deploy identity-based file access controls, including integrated removable media, file, network, and email encryption.
- Increase the freedom by which IP can be productively used, while at the same time ensuring its usage is governed, controlled, and audited regardless of user access privileges.

# Digital Guardian IP Protection Differentiators

Digital Guardian offers unique capabilities that provide scalable and cost-effective IP protection not available from other DLP or IT security solutions. These include:

**User, Content & Context Based Awareness and Classification**
Most IP is stored in a managed repository like versioning control or content management systems which often includes native data classification capabilities. Digital Guardian's automated classification model can use multiple context-based parameters to automatically classify sensitive IP sourced from a secure application or system, regardless of its actual content, or by requiring users to manually apply the application's own classification framework. Either way, IP classified by Digital Guardian will be permanently recognized by its Agents at the point of use, which autonomously enforce policy based on the file's sensitivity and the user's right to complete a given transaction. Digital Guardian classification meta-tags are permanent, tamper-resistant, and inheritable, meaning the classification cannot be removed by an end user (unless authorized), and if any portion of the classified document is transferred to a new file, it inherits the original file's classification tag.

**Visibility, Monitoring and Control at the Point of Use**
As privileged users interact with IP, Digital Guardian forensically records and manages their use of it. If the user attempts an activity in violation of policy, agents automatically implement a risk-appropriate security control before the transaction occurs. Digital Guardian controls are flexible to enable privileged users to make informed decisions whether to complete an activity, include using real time warning or justification prompts. Enforcement options also include blocking an activity outright in extreme circumstances, or applying a persistent access control like identity-based encryption to data in motion (e.g. as it is copied to an external drive). Moreover, unlike other data security solutions which require rules to be written to record specific activities, Digital Guardian forensically monitors and records all system, application, and data-level transactions by a privileged user out of the box whether they occur on or offline. Types of activities Digital Guardian logs by default include:

- Application launches and running processes
- Data written to CD or USB device
- Network events, by port and protocol
- File uploads and downloads, including via secure tunnels (e.g. social media or private e-mail account),
- Cut and paste between applications
- Local and network printing
- Screen captures
- File transfers to a remote locations

### Secure Collaboration with Identity-based Encryption

Digital Guardian policy controls include three forms of encryption fully integrated into the platform and enabled by a common policy framework: Removable Media Encryption (RME); Adaptive File Encryption (AFE); and Adaptive Mail Encryption (AME). Digital Guardian's unified encryption solution is built upon a transparent, automated key management system using AES-256 cryptography to provide file-level security without the complexity of a manual Public Key Infrastructure (PKI). Digital Guardian's unified and rules-based security model fundamentally eliminates the need to manage multiple and disparate point encryption solutions to maintain consistent end-to-end data protection in collaborative environments.

- **Removable Media Encryption (RME)** is used to dynamically encrypt files copied to removable media (USB, CD/DVD, etc.). RME can be configured to selectively encrypt files based on data sensitivity, device security, or by default for all transactions. RME policy rules support transparent, identity-based encryption between internal users, or password-based encryption for file access on machines without Digital Guardian endpoint agents.
- **Adaptive File Encryption (AFE)** provides identity-based file encryption for sensitive IP at-rest or in-motion on the local disk or remote network locations with transparent decryption between privileged users. AFE fills the security gap left by full disk encryption solutions by ensuring only authorized privileged users may access sensitive data, regardless of their system rights (i.e. IT administrator). AFE policies are integrated and transferrable with the RME and AME modules.
- **Adaptive Mail Encryption (AME)** offers automatic encryption of email content and attachments sent inside or outside the enterprise, including to authorized partners, contractors, and clients. Unlike many traditional email encryption solutions that rely on voluntary user compliance to encrypt data prior to being sent, AME can enforce user-based policy controls, or use the same automated policy framework as RME and AFE to ensure IP remains protected as it leaves the enterprise. AME eliminates the cost and complexity of managing a separate email encryption infrastructure, and integrates with both enterprise and web-based email systems. Like RME, AME can be configured for transparent encryption between internal users, or enforce password-based encryption for file access on machines without Digital Guardian endpoint agents.

The Digital Guardian technology platform offers the most comprehensive and flexible solution available for protecting Intellectual Property. By combining data-centric visibility with user-aware access and control policies, Digital Guardian enables organizations to increase the secure collaboration of IP across globally-distributed users of varying policy privileges without interrupting the business process. Digital Guardian is not designed to simply scan for content and block network events like traditional DLP; rather, it applies policy-based logic to understand the context of data use and enforces the most risk-appropriate controls to maximize the productive use of IP by privileged users.

# Companies Serious About IP Security Look to Verdasys

Verdasys delivers data security solutions for companies that take a strategic and risk-based approach to protecting intellectual property. Digital Guardian protects sensitive data for dozens of the world's largest companies in manufacturing, lifecycle sciences, and high-tech, along with government and military agencies. It secures everything from software code to next-generation automobile designs to top secret intelligence. Below are a few examples of how Digital Guardian is used to protect IP:

- **Semiconductor Manufacturer** A multi-billion dollar fabless semiconductor company with over 3,800 patents worldwide for innovations in both wired and wireless technologies turned to Verdasys to protect their IP and maintain strict export control compliance. They deployed Digital Guardian agents on more than 12,000 Windows and Linux endpoints across the enterprise, including file servers, Citrix servers, desktops and laptops. Digital Guardian now protects their intellectual property while enabling and controlling its use between authorized internal and external collaborators, such as contractors, partners, and suppliers.

- **Chemical Manufacturing Company** A $30 billion chemical manufacturing company turned to Verdasys to classify and control IP on their enterprise network after experiencing a data breach by a privileged user which totaled over $400 million in damages. Digital Guardian is used to provide IP lifecycle management from creation through production on 50,000 internal endpoints across three continents, plus an additional 7,000 machines at supplier and partner sites worldwide. The company also utilizes Digital Guardian to protect trade secrets for plant and machinery designs, thus enabling manufacturing facilities to come online faster in more cost-effective regions knowing their trade secrets will not be compromised when working with foreign governments and engineering partners.

- **Auto Racing Company** Digital Guardian is also used to contain trade secrets within one of the most competitive environments in the world – F1 racing. A perennially-favored racing team deploys an entire mobile IT environment at every race, and relies on Verdasys technology to protect critical racing data and other IP from falling into the hands of competing teams. Digital Guardian protects highly differentiated information, from the optimized gas mixture in their racing tires to real-time track telemetry to next generation engine designs, helping to assure the company's world-class brand remains synonymous with innovation and success. Digital Guardian's ROI to the company was realized after its user activity logs were used to prove the guilt of a privileged insider caught attempting to steal IP for a competing racing team. Digital Guardian identity-based event forensics directly resulted in the company receiving $100 million in restitution from the competitor along with award of that season's F-1 World Championship title, which generated another $500 million in attributable revenue.

- **Auto Manufacturer** A $13 Billion auto maker needed a solution to protect IP essential to its brand identity. The company deployed Digital Guardian across its vendor supply chain, also used by other car manufacturers, to safeguard the information most important to their competitive advantage. With Digital Guardian, the company eliminated many of the inefficient processes and procedures required to securely transact information with shared suppliers, which lowered costs and improved business speeds. They also use the same Digital Guardian deployment to maintain PIPEDA compliance, a Canadian federal regulation for safeguarding employee records. With Digital Guardian, the manufacturer dismantled a costly and ineffective information security model based on disparate and non-integrated point solution, and adopted a data-centric approach using a flexible and integrated technology platform which combines their requirements for IP protection and regulatory compliance into a single, strategic program that has proven to scale and evolve as new data security challenges emerge.
- **Technology Manufacturer** Digital Guardian is used to protect highly sensitive IP for a $13 billion global technology company that needed to bring design labs online in China and India. With offices in four continents, this company utilizes Digital Guardian to provide sophisticated content analysis and multi-level classification in several languages. Its scalable and flexible architecture enabled a centralized and relatively small security team to effectively analyze and respond to potential policy violations across their global operations, particularly in regions that pose a high risk of IP theft. Digital Guardian allows the manufacturer to realize the economic advantages of research and production in these emerging markets with data-level visibility and risk-based controls assuring their data will not be compromised.

## The Verdasys Difference

The Digital Guardian solution is the foundation of strategic data security programs for organizations around the world. From the Digital Guardian technology platform, companies are able to build out iterative risk management processes using real-time policy communication, consistent and unified policy enforcement, and risk appropriate controls designed to drive the maximum business value from IP.

With experience designing and deploying strategic data security programs at over 200 of the world's largest companies, Verdasys has the most extensive "real world" experience and proven track record of any enterprise information protection vendor. From implementation to usage analysis and policy control design, Verdasys has the expertise to help create a data security program that aligns with your business objectives. Verdasys subject matter experts work with clients using our proven methodologies to implement a measurable data security solution through each phase of data discovery, classification, risk analysis, policy deployment, training, and business process integration. The combination of best-in-class technology and services allows Verdasys to help customers create an environment that increases both the security and productivity of IP at the same time.

## Conclusion: Unlocking Intellectual Property Drives Competitive Advantage

Organizations struggle to find the balance between IP collaborating and protection in a dangerous world. The most effective information protection programs combine usage monitoring, risk analysis, policy awareness, and productive controls to drive competitive advantage. Verdasys Digital Guardian delivers the most complete solution to protect intellectual property throughout collaborative and distributed business processes.

Digital Guardian is the only solution proven to deliver integrated content, context and user-determined data discovery to accurately identify and classify intellectual property at enterprise scale; it is the only solution that offers persistent and inheritable meta-tagging to support data lifecycle management; it is the only solution with fully integrated identity-based file, email and removable media encryption; and it is the only solution that forensically logs all system, application, and user attributable data events out of the box. The Digital Guardian security model works independently of system privileges, and continuously manages every aspect of acceptable IP use inside our outside the corporate network.

With Digital Guardian, organizations have an innovative and complete end-to-end solution for mitigating the risks to sensitive data in highly competitive industries. It is the premiere enterprise information protection solution for companies that are serious about implementing a strategic data security program.

## ABOUT VERDASYS

Verdasys (Twitter: @Verdasys_Inc) provides Enterprise Information Protection (EIP) solutions and managed services that secure sensitive data and assures the integrity of business processes that enable midsize and global businesses to successfully compete in collaborative and mobile environments. Digital Guardian, recognized as a Leader in Gartner's 2011 Magic Quadrant for Content-Aware Data Loss Prevention, is a proven technology platform that provides complete policy-based data lifecycle monitoring, classification, forensics, and control on endpoints and servers; virtual machines and enterprise applications; networks; mobile devices; and cloud environments. Digital Guardian protects IP and regulated data from compromise by insiders, contractors, partners, and targeted cyber attacks. Since 2003, millions of Digital Guardian agents have been deployed to protect critical data for global leaders in financial services, insurance, technology, manufacturing, and healthcare industries. Companies serious about information protection choose Verdasys.

VERDASYS®

Corporate Headquarters
860 Winter Street, Suite 3
Waltham, MA 02451 USA
info@verdasys.com
781-788-8180

**www.verdasys.com**