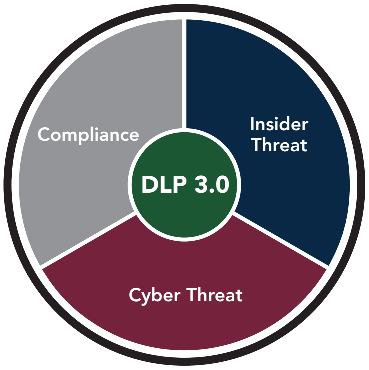
VERDASYS®

DLP 3.0

MEETING TODAY'S DATA PROTECTION CHALLENGES: DLP 3.0 AND ENTERPRISE INFORMATION PROTECTION

WHITE PAPER



Executive Summary

Meeting Today's Data Protection Challenges: DLP 3.0 and Enterprise Information Protection
Data Loss Prevention (DLP) 3.0 redefines the risks and threats to a company's sensitive information, the incremental changes and expansion of these risks and threats over time, and most importantly, the increased complexity and challenges inherent in deploying systems and processes to defend against them. Enterprise Information Protection (EIP) is an integrated approach that offers an effective DLP 3.0 defense, securing sensitive data from a constantly evolving threat environment. Although an EIP approach includes people, process and technology, this paper focuses on the technology portion of EIP.

Defining DLP 3.0

DLP 1.0 focuses on compliance and protecting clients' PII and PHI data. First generation DLP was, and still is, primarily focused on the financial services, insurance and health care industries being driven by PCI standards as well as HIPAA, GLBA and many state privacy laws. Regulation driven and prescriptive in nature, DLP 1.0 begins and ends with broad controls and does not recognize changing risks or threats.

DLP 2.0 focuses on the insider threat and includes advanced data types: intellectual property, trade secrets, critical business plans and classified information. The threat posed by insiders is not new but has exploded as a risk with the advent of multi-gigabyte storage devices and cloud file sharing. Second generation DLP products extend from the network to host-based sensors and agents for desktops, laptops and servers, collecting a wide range of data events in order to define risks and threats and apply more fine grained and appropriate controls.

DLP 3.0 adds the latest and fastest growing threat to critical business information: cyber attack, also known as Advanced Persistent Threat (APT). Most often initiated as an outside attack through phishing, spear phishing or zero day exploits, these attacks succeed in penetrating a company's perimeter and stealing the credentials of insiders before finding and exfiltrating targeted data. DLP 3.0 is a nascent market, with many new companies offering countless specialized products but all focused on specific points in a cyber attack, forcing a disjointed and complex defense.

The True Challenge of DLP 3.0

Because the threats and risk of all three generations of DLP must be addressed, and because this is most often done with three or more different approaches, technologies and organizations, risk, compliance and security teams find themselves mired in disjointed and increasingly costly disparate programs that are doomed to fail. No company can expect to cover the changing threats, multiple business technologies and complexity of security products unless the process, programs and technologies are unified into a single EIP approach. That approach must begin with an integrated technology platform and extend to process and people.

What Is an EIP Approach and Why Must It Be Taken?

Enterprise Information Protection (EIP) is an approach that includes people, process and technology. However, the technology: must be a single integrated platform; must be capable of offering unified features that protect against the changing threats described herein; must work across the multiple business technologies in use; and most importantly, must simplify the deployment, operational management and definition of data protection policies and controls if there is any chance for the people and process parts of EIP to succeed in a cost effective manner.

Companies Must Mature Their Data Protection Programs and Must Do So With an EIP Approach

In order to protect sensitive data from compromise and loss, companies must mature their DLP programs to cover all three generations of data loss threats: compliance, insider threat and cyber attack. Companies who do not build, mature or modify their data protection programs and who maintain sensitive data related to business operations will undoubtedly suffer a data compromise. Companies who find their existing DLP technology is not integrated into a common platform or does not meet a majority of the DLP 3.0 requirements should immediately begin evaluating replacement technology. A successful enterprise-wide data protection program must be built on an EIP platform that reduces complexity while offering data risk visibility, application control, classification, unified policy enforcement and deep forensics to meet the requirements of all three generations of DLP 3.0: compliance, insider threat and cyber threat.

A successful EIP program includes not just a technology platform but also people and process however it is the technology platform's unified views of risk intelligence, flexibility of a single policy engine and detailed forensics that enable both people and process to be successful. Without the platform, the complexity of managing multiple data security tools against threats that continue to transformation and advance across the business and technology systems that are often not covered by existing security tools create a recipe for a poor end user experience and disastrous data loss.

1. Introduction

The goal of this paper is to reconcile the growing number of and severity of data loss incidents that are occurring against the increased spending reported by analysts on security products. Something is amiss when the 2012 Verizon Business Report states that in 2011 some 855 data loss or compromise incidents occurred, the highest level since the report started in 2004[1] at the same time the Gartner reports the world wide spend on IT Security falls around $60 billion in 2012[2].

How can companies be spending this much money and the rate and damage of data loss is still rising?

This white paper utilizes the term Data Loss Prevention (DLP) 3.0 to define a market, the threats in that market and the technologies that have been developed to address the market. The paper also uses the term Enterprise Information Protection (EIP) to define a specific approach to addressing all three generations of data loss prevention discussed in this paper.

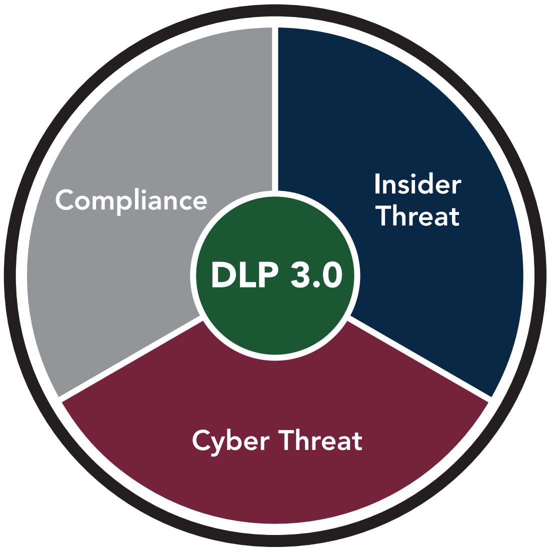
2. Meeting Today's Data Protection Challenges: Defining DLP 3.0 and The Enterprise Information Protection Approach

DLP 3.0 redefines how we look at the risks and threats to sensitive data and how they are evolving and becoming increasingly complex to manage across all of the different platforms (OS, Virtual, Cloud) and business models (remote workers, outsourcing, social media) inherent in today's enterprise. DLP 3.0 changes the discussion from an IT centric view of security (isolated, unrefined, blocking) to a business centric view where data protection must be defined in terms of the risks and threats that companies can define, measure, prioritize and mitigate. Companies who do not or cannot take this foundational and holistic approach to observe, analyze and understand the true risks to their critical business data will incur a breach and suffer the expensive consequences: competitive loss, customer loss, reputational loss and regulatory fines. Every month the newspapers and technology publications share the data loses of companies who do not open their eyes to DLP 3.0. Worse, the attitude of "it won't happen to me" still pervades many organizations even with the wide reporting of threats and loses.

THE HISTORY OF DATA THREATS AND TECHNOLOGY:

DLP 1.0

First generation data loss prevention technology (DLP) and programs focused on compliance and protecting clients PII and PHI data. First generation DLP was and still is primarily focused on the financial services, insurance and healthcare industries being driven by PCI standards as well as HIPAA, GLBA, EU and UK privacy and many US State privacy laws. Regulations, by definition, are completely prescriptive and use the term risk only to define the risk of an ineffective prescriptive control. The fast changing landscape of technology (cloud file sharing, virtualization and mobile devices) and threats (insiders, hacktivists and cyber attack) has made all of these regulations and most of the technology and programs that follow them ineffective and outdated. Worse, as companies further invest to be compliant, not focusing on the changing risk and threat landscape, they are actually creating more risk that their data will be compromised. First generation DLP is more concerned with meeting audit regulations than it is in protecting data as it has no ability to define new or unknown risk, yet these programs still represent a majority of DLP technologies deployed in the market.



[1] Verizon 2012 Data Breach Investigations Report

[2] Forecast Overview: Security Infrastructure, Worldwide, 2010-2016, 2Q12 Update Published: 8 August 2012 Analyst(s): Ruggero Contu, Christian Canales, Lawrence Pingree

Examples of DLP 1.0 use cases:

- PCI compliance
- HIPAA/HiTech compliance
- GLBA & State Privacy compliance
- FISMA compliance

DLP 2.0

The second generation of DLP focused on the insider threat and moved beyond PII and PHI data to include intellectual property, trade secrets, critical business plans and classified information. Defined by the infamous Bradley Manning WikiLeaks case, insider threat had been an ongoing problem for many years but has exploded as a risk with the advent of multi-gigabyte storage devices and cloud file sharing.

First generation DLP products, with their network and content limitations, have failed to offer risk visibility or mitigation capabilities to meet the DLP 2.0 challenge and a second generation of DLP products then emerged. These solutions move beyond the network, focusing on host-based technology for desktops, laptops and servers and on the varying platforms on which they reside, including virtual systems. They capture data events across the enterprise and aggregate this data to show risk in the form of "file types" and "amounts" of data moving across and off the enterprise as well as trends of data usage by employees with the goal of recognizing risk events and taking action to prevent them.

Some first generation DLP providers have attempted to move to DLP 2.0 by adding limited functionality endpoint agents and trying to cover the insider threat use case. These solutions are characterized by an over reliance on content-based scanning technology as noted in Gartner 2013 Content Aware DLP Magic Quadrant. This "content" limitation can be seen in DLP solutions that require an agent to transmit "file content data" to network components for scanning to see if matches exist against policy dictionaries.

DLP 2.0 Use Cases

- Privileged user data access management and control
- Knowledge worker data access management and control
- Endpoint and network data event monitoring, access and usage statistics
- Mobile systems data monitoring and control
- Off network and offline systems data monitoring and control
- Data forensics and case management
- ITAR/EXPORT Control Compliance
- Supply chain IP protection

DLP 3.0

DLP 3.0 adds the latest and fastest growing threat to critical business information, "cyber threat". The most aggressive of these cyber threats often fall under the characterization of Advanced Persistent Threats (APT). Cyber attacks are most often initiated through phishing, spear phishing or zero day exploits. These attacks succeed in 1) penetrating a company's perimeter defenses, 2) spreading throughout the host network, 3) stealing (or escalating) the credentials of insiders and then finding sensitive data and 4) exfiltration of targeted data, usually via covert and encrypted channels.

Cyber attack is the fastest growing threat to all companies big and small and a major focus of awareness programs by the US Congress, FBI and Department of Defense. The cyber attack threat is massive because of the attackers are a mix of nation states and organized crime syndicates who are very well trained and funded. Cyber attack builds on the insider threat premise but requires additional capabilities and programs to successfully recognize and defend against the attack. In addition, the combined insider and outsider threat has emerged where a compromised insider introduces the malware, bypassing the latest generation of cyber threat perimeter defenses technology.

DLP 3.0 Use Cases

- Initial breach detection and investigation
- Reconnaissance threat detection and containment
- Lateral propagation infection detection and blocking
- Command and control detection and blocking
- Data exfiltration detection and blocking

3. Product Challenges

Companies attempting to protect their data face challenges not only from data loss threats, but also from the vendors who provide security technology. One approach is purchasing from the "big box" security retailers who have acquired multiple security technology companies over the years and deliver them as silos or with a thin veneer of integration called "product suites". History has shown that, in most cases, these technology acquisitions don't ever seem to come together and rarely reduce overall risk.

Many of these same vendors have attempted to morph their acquired first generation DLP products into versions that can address the risks of second or third generation DLP. These approaches have not been successful. In a 2011 Gartner survey of CIOs, DLP deployments ranked second as the most failed type of technology project (Gartner Survey of CIOs, March 2011). Some issues that cause these failures include:

- An overreliance on content scanning as the only means of identifying sensitive data.
- The requirement to scan content on a network-based system, requiring all host data be sent across the network consuming huge amounts of bandwidth and making scalability impossible.
- An inability to track sensitive data through the life cycle of its movement, relying on a single point of action to determine policy violations.
- The lack of ability to capture the context of a data event (application, file type, file name, computer, user and often action) and therefore better determine true intent and risk.
- The challenge of deploying acquired technology that is not integrated in a meaningful way.
- Overuse of "one size fits all" policies that overwhelm incident response teams.

A different approach from the "large security vendor suite" is to partner with the start-up "best-of-breed" vendor. Few industries rival the security market for start-up companies that emerge when a new business problem or threat is defined. Like in the DLP 1.0 market back in 1993, in the current cyber threat market there are many of these vendors vying for leadership. Although each almost always offer a unique and effective solution to the challenge they are trying to solve, they all too often are focused on only a small part of the overall problem. Cyber threat is a good example as many of the startups are focused wholly on the initial cyber attack and offer little or no features to defend against the second, third or fourth stages of these unpredictable attacks.

Ultimately, a company that goes down either path will end up with the same problem: being forced to deploy multiple products to cover multiple data protection uses cases across all three generations of DLP threats. The result, a security staff that has to learn how to operate three or more different user interfaces, policy frameworks, reporting structures and control methodologies. Let's not forget these are complex products and take training and practice to master. Add to that both the changing threats and the changing technologies being deployed across the enterprise and it is no wonder that companies that have invested millions in hardware and software, have growing security departments with many able to pass an outside audit, still lose data. The existing environment is a recipe for disaster and best described as trying to play "whack a mole" where the moles represent different threats, but having to use a different hammer (for each different product in use) with each "attempted whack".

There is a third approach which is more common in business systems technology and that is the "platform approach". Companies like SAP, Fujitsu and IBM grew to prominence by offering their customers a core computing platform that supports multiple business processes: financial, supply chain, manufacturing, etc. This platform approach offers a common set of user interfaces, policy and control frameworks and report building engine. The benefits of this common platform approach over deploying and managing multiple software products or disparate "suites" of products:

- Reduced learning curve and ease adoption through shared interfaces.
- Reduced policy and process complexity due to the common frameworks and models.
- Easier coverage of changing business needs through an extensible platform.
- Reduced deployment and support costs with the single solution.

4. DLP 3.0 Requires a "Platform Approach"

It is often said in security circles that "it is all about protecting the data" and an argument can be made that if one looks across DLP 3.0 and focuses on the protecting the data, a necessary platform approach emerges as the only model that can attempt to cover the changing threats, multiple business technologies and complexity of security products. In the DLP 3.0 world a platform approach is required because:

- The risk threats and attack types change too quickly.
- Lack of extensibility in disparate security product leads to ineffectiveness as business models change.
- There is very little ability for companies to capture and understand their real risk to data loss.
- With current data loss incidents of all types, the reaction time to a loss is weeks and months, not hours.
- The complexity of existing systems or new systems is too intricate to effectively train security responders.
- Very few companies have operationally deployed effective policies and controls to protect data beyond the DLP 1.0 compliance requirements.

A platform approach would address all three generations of DLP. It would reduce the complexity of the existing security environments and offer a starting point for the creation of a continuously evolving and improving data protection program. But what would this platform need to look like and what would it need to accomplish?

THE REQUIREMENTS A DLP 3.0 PLATFORM

- Visibility, across the enterprise, to capture data events in full context – offering a complete view of risk intelligence of data loss threats.
  - This is achieved by "instrumentation" of sensors on as many host systems and networks as possible that are autonomous and intelligent to collect context-based risk intelligence on data events.

- A single, integrated reporting engine to aggregate data, define and measure risk and create operational reports that include near real-time alerting and incident management as well as longer term trending analysis.
  - Captured data must be aggregated and correlated into actionable risk intelligence and delivered as useful alerts, incident workflows and reports through a central data warehouse and reporting engine.
  - Reporting should include dashboards that look across data flow channels (network, Web, cloud, USB, mobile, Webmail, email, FTP, etc.) and all drill down to see the context of each specific event (user, machine, action, application, file type, file name, etc.).
  - Data output capabilities to push aggregated risk intelligence to SIEM and other forensic technologies.

- A single integrated command and control interface to define risk-based policies and controls and push those controls out across the network and endpoints to mitigate risk in a measurable way.
  - Effective risk mitigating controls are automated, event-based and occur in real-time before the data loss event occurs. Policies include data type and amount, user, group or role, transaction type and include multiple controls.
  - Controls fire when policies are violated with different types of controls being used to mitigate different levels of risk. A low risk control might be a simple prompt with justification where a higher risk event might include data encryption or transaction blocking.
- Forensic data event capture in a case management tool that creates evidentiary sound reports because DLP 2.0 (insider threat) will often end up in litigation.
  - The data events captured have little value if they cannot be used to prosecute an insider found compromising data with two critical goals: (1) that a court case is avoided because the data events captured as so compelling as to force a guilty plea, and (2) the guilty plea acts as a future deterrent within the company.
  - Data events must be captured with assurance of non-repudiation. Data event logs must be evidentiary grade with chain of custody, tamper proof and include restricted data access control to be introduced in a legal process.

5. Enterprise Information Protection: A Data-Centric, Risk Driven Platform Approach for DLP 3.0

The technology foundation of Enterprise Information Protection (EIP) delivers a platform approach to DLP 3.0, but EIP moves beyond just technology and encompasses an information-centric framework that begins with a technology platform and then adds people and process to create a complete and continuously improving data protection program. The EIP technology platform meets the full set of DLP 3.0 requirements: risk visibility and measurement; risk prioritization; integrated policy management and control; integrated data event aggregation and reporting; and forensic data event capture and case management.

EIP moves beyond the indistinct DLP market defining a holistic approach to mitigating data loss risk, a cross enterprise approach that includes (and must) include lines of business and a platform approach that covers three generations of DLP and should attempt to be “future proof” and cover “DLP 4.0” and beyond. The ultimate goal is to create a proactive, sustainable and continually improving enterprise information protection program across the organization that enables collaboration and competitive advantage while mitigating the risk of data compromise across all three generations of DLP threats. An EIP program takes a risk-based, data-centric approach security. In other words, it’s about the data and understanding:

- The full context of data events to define what is sensitive data, where it is located and how it is being used, offering true data risk intelligence.
- The visualization of data risk intelligence in aggregated dashboards and reports that define and measure risks, incidents, trends and alerts that can be communicated across all lines of business.
- A unified policy and control model that effectively mitigates data risk in a measurable way.
- Historically what data events occurred that violated corporate and regulatory policy as well as what incidents occurred that describe or define an insider attack or cyber attack, and that this forensic information is captured in data event logs that are.
- Forensic data event capture in a case management tool that creates evidentiary sound reports because DLP 3.0 will often end up in prosecution evidentiary grade and can be used in legal proceedings.

6. DLP Requirements by Generation

By breaking the EIP approach down into technology, process and people, each area can be described in terms of critical requirements and value. The following chart is a list of either incremental or new requirements for each generation of DLP. In many cases, the new requirements are incremental (2) with other being new requirements (3), showing the necessity of an integrated platform approach.

DLP 1.0 SOLUTION REQUIREMENTS	DLP 2.0 SOLUTION REQUIREMENTS	DLP 3.0 SOLUTION REQUIREMENTS
Independent data incident monitoring (sensors, agents & appliances); Endpoint, Servers, Network, Virtual, Mobile and Cloud	Independent data event (and incident) monitoring (sensors, agents & appliances); across Endpoint, Servers, Network, Virutal, Mobile and Cloud (2)	Integrated, autonomous layers of defense across, network, endpoint and servers including operating system and system memory (2)
Monitor and control all data movement channels; Email, USB, Cloud Share, Mobile, Print, etc…	Content, context, user and application aware event collection across all data events and channels, Email, USB, FTP, Web, Virtual, Cloud shares, Print, Mobile, SharePoint, etc.	Inbound attack detection, executable detection, application control, inbound traffic monitoring, threat detection engines, attack threat feeds. (3)
Entensive dictionaries, policy models for PCI, HIPAA, GLBA, PCI, FISMA…(1)	Greater policy flexibility to define when and how data protection controls will fire and more interactive data controls to drive real time awareness and education and end users(3)	Education & Awareness Prompting to end user before a data incident occurs (2)
Content, context, user and application aware event collection	Policies that actuate data tagging automatically or by data owner action (3)	Command & control detection and blocking; inbound outbound monitoring Intel feeds on known command and control systems (3)
Continuous event auditing and reporting across data events and incidents	Integrated data tagging (instantiating classification models) persistent tags, inheritance (3)	Secondary infection, recon stage blocking system, memory and network (3)
Integrated, automated FIPS-140 Disk, file and email encryption	Integrated FIPS 140-2 File, Email, Removable Media, Server and File Share Encryption (2)	Data exfiltration blocking; network blocking, host blocking, encryption, threat intelligence onknown bad destinations (2)
Education & Awareness Prompting to end user before a data incident occurs	Data event aggregation, trending analysis, behavior analysis, reporting and alerting (2)	Data access, data usage, data movement, application usage, and memory events — collected and aggregated in a centralized forensic analysis engine from across the enterprise including network, endpoint and virtual systems (2)
Full detection and control capabilities on or off the network and on or offline	Education & Awareness Prompting to end users including justification, to prevent data incident before they occur (2)	Malware Detection Engine, Static and Dynamic Analysis, Virtual execution of malware (3)
	Integrated forensic investigation and case management system (3)	Adaptive policies, combination of risk factors elevates response control (2)
	Full detection and control capabilities on or off the network and on or offline with self-protection (2)	Adaptive policies, combination of risk factors elevates response control (2)
	Global, Scalable, Localized for International Deployments (2)	

(1) Requirement does not carry to next generation (2) Requirement is incremental (3) Requirement is new

DLP 1.0 REQUIREMENTS AND VALUE

DLP 1.0 is focused on compliance with the many regulatory laws that almost all businesses with operations in the US and Europe must follow. Traditionally a network-based solution was utilized to help meet DLP 1.0 requirements but as regulations have changed and limitations of network DLP become recognized a wider approach is being adopted. Not that Network DLP has lost its value, instead it is recognized that a network approach, combined with endpoint, server, virtual agents and encryption technologies is a much more sound approach. As stated, all of these capabilities should be delivered in a single platform.

DLP 1.0 SOLUTION REQUIREMENTS	VALUE
Independent data incident monitoring (sensors, agents & appliances): endpoint, servers, network, virtual, mobile and cloud.	Independence of the technology agent offers greater visibility with greater scalability. Agents or sensors dependent on other technologies, either internal to the solution or external to the system create reliances (and limitations) based on the weaker system. Moving sensitive data over the network in order to protect it is a system limitation that puts more data at risk and ties up bandwidth, thereby reducing scalability.
Monitor and control all data movement channels: email, USB, cloud share, mobile, print, etc.	Monitoring all channels is required for a holistic approach: leaving a channel of data movement uncovered is creating an unknown data loss incident. Controlling these channels is required by most regulations.
Extensive dictionaries: policy models for PCI, HIPAA, GLBA, PCI, FISMA, etc.	Multiple, complex and changing regulations make internal, manual management costly and difficult. Having the solution include as much of the regulatory information as possibly simplifies management.
Content, context, user and application aware event collection.	Content-based data inspection alone is inherently overburdened with false positives. Data event context (user, file type, file name, application, machine, etc.) is used in conjunction with content inspection and greatly reduces false positives.
Continuous event auditing and reporting across data events and incidents.	Regulatory incident collection alone will show only the "known incidents" as defined by the limitations of the "incident policies" in the DLP or security solution. Broader, continuous data event captures will uncover the "unknown" incidents greatly reducing the chance of ugly surprises that cause audits to be failed and negative headlines to be made.
Integrated, automated FIPS-140 disk, file and email encryption.	FIPS-140 encryption is a requirement in most regulations although many specify at most full disk encryption. Full disk encryption and file encryption at effective for lost laptop and lost device use cases. Automated file and email encryption as an integrated data protection control is very effective in reducing data loss risk because it eliminates the need for multiple encryption products, offers a more refined level of user access and usage control and more easily shows compliance in audit reports.
Education and awareness: prompting to end user before a data incident occurs.	Enabling a user to understand a risky action and self-correct before the data event completes is a much more efficient way to be compliant, eliminating a majority of incidents and eliminating the complex and costly workflows required to track an incident once it has occurred.
Full detection and control capabilities on or off the network and on or offline.	Required by regulation, all incidents must be captured to maintain compliance with PCI requirements.

DLP 2.0 REQUIREMENTS AND VALUE

DLP 2.0 extends data protection to cover the insider threat as well as more complex data types including: business plans, intellectual property, trade secrets and classified materials. DLP 2.0 incrementally adds to many of the DLP 1.0 requirements with additional refinement of capabilities needed to cover more complex threats. In addition, the inclusion of greater context awareness, native tagging of files for classification and the ability to add forensics and legal case management are added.

DLP 2.0 SOLUTION REQUIREMENTS	VALUE
Independent data event (and separate incident) monitoring (sensors, agents & appliances): across endpoint, servers, network, virtual, mobile and cloud.	Building on the DLP 1.0 requirement, DLP 2.0 adds critical capabilities around broader data event capture across more environments in order to monitor knowledge workers and privileged users as they interact with sensitive data.
Content, context, user and application aware event collection across all data events and channels: email, USB, FTP, Web, virtual, cloud shares, print, mobile, SharePoint, etc.	Because the DLP 2.0 requirements include more data types that are much more difficult to define (formulas, CAD files, media files, process flows, etc.) great emphasis is put on advanced data awareness including context, application and user based definitions. Content inspection often becomes the least successful method of defining sensitive data.
Policies that actuate data tagging, either automatically or by data owner action.	Policies must also enable data tagging (see integrated data tagging requirement) so that once sensitive data is defined a marker can be placed with the file (meta data or other method) to "lock" that sensitivity in place. Existing data can be tagged automatically by content or context. New data is often best tagged by the data creator or owner directly with content and context policies used to check the accuracy of the classification level.
Integrated data tagging (instantiating classification models) persistent tags, inheritance.	Operationalizing a data classification program is critical to protecting data from DLP 2.0 threats. Data classification tags added to the meta data of sensitive files define the files' sensitivity as it moves through a business process allowing the appropriate data security control to be activated if a risk threshold or improper activity occurs. Persistence means the tag cannot be removed by IT admins or other advanced users, and inheritance means the tag is carried across buffer activity (copy and paste, export, etc.) so that new file formats are also tagged.
Integrated FIPS 140-2 file, email, removable media, server and file share encryption.	Encryption as an automated control is critical in DLP 1.0 as most regulations require it for data loss, but in DLP 2.0 encryption takes on not only a loss control but a critical data access control. File and email level encryption can limit who has access to the open and use the file (including privileged users such as IT administrators.) This control when activated on a file share, desktop or laptop offers a critical insider threat mitigation control.
Data event aggregation, trending analysis, behavior analysis, reporting and alerting.	Insider threat attacks are planned and often carried out at low levels over a long period of time but always deal with very sensitive data being moved out of the enterprise. Therefore, any movement of sensitive data must be captured and policy engines must be able to issue alerts on granular parameters such as change in data usage, amount or application usage behavior. Reporting engines must offer the ability to view all data events related to a data type or user over time periods of six months or greater.
Education and awareness: prompting to end users (including justifications) to prevent data incidents before they occur.	Incremental to DLP 1.0, this forces all end users to be accountable for their actions and offers a high level of deterrence to compromised actors. Also enables a flexible control so that critical business transactions are not blocked and a feedback loop through prompts with end user entered justifications offers intelligence and risk mitigation for special business activities and side cases.
Integrated forensic investigation and case management system.	Where regulatory requirements fine companies for violations, IP and trade secret incidents offer legal recompense. Employees, contractors and partners who steal sensitive data can be prosecuted, but in order to do so, evidence must be collected that is admissible in a court of law. DLP systems that do not offer evidentiary sound case management are not useful in deterring insider attacks or in seeking successful legal action.

DLP 2.0 SOLUTION REQUIREMENTS	VALUE
Full detection and control capabilities on or off the network and on or offline with self-protection.	In the DLP 2.0 threat environment, the insider who can circumnavigate security will succeed in their attack. Often, the attacker is aware of the security measures in place and will actively seek to control and defeat them. Robust coverage with tamper resistance, self-protection and other stealth capabilities are critical.
Global, scalable, localized for international deployments.	Although DLP 1.0 compliance requires some levels of scalability and global deployability, in the DLP 2.0 world it is a must have. Where regulations are often local or regional and operations the same, in the product world, supply chains and manufacturing are almost always global. Controls that interact with end users must be in their local language, polices must accept variables based on location and language and scalability must reach to greater than 10K users.

7. DLP 3.0 Requirements

DLP 3.0 extends data protection to defending against cyber attacks focused on stealing data. The initial form of these attacks can vary greatly with most starting outside the organization but quickly move inside and across the enterprise. Once a cyber attack has penetrated the enterprise, many of the traits and activities resemble an insider attack as highly privileged users credentials are compromised and used to enable the attackers to move around the enterprise to find the data they are targeting, and then move that data to an exfiltration point. Therefore many of the data protection requirements for DLP 2.0 extend into cyber attack defense some with incremental capabilities added and new requirements are focused on detecting initial attacks and on breaking illicit command and control communications. When reading the requirements, one quickly realizes that cyber threat defense is the ultimate definition of integrated "defense in depth" because each new attack is different and the defender must assume that historic forensic data like signatures or categorization will fail to prevent the next attack.

DLP 3.0 SOLUTION REQUIREMENTS	VALUE
Integrated, autonomous layers of defense across: network; endpoint and servers including operating system; and system memory.	Cyber attacks take many forms and even entirely new forms as old attack models fail. The attackers can use a mix of attack vectors including "compromised insiders". Attacks have multiple stages and include multiple paths of infection, account compromise and data movement. Defensive systems must offer independent layers of defense across as many systems and subsystems as possible to detect and thwart attacks. Early detection and reduced reaction time are critical to cyber attack defense.
Inbound attack detection: executable detection; application control; inbound traffic monitoring; threat detection engines and attack threat feeds.	Of all the stages of a cyber attack the initial penetration stage is probably the most difficult to detect and defend due to the sheer number of machine and human exploits. Therefore cyber threat defense must include a variety of capabilities covering rogue applications, inbound communications, the ability to check suspected code for malware and the input of the latest attack intelligence information to update detection policies.
Education and awareness: prompting to the end user before a data incident occurs.	End user prompting during a cyber attack is a highly effective means of alerting a user to a "human targeted attack" in real-time and defeating potential phishing and spear phishing attacks. Prompting can also be used to enforce best practice polices and keep employees from making simple but risky mistakes like clicking on a dangerous links or going to a known bad Website. In some cases, prompts can even delay or prevent a data exfiltration.
Command and control detection and blocking: inbound and outbound monitoring; Intel feeds on known command and control systems.	A significant weakness in many cyber attacks is the need to contact a control system to update attack models and stages. During the reconnaissance stage and exfiltration stage multiple calls are made. A defensive system can defeat many types of attacks by monitoring inbound and outbound traffic for these types of calls. Intel feeds with the latest intelligence on the types, formats, destinations and encryption models of these calls are critical in blocking them and defeating the attack.

DLP 3.0 SOLUTION REQUIREMENTS	VALUE
Secondary infection, recon stage blocking: system; memory; and network.	Once a system is infected, the attack moves to infect other more critical systems, compromise additional user accounts and gather information about the network in hopes of locating the targeted data for theft. Defensive systems that monitor internal traffic, endpoint systems that look for malware code running in system memory and endpoint event collection that alerts IT teams to user activities outside of normal operating parameters all help is recognizing and defeating the attack.
Data exfiltration blocking: network blocking; host blocking; encryption; threat intelligence on known bad destinations.	In the final stage of the attack, the malware attempts to move the targeted data to an exfiltration point and then from that point off the network. This is where the DLP 2.0 capabilities can help defeat a 3.0 threat. Endpoint and network agents work together here to recognize, through context and data classification, the movement of sensitive data and fire off automated controls to defeat the attack. Controls can include data movement blocking across the network or at the endpoint and automatic encryption so that any exfiltrated files are useless.
Data access, data usage, data movement, application usage and memory events collected and aggregated in a centralized forensic analysis engine from across the enterprise including network, endpoint and virtual systems.	When cyber attacks are detected it is critical to collect as much forensic evidence about the attack as possible to reconstruct the attack and determine its nature and structure. This information offers immediate defense value by modifying policies and controls to defeat similar attacks. It offers a wealth of forensic information to pass to SIEM and other analysis tools that can correlate even more data a broader set of systems.
Malware detection engine: static and dynamic analysis; virtual execution of malware.	Another defense in depth layer, any potential code that comes inbound to the enterprise must be intercepted, inspected and even “fired off” in a protected environment to determine if it is a threat. Malware will often disguise trojans, rootkits, worms, viruses and other complex malicious software as innocuous looking items on a network. A malware detection engine offers a significant layer of defense in the initial attack stage.
Adaptive policies: combination of risk factors elevates response control.	Another advanced defense in depth capability critical to detecting and defeating a cyber attack is the ability to create and deploy adaptive policies that will, based on cyber attack risk factors, deploy a control or series of controls to gather forensic evidence of an attack or defeat an attack. An example being when an endpoint agent does not recognize an executable firing it automatically kicks off a system memory forensic scan.

Remembering that the goal of a data-centric EIP platform is to create a proactive, sustainable and continually improving EIP program, it should be restated that an integrated technology platform that effectively delivers on all or a majority of the requirements listed offers the ability to:

- Quickly and effectively recognize new and changing threats to data.
- Define and prioritize real risks to sensitive data from poor business process, insider threat and cyber threat, holistically looking across the enterprise and all channels through which data moves.
- Reducing reaction time to data threats, attacks and incidents to hours enabling effective incident management and policy changes to be put into effect before catastrophic events occur.
- Greatly reduce the complexity of security systems, policies, processes and controls, enabling security professionals to work successfully with lines of business to build a successful EIP program.
- Ultimately, to build and deploy EIP programs that are operationally effective and enable the programs to continuously adjust and improve to the ever changing generations of DLP: compliance, insider threat, cyber threat and whatever the next generation of threats expose.

8. Enterprise Information Protection and the Digital Guardian® Platform

Digital Guardian is a risk-based, data-centric security EIP platform that delivers DLP 3.0 visibility, risk intelligence and protection for sensitive data across compliance risk, insider threat and cyber threat. Digital Guardian offers endpoint, server, network, virtual, mobile and private cloud sensors and agents to:

- Capture the full context of data events to define what sensitive data is, where it is located and how it is being used. It offers true data risk intelligence across end point and servers (Windows, Linux, Mac), virtual environments (Citrix, VMware, Microsoft), mobile environments (iOS) and across networks (all 65,535 network ports including those of proxy servers, internal network traffic and MTAs.)
- Deliver risk intelligence in aggregated dashboards and reports that define and measure risks, incidents, trends and alerts that can be communicated across all lines of business.
- Define and deploy a unified policy and control model that effectively mitigates data risk in a measurable way.
- Detect, contain, investigate and defeat cyber attacks with an integrated and layered defense that includes: enterprise-wide traffic monitoring; malware detection and blocking; command and control detection and blocking; end user prompting; automated encryption; centralized forensics and adaptive defensive policy-based controls.
- Provide integrated forensic data event capture in a case management tool that creates evidentiary sound reports proven in prosecution across North America and Europe.

With Digital Guardian, this holistic data-centric "visibility" enables organizations to define and apply data security policies to users, to threats and to applications covering compliance, insider threat, privileged users, contractors, outsourcers, partners and most importantly cyber threats, significantly reducing the risk of data loss. Digital Guardian enables companies to deploy a continuously improving EIP program that covers all the generations of DLP risk and threats.

9. Conclusion: Companies Must Mature Their Data Protection Programs and Must Do So With an EIP Approach

In order to protect sensitive data from compromise and loss, companies must mature their DLP programs to cover all three generations of data loss threats: compliance, insider threat and cyber attack. Companies who do not build, mature or modify their data protection programs and who maintain sensitive data related to business operations will undoubtedly suffer a data compromise. Companies who remain wed to DLP 1.0 programs focusing on meeting compliance requirements with network based DLP products alone are also at a high level of risk for a data compromise as their prescriptive program model and one dimensional product prevents them from seeing and recognizing a majority of the risks and threats they face. Companies who have matured to the DLP 2.0 level should immediately begin extending this program to cover cyber threat defense. They should start by extending existing DLP programs and resources and evaluate existing DLP technology including network agents, automated encryption and advanced forensics for use in cyber attack defense before they move to purchase new disparate specialty tools. In all cases, companies who find their existing DLP technology is not integrated into a common platform or does not meet a majority of the DLP 3.0 requirements should immediately begin evaluating replacement technology.

A successful enterprise-wide data protection program must be built on an EIP platform that reduces complexity while offering data risk visibility, application control, classification, unified policy enforcement and deep forensics to meet the requirements of all three generations of DLP 3.0: compliance, insider threat and cyber threat. A successful EIP program includes not just a technology platform, but also people and process. However, it is the technology platform's unified views of risk intelligence, flexibility of a single policy engine and detailed forensics that enable both people and process to be successful. Without the platform, the complexity of managing multiple data security tools against threats that continue to transformation and advance across the business and technology systems that are often not covered by existing security tools create a recipe for disastrous data loss.

Digital Guardian® is a data protection platform that covers compliance, insider threat and cyber threat defense across as many systems and use cases as any mix of DLP, encryption, cyber threat defense and forensic products. More importantly, it offers the powerful advantages of an integrated platform. With over 250 customers utilizing Digital Guardian to protect their most critical data across more than 2 million systems, Verdasys brings to bear more than just technology. Our experience working with the world's leading companies in deploying successful EIP programs empowers our services and support teams to help your organization deploy EIP technology, methodology and process. Verdasys is the preferred partner for companies serious about protecting their sensitive information. Our customers' success speaks for itself.

ABOUT VERDASYS

Verdasys (www.verdasys.com) provides Enterprise Information Protection solutions and managed services to secure sensitive data and assure the integrity of business processes, enabling midsize and global businesses to successfully compete in collaborative and mobile environments. Digital Guardian, a Leader in Gartner's 2012 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.

VERDASYS®

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

www.verdasys.com