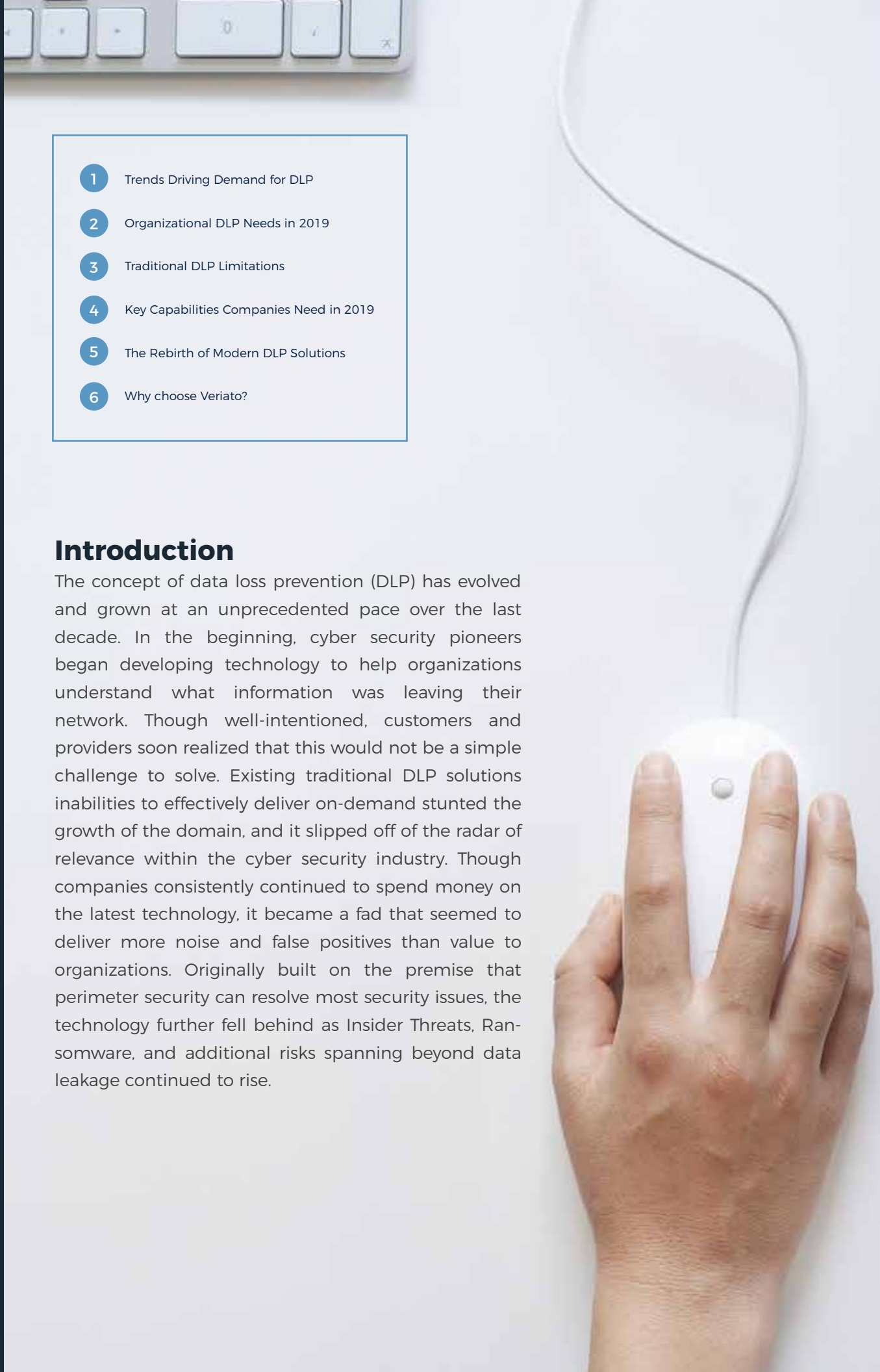
The Evolution of **DLP**

Veriato

www.veriato.com



Introduction

The concept of data loss prevention (DLP) has evolved and grown at an unprecedented pace over the last decade. In the beginning, cyber security pioneers began developing technology to help organizations understand what information was leaving their network. Though well-intentioned, customers and providers soon realized that this would not be a simple challenge to solve. Existing traditional DLP solutions inabilities to effectively deliver on-demand stunted the growth of the domain, and it slipped off of the radar of relevance within the cyber security industry. Though companies consistently continued to spend money on the latest technology, it became a fad that seemed to deliver more noise and false positives than value to organizations. Originally built on the premise that perimeter security can resolve most security issues, the technology further fell behind as Insider Threats, Ransomware, and additional risks spanning beyond data leakage continued to rise.

1

Trends Driving Demand for DLP

Recent trends in cyber security have led to a growing need for data loss prevention and protection technology in companies.

- The average cost of a cyber breach today is about $3.67 million, and causes can be linked to everything from **Insider Threats** to third-party security failures. The need to prevent data loss from various threats remains a key concern for organizations. (https://www.symantec.com/security-center/threat-report)

- **GDPR** non-compliance can cost a company up to 4% of global revenue, making data loss much more expensive than the already costly breach notifications and recovery. (https://www.itgovernance.co.uk/dpa-and-gdpr-penalties)

- Data loss often stems from a company's employees, whether intentional or accidental. 90% of companies feel vulnerable to **Insider Threats**. 64% of companies surveyed also plan to increase their focus on **Insider Threats**. (https://www.veriato.com/docs/default-source/whitepapers/insider-threat-report-2018.pdf)

- Traditional DLP solutions are evolving to include capabilities that span beyond just data leakage as new vendors join the market offering new services. The domain went from including 12 vendors in 2017 to almost 40 in 2019. Customers are buying in. Revenue generation in the industry also increased from $600 million in 2014 to an estimated $1.7 billion in 2019, indicating that companies are continually investing. (https://www.statista.com/statistics/986319/worldwide-dlp-market-revenue-forecast/).

Given these trends, a decade later, companies are still faced with the same critical decision: How will we protect our data? Thanks to these trends across the industry, the rebirth of a modern-day DLP solution is upon us.

2

Organizational DLP Needs in 2019

Data loss prevention tools have promised to deliver on a critical mission, to protect against the loss of valuable information from a company's network. The intent is to provide visibility into the location and usage of data across a company, apply policies based on content and context, and enable companies to respond before any data exfiltration occurs. (Gartner) Discovered threats, whether accidental or intentional actions by users, could then be addressed through blocking, filtering, or execution of other measures that prevent data loss.

The intent is to provide visibility into the location and usage of data across a company, apply policies based on content and context, and enable companies to respond before any data exfiltration occurs.

Key drivers for the increase in attention and demand for DLP include:

Need for policy enforcement: Having an information security policy is a fundamental best practice but is considered a deterring control. Policy alone will not physically prevent the loss of data, and technology is required for enforcement.

Continuous efforts to identify and reduce risk: Companies are seeking ways to identify risks, fix the processes, and educate users on the correct ways to send and store sensitive information. Beyond following traditional risk management and audit frameworks, organizations also need the ability to shed light on broken or insecure processes within the organization that those processes might miss.

Need for policy enforcement: Having an information security policy is a fundamental best practice but is considered a deterring control. Policy alone will not physically prevent the loss of data, and technology is required for enforcement.

Continuous efforts to identify and reduce risk: Companies are seeking ways to identify risks, fix the processes, and educate users on the correct ways to send and store sensitive information. Beyond following traditional risk management and audit frameworks, organizations also need the ability to shed light on broken or insecure processes within the organization that those processes might miss.

3

Traditional DLP Limitations

Policy-based security is not enough. Since its inception, DLP technology has evolved. Starting out a policy-based technology, meant that the technology could mainly focus on predetermined rules and known threats - rigid rules that If not fine-tuned could be a nightmare. The technology was unable to learn or make intelligent conclusions on what might be a threat. Dealing with the unknown threats, without context created more noise. As **AI** and **Machine Learning** applications in Cyber Security mature, context-based management became a way to address this challenge.

It's a reactive technology, falsely branded as proactive. While some would consider having a DLP solution to be proactive security, traditional **DLP** is deemed to be reactive. The technology detects losses as they are leaving the organization and then reacted upon with action if configured to do so. A truly proactive solution provides just in time user feedback before the information export request goes through. For example, before a user sends an email that contains **PII**, they may get a pop-up window that reminds the user of the policy and forces email encryption. If there is additional context regarding other suspicious user behaviors, those can be taken into account as well before alerting or recommending another action. This is when data loss prevention truly becomes proactive.

Complex and ineffective deployments create longer ROI windows. Companies attempting to roll out enterprise DLP solutions were seeing more failures than successes across the industry. Vendors promised easy deployments with full out of the box capabilities, only to learn that much fine-tuning and effort was required to get the technology to provide true value. Traditional DLP is only as good as the policy and rules it's fed.

Automated responses aren't always helpful: An inherent shortcoming of policy-based DLP is that the technology alone isn't smart enough to distinguish suspicious from arbitrary, resulting in the potential for excessive false positives if not configured appropriately. Companies became reluctant to automate blocking of user activity out of concern of disrupting legitimate business processes without proper context.

4

Key Capabilities Companies Need in 2019

Shifting focusing beyond perimeter security has led the use cases of DLP to evolve, and context has become even more critical. Preventing the loss of data in an organization means considering what data is at risk when at rest within the network, in transit, and at rest outside of the network. Next generation DLP solutions provide visibility into each of these use cases by focusing on network activity, endpoints, virtual storage areas, and cloud implementations.

- **Endpoint Devices**: Organizations should have insight into data leaving devices, whether through USB exfiltration, applications that can be used to share data, and more.
- **Storage Devices**: Organizations should have insight into sensitive information sitting within files stored on the network giving organizations insight into who has access to and what's being done with data.
- **Network Devices**: Organizations should have insight into data in use or in transit on the corporate network. Typically through network taps, the technology scans content traversing the network over various ports and provides insight on such activities.
- **Cloud Environment**: Companies are opting for an extension of traditional DLP capabilities into their cloud environment through cloud access security broker (CASB) solutions. (https://www.veriato.com/resources/blog/blog-post/veriato-blog/2019/04/16/what-is-dlp-why-does-it-matter-and-what-is-your-current-strategy-missing)

Users actions within any of these categories can generate hundreds of alerts in traditional DLP solutions making the keyword, context. Across all of these channels, it's important to integrate context and intelligence in this process to reduce the amount of fine-tuning that has to occur and thus limits the number of false positives.

5

The Rebirth of Modern DLP Solutions

The most significant shift occurring is that modern day DLP doesn't just focus on policy-based perimeter security anymore. A good DLP solution integrates traditional DLP with valuable context in order to allow technology to make more intelligent decisions with less false positives and limited human interaction. This enables use cases well beyond preventing simple data leakage.

Insider Threat management: Most data loss is end-user driven. Across the four aforementioned channels, the greatest risk tends to lie in people sending or uploading information that they shouldn't through insecure channels. By monitoring this, organizations can empower their teams to respond to the Insiders causing data loss.

Visibility and contextual awareness: The evolution and inclusion of contextual awareness capabilities is increasing the value of DLP technology. Historically, DLP solutions have focused on the identification of sensitive data through traditional data strings. For example, a tool may search for content that looks similar to a credit card number or social security number. Businesses could also opt to search for keywords that could identify confidential information. Albeit a reasonable start for the industry, these methods often produced many false positives and some false negatives. Traditional methods provided visibility but lacked context.
(https://www.veriato.com/resources/blog/blog-post/veriato-blog/2019/04/16/what-is-dlp-why-does-it-matter-and-what-is-your-current-strategy-missing)

Artificial Intelligence and UEBA integration: The integration of artificial intelligence and machine learning in DLP solutions is paramount to solving these challenges at rates much faster than human beings alone ever could. By analyzing mass amounts of content, applying context, and continually fine-tuning the technology for each organization, next-generation DLP solutions are enabling greater loss prevention capabilities. The fundamental operating principle of User Entity Behavior Analytics (UEBA) is to create a picture of what normal user and organizational behavior looks like, in order to know what can be considered abnormal behavior. Once there is a baseline to compare against, technology can begin to alert on suspicious user behavior. Overlaying this context with traditional DLP allows greater accuracy as organizations look to automate responses to legitimate threats.

6

Why Choose Veriato?

Veriato provides Artificial Intelligence based technology that can fill data loss protection needs, and more.

Identification

Identification of corporate espionage (IP theft): Veriato Cerebral monitors and alerts when sensitive documents or IP is accessed, copied, printed, or moved under unusual circumstances. IP is different for every company and also requires context to manage accurately. Additionally, Veriato AI can monitor psycholinguistic patterns to detect disgruntled employees by monitoring their sentiment for possible signs of a threat

.

Monitoring

Monitoring of data exports to unapproved cloud environments: Veriato Cerebral will watch all cloud uploads and trigger alerts if a user is suddenly printing unusual volumes or unusual data.

Insight

Insight into removable storage devices such as USB: Veriato will watch all USB drives and removable storage devices. If a user is suddenly copying large volumes or abnormal data, security will be alerted.

Awareness

Awareness of abnormal print jobs: Veriato will monitor all print jobs. If a user is suddenly printing unusual volumes of data, security will be alerted.

Tracking

Tracking of critical documents: Veriato can add specialized documents as keywords. If someone outside the privileged group such as board members, c-suite, and engineering management, accesses the sensitive document, security will immediately be alerted.

Support

Support during employment termination: Veriato watches for changes in behavior that signify an employee may be leaving the company such as the sudden archiving of email, large data downloads, moving large volumes to cloud storage or an unusual amount of email attachments.

Summary

The Cyber threat landscape is widening, and security strategies and technologies are continually working to keep up. DLP can help prevent unauthorized information from leaving the organization through human error, malicious Insider Threats, and other means, but it doesn't stop there. Modern DLP solutions can overlay traditional analysis with context from Insider Threat program technology and other sources to provide a more intelligent view of data leaving the organization.

To learn more about how Veriato can help you mitigate data loss, contact a Veriato representative today.

Over 3,000 enterprises, & thousands of SMBs have placed their trust in our solutions

Our solutions are deployed in **110+ countries**

Veriato USA

4440 PGA Boulevard , Suite 500

Palm Beach Gardens, FL 33410

Veriato EMEA

3rd Floor, Crossweys House

28-30 High Street

Guildford, Surrey

GU1 3EL United Kingdom

https://plus.google.com/+Spectorsoft

https://www.linkedin.com/company/veriato

https://twitter.com/veriato

https://www.youtube.com/SpectorSoft

https://www.facebook.com/VeriatoInc/