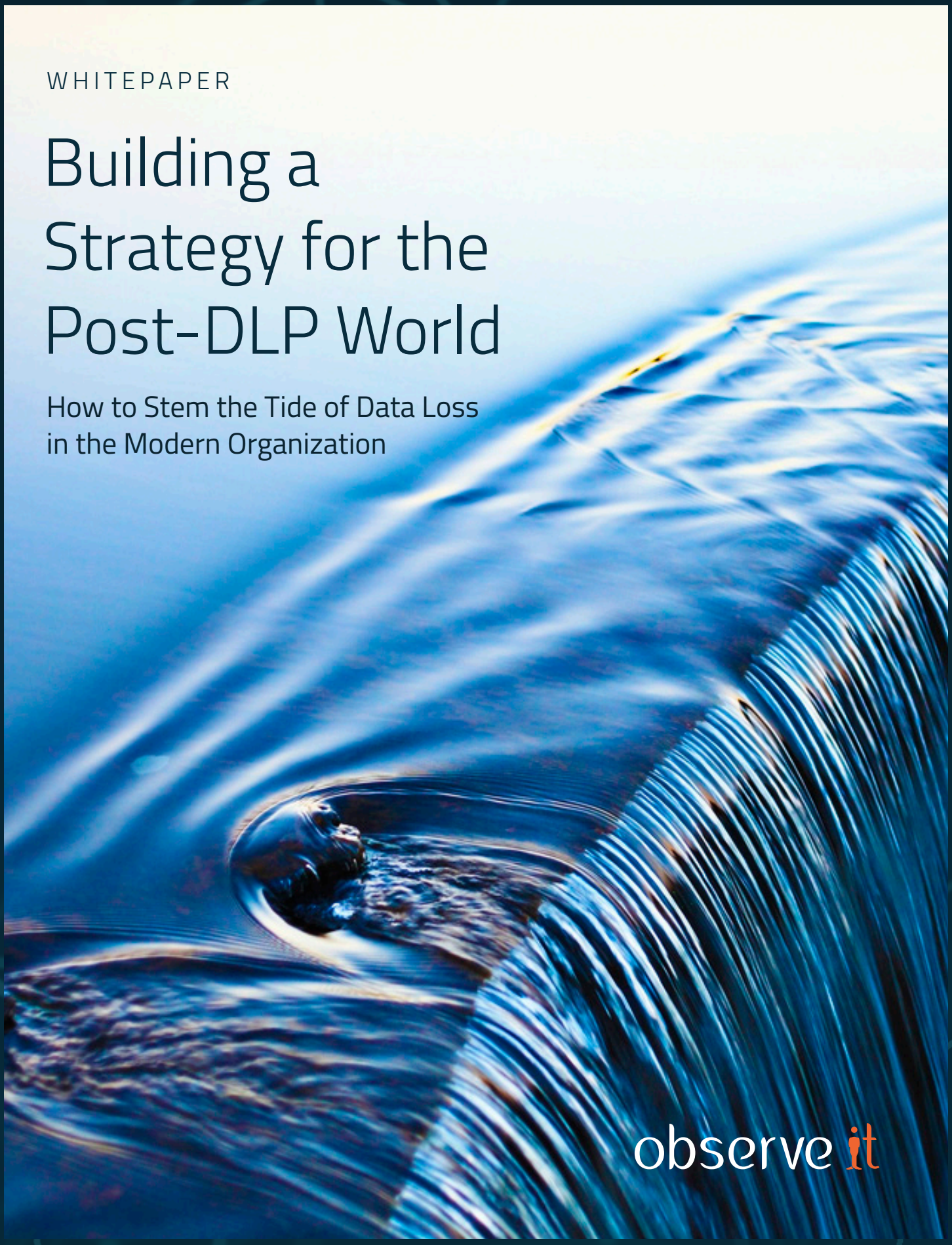
WHITEPAPER

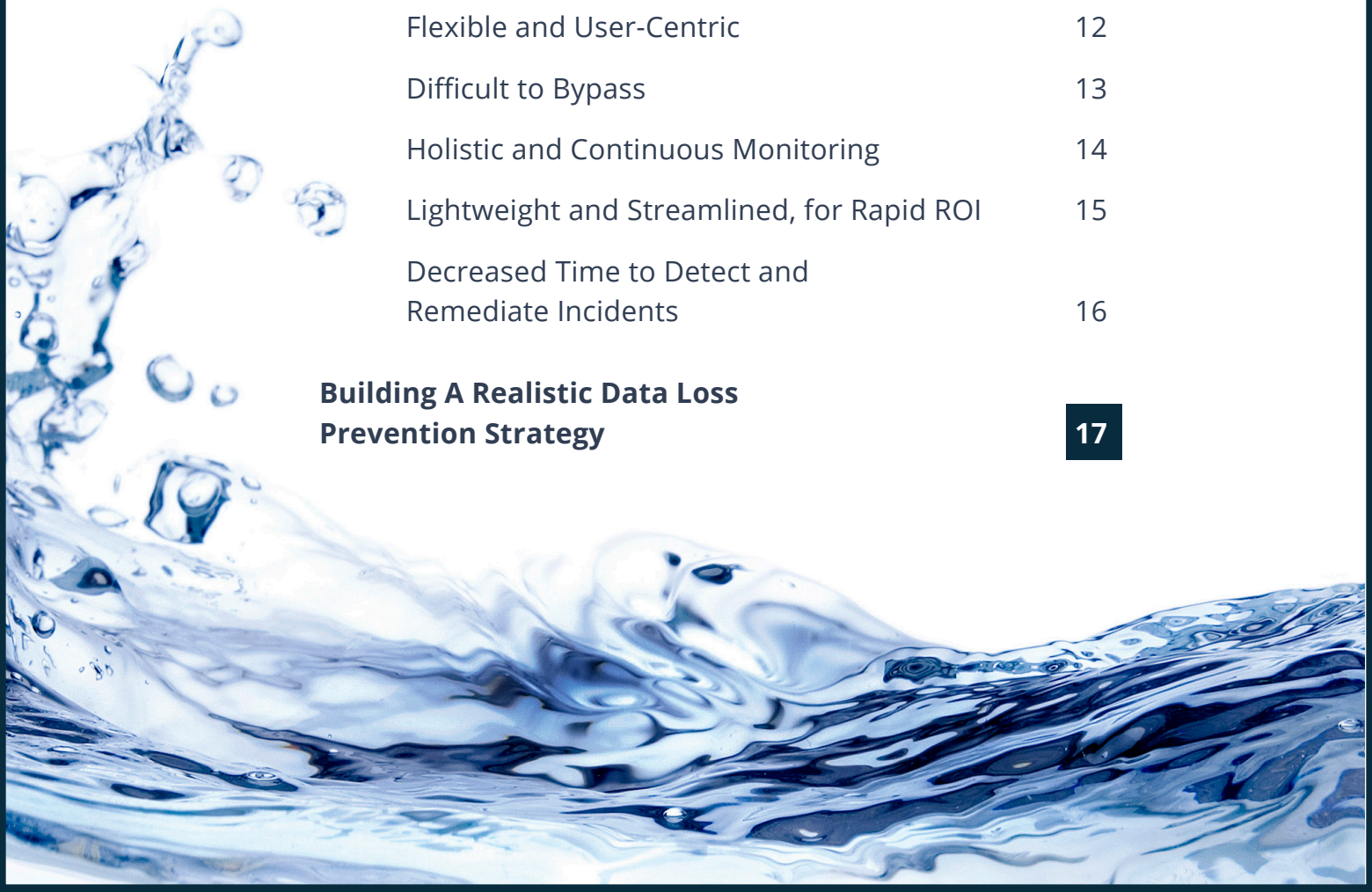
Building a Strategy for the Post-DLP World

How to Stem the Tide of Data Loss in the Modern Organization



observe it

Table of Contents



1. What is Data Loss Prevention?

3 million

Electronic records are stolen every single day

A whopping three million electronic records are stolen every single day. Data loss is a big problem, and has been ever since the dawn of the internet. The magnitude of the problem increases every day, as unstructured data grows—currently at a rate of 62% per year. Additional complexities related to data protection arise when organizations need to comply with standards like the new EU GDPR, SOC 2, PCI DSS, and industry-specific standards like HIPAA.

Every organization that deals with electronic data needs to have a data loss prevention strategy in place. Specifically, organizations need to know:

- Where does confidential or sensitive data reside?
- How is it being used and accessed?
- How can the organization prevent loss of this data?

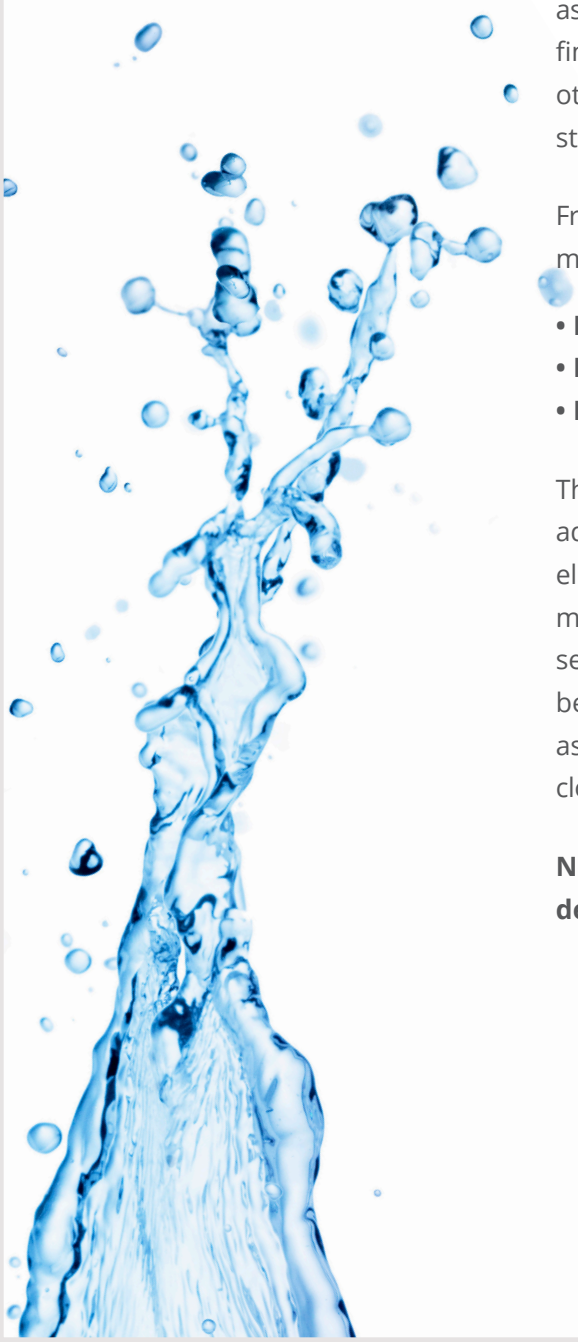
In this white paper, we'll take a look at how organizations have been dealing with data loss to date, why these strategies are failing, and what a better path forward looks like. We'll provide you with the information you need to build a data loss prevention strategy that works for the modern business.

1.

What is Data Loss Prevention?

The History of DLP

DLPs attempt to classify data, track it, and prevent it from leaving the organization via unauthorized channels



For years, data loss prevention tools (DLPs) have been the first line of defense against data leaving an organization's four walls. DLPs attempt to classify data, track it, and prevent it from leaving the organization via unauthorized channels. DLPs arose in direct response to compliance requirements, including PCI DSS, around 2005. So this type of technology is nothing new.

Over time, data discovery and classification features became an integral aspect of what DLPs offered. These features enabled organizations to find out what data they possessed and classify it based on sensitivity and other key factors. Next, DLPs started adding security features to actually stop data exfiltration attempts.

From here, DLP evolved into three different form factors (we'll elaborate more on these in the next section):

- **Endpoint DLP**
- **Network DLP**
- **Email DLP**

Then, as the cloud took hold and software-as-a-service became widely adopted, DLPs began to offer visibility into SaaS apps where many electronic records were now being stored. This capability provided a means of discovering and classifying data in the cloud. Next, cloud access security brokers (CASBs) appeared on the scene. CASBs are situated between an organization's on-prem infrastructure and the cloud, acting as a gatekeeper that lets the organization extend its security policies to the cloud (including their DLPs, in this case.)

Now that you have a sense of how DLPs evolved over the last decade-plus, let's take a look at what's under the hood.

1.

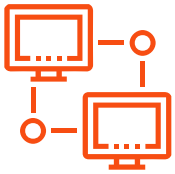
What is Data Loss Prevention?

How Data Loss Prevention Works

How a certain DLP solution works depends on its type and what it is designed to monitor and protect. DLPs are designed to offer data loss prevention by monitoring everything from cloud storage, to web proxies, to SPAN or Tap, depending on where in the system they sit.

Endpoint

Endpoint data loss prevention, the most prevalent form, works by deploying endpoint agents to desktops, laptops, and servers within an organization. Admins can then enable or customize policy templates based on their organizations needs and preferences. Once in place, the DLP begins to monitor and prevent confidential data from being copied or downloaded, whether end users are offline or online. If something inappropriate takes place, the system notifies both the employee and the IT admin or manager. The IT admin must then figure out how to remediate the incident and report on plans for risk reduction going forward.



Network

Similarly, **network data loss prevention** works by having admins enable or customize DLP policy templates. Then, when an employee or other user sends confidential data via the network, the monitoring tool detects the incident. Depending on how your DLP is set up, it can block the attempt, remove the user, and/or tag the activity for encryption. The system will then, much like endpoint DLP, notify the employee and IT admin. The IT admin must then figure out how to remediate the incident and report on plans for risk reduction in the future.

Email

Email data loss prevention is perhaps the most specific and niche type. Most organizations choose network or endpoint DLP, because they also monitor email. Similar to the other two types, email DLP looks for signs of data leaving an organization, sends up a flag, and places the burden of remediation on the IT team.

1.

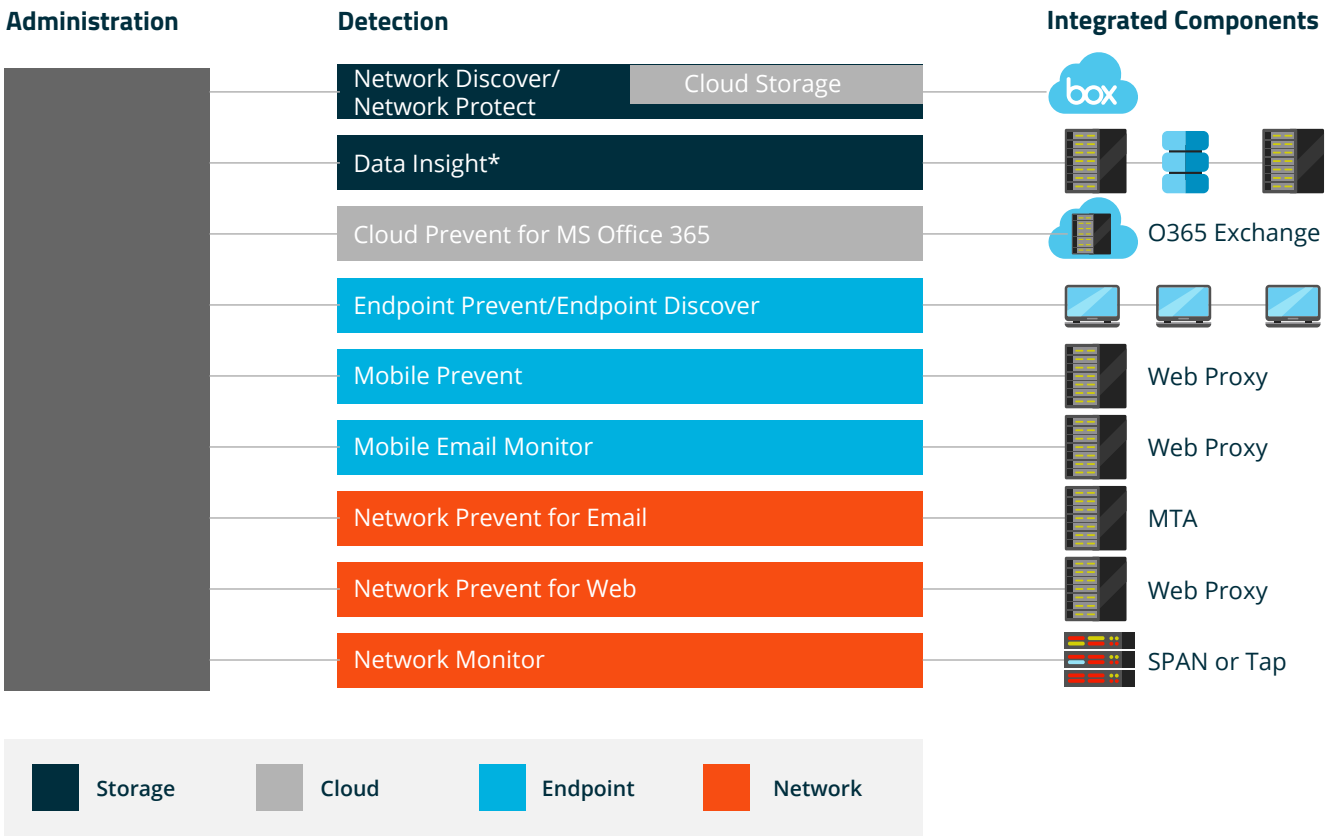
What is Data Loss Prevention?

How Data Loss Prevention Works

Data discovery often happens at the level of the endpoint, as does monitoring and blocking of out-of-policy behavior that could lead to exfiltration (such as USB storage, printing, and remote desktop access.) Monitoring and prevention are executed via protocols including SMTP, HTTP, IM, FTP, and TCP.

Below is a graphic illustrating a common DLP architecture:

Architecture Overview



Now that you understand the history of DLPs and how they work at a basic level, let's take a look at where things are going wrong.

2. How Legacy Data Loss Prevention is Failing Organizations

DLP tools aren't able to **stop insider threats** because they weren't designed to

While the idea of data loss prevention sounds great in theory and has worked relatively well in the past, research shows that successful DLP implementations are very rare. DLP as a tool has done a good job on the compliance front, which traces back to its origins as a technology. It allows organizations to classify data based on risk, which helps them check compliance boxes. However, DLP has failed miserably as a security tool—an area that is at least as, if not more, important than compliance.

Why don't DLPs work for security? To put it simply, conventional DLP tools that regulate the exchange of network data are aren't able to stop insider threats because the tools weren't designed for that purpose. According to Gartner, DLPs simply don't protect all data or cover all loss scenarios.

Additionally, DLPs are a pain to administer and maintain. Organizations struggle with their heavy kernel-based agents, the time-consuming data classification process, ongoing maintenance, and disconnects between data owners and DLP administrators.

Now, let's take a look in depth at these challenges and limitations, which illustrate how DLPs are failing the modern organization.

2.

How Legacy Data Loss Prevention is Failing Organizations

Classification Challenges in the Era of Unstructured Data

By 2022, **93% of all data** will be unstructured

Detecting and preventing the loss of data was a lot easier when there was less of it. Today, data discovery and classification is a very onerous process, because unstructured data grows every day. In fact, by 2022, it's expected that 93% of all data will be unstructured. There's no easy way to apply a data classification scheme when new documents, records, and pieces of data are created by the minute.

While it's true that some organizations must classify their data in order to meet compliance mandates, data classification as a means to secure systems and prevent loss is not a winning strategy.

To illustrate how data classification challenges arise and why they lead to security gaps, let's take a look at an example. Say a security or IT administrator at a large enterprise is tasked with classifying data across the organization. This person's job is to know what's going on with data at a granular level across the entire company—from marketing, to development, to operations and beyond. To do the job properly, the admin would have to reach out to each line of business not just daily but hourly and even up to the minute to find out which files are sensitive and classify them. With new documents being created all the time and unstructured data growing exponentially, this method is completely unrealistic.

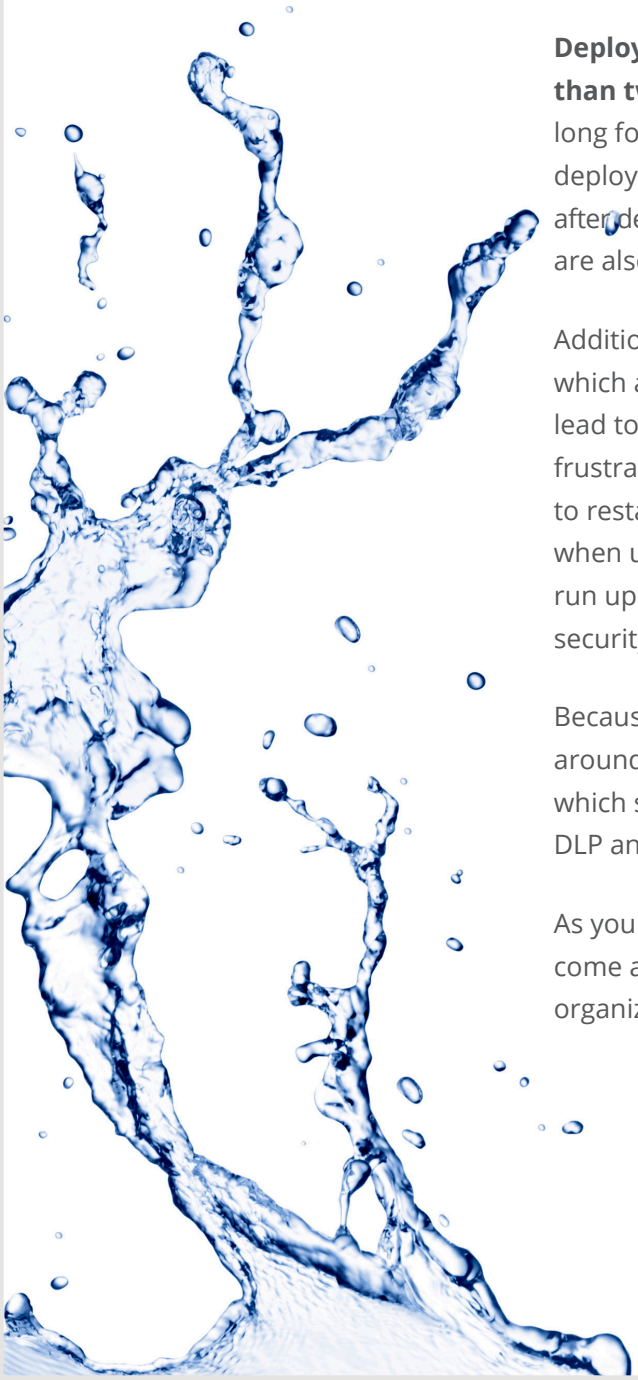
Because perfect data classification is an impossible goal, data-centric DLP schemes are failing to protect today's modern business against data loss. DLPs have proven to be ineffective at detecting and preventing data loss in today's fast-paced, data-rich organizations.

2.

How Legacy Data Loss Prevention is Failing Organizations

Operational and Maintenance Hurdles

There are also quite a few operational and maintenance challenges that accompany the deployment and ongoing usage of DLPs. As a result, many organizations that deploy enterprise DLP systems struggle to move beyond the beginning phases of discovering and monitoring data, as Gartner has pointed out.



Deployment itself can be very complex, in many cases taking more than two years to fully complete. As you can imagine, that's far too long for a competitive business today. For this reason, incomplete DLP deployments are common, and many administrators complain that, even after deployment, fine-tuning alerts is a never-ending process. False positives are also common, which adds to the operational burden of running a DLP.

Additionally, DLPs are well-known for their heavy, kernel-based agents, which are quite taxing on endpoints—and thus on end users. They often lead to system and app crashes, which can slow down productivity and frustrate users. It's common for users to be forced to interrupt their days to restart machines after DLP-caused crashes. Security gaps can arise when users attempt to bypass DLPs for this reason. Finally, DLPs may also run up your organization's machine overhead and even conflict with other security tools like antivirus software.

Because of these headaches, DLP agents often acquire a bad reputation around the organization, encouraging employees to skirt them altogether, which stokes conflict between the security or IT admins who manage the DLP and end users.

As you can probably tell, the operational and maintenance burdens that come along with DLPs often make them frustrating and impractical for organizations who want to run a lean, streamlined business.

2.

How Legacy Data Loss Prevention is Failing Organizations

Lack of Insider Threat Detection and Response

"I haven't seen an enterprise DLP my team can't bypass in a matter of seconds."

CISO, Major Global Financial Services Organization

Additionally, 60% of all data leaks are carried out by insiders, with an estimated $5 million in costs per insider-caused security breach. Data classification schemes can't do much to identify risky behavior, which is why DLPs often miss indicators of insider threats.

Moreover, DLP tools that work by regulating the exchange of network data are not designed to successfully catch or stop insider threats. They simply weren't designed to do so.

As we mentioned above, if an insider knows how the DLP is implemented (which many technical users do), they are likely to be able to bypass it. In fact, one of ObserveIT's customers, the CISO at a major global financial services organization, told us, "I haven't seen an enterprise DLP my team can't bypass in a matter of seconds." That can spell real trouble if you're relying on your DLP to monitor and stop data loss.

On top of being ineffective at catching insider threats and easy to bypass, **DLPs also lack user activity monitoring and context about the movement of data, which means they have no investigational capabilities**. They do not offer any visibility into what happened before, during, or after a data exfiltration incident. Without these types of actionable forensics, DLPs can actually drive down the mean time to detection and response for an organization, as admins must spend their time painstakingly correlating logs to try to figure out what happened.

These shortfalls are obviously major problems and illustrate well how DLPs are failing today's organizations.

In the next section, we'll talk about an ideal future state in which security teams are able to effectively detect, prevent, and stop data loss.

3. A Vision for the Post-DLP World

"By 2020, **85% of organizations** will have implemented some form of integrated DLP, up from 50% today."

Gartner Report

As Gartner's report, "It's Time to Redefine Data Loss Prevention," clearly illustrates, it's time to take a more holistic approach to identifying and stopping data loss. Data protection needs to be built into all organizations' security and compliance strategies from day one, and it needs to be executed in a way that takes the rapid proliferation of data and complexity of today's technological landscape fully into account.

DLPs on their own are not up to the task. So what does a post-DLP world look like? What types of tools and technologies do teams need to invest in to fully protect their data against all types of loss, including insider threats? Let's take a look.

3.

A Vision for the Post-DLP World

Flexible and User-Centric

User-centric strategies focus more on behavior than data classification

First of all, **data loss prevention strategies need to be flexible and user-centric**—as opposed to rigid and data-centric, the way DLPs are today.

Flexible prevention policies, rather than static data classification schemes, track files in use, in motion, and at rest. They identify common exfiltration points like file-copying, USB drive usage, printing, cloud storage (especially personal cloud storage) and emailing with or to personal accounts. All of these actions are likely indicators of data loss in progress. Applying a flexible rubric like this, rather than one that demands a static data classification scheme, is more likely to catch threats.

To put a fine point on it, user-centric strategies are focused more on user behavior than on data classification. They don't focus so much on carefully cataloging which pieces of data are sensitive or at risk. Instead, they look for likely indicators of compromise.

To achieve the goal of being more flexible and user-centric, a tool like ObserveIT comes equipped with a built-in insider threat library. This out-of-the box library of alerts enables prevention around the 200 most common insider threat indicators. This library contains a list of common user behaviors that indicate potential data compromise, and can be used for real-time capture and alerting whenever user behavior indicates risk.

3.

A Vision for the Post-DLP World

Difficult to Bypass

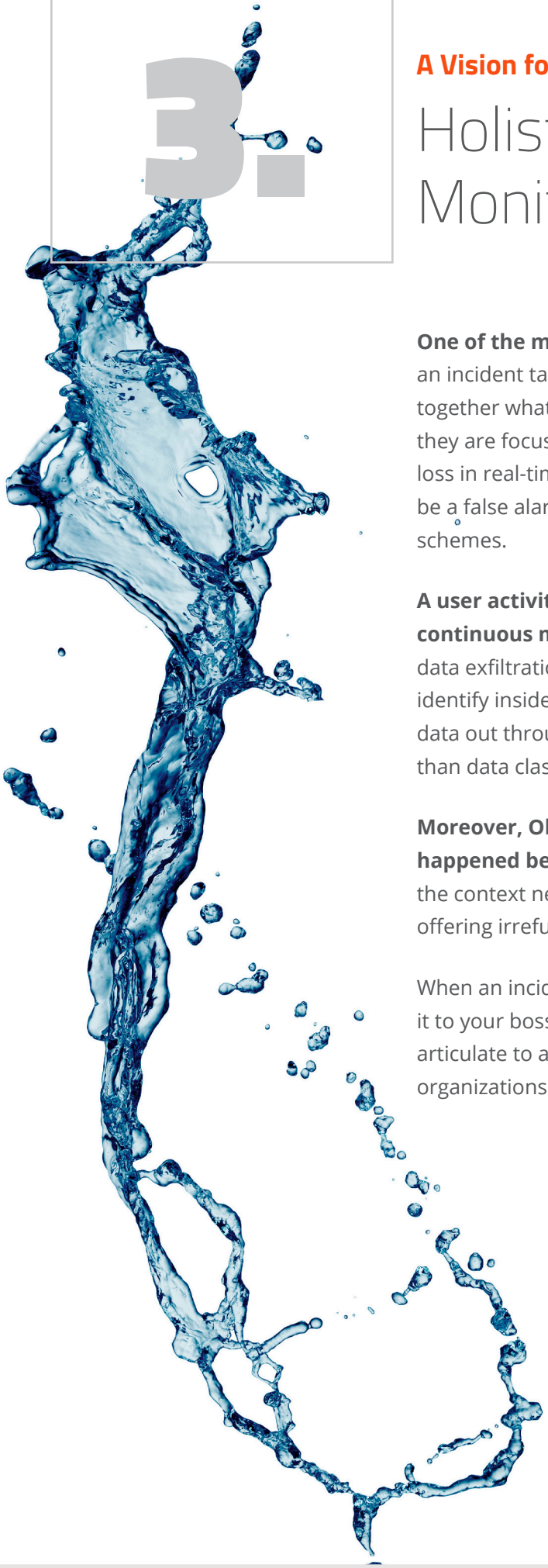
The strongest data loss prevention tools have **user education built right in**

Additionally, you want to invest in tools that are difficult for users to bypass. If a DLP is onerous to use, then innocent and well-meaning users may discover a way to get around it, leaving you open to accidental data loss. If a user has more malicious intentions, then the ease with which they can bypass a DLP opens you up to intentional data exfiltration as well. As headlines illustrate, sensitive data can command a high price on the black market, tempting employees into selling it for personal gain.

The ease with which technical users are able to bypass DLP makes it a no-go for organizations who need a tool they can depend on to keep data secure.

A tool like ObserveIT, on the other hand, has a watchdog mechanism built in that makes it very difficult for users to kill the agent. If they do, the agent automatically restarts itself to ensure that it is always up and running. It also contains a self-monitoring system, so if a user does try to shut down the agent, an admin will be alerted immediately and can take action to prevent further risky behavior—whether intentional or accidental.

The strongest data loss prevention tools also have user education built in, so that employees and other users who try to act out of policy are not only immediately blocked from doing so, but also provided with information about what they are doing wrong. In some cases, this step acts as a deterrent against intentional data theft, but in many cases it simply serves as a helpful and in-context reminder of how to avoid putting the organization at risk. This knowledge contributes to an organization's overall security and decreases the likelihood of a data loss scenario taking place.



A Vision for the Post-DLP World

3. Holistic and Continuous Monitoring

One of the major downsides of DLPs is that they only monitor logs. If an incident takes place, admins must sift through log files and try to piece together what happened with little to no context. Additionally, because they are focused on logs, DLPs are often not able to alert admins to data loss in real-time, and even if an alert does fire, it's quite common for it to be a false alarm due to the sensitivity and inaccuracy of data classification schemes.

A user activity-centric tool like ObserveIT provides holistic and continuous monitoring. It monitors user activity in depth, looking at data exfiltration points like cloud apps, USB insertions, and print jobs to identify insider threat indicators. It looks for examples of users taking data out through unauthorized channels, which is much more practical than data classification in terms of identifying real threats.

Moreover, ObserveIT is able to offer a holistic view of what happened before, during, and after an incident. This step provides the context necessary to respond quickly and accurately to the threat, offering irrefutable evidence of exactly what took place.

When an incident occurs, what would you rather have on hand to explain it to your boss? Low-level log files or a holistic picture that is easy to articulate to anyone in the organization? Yet again, DLPs simply can't keep organizations secure.

Gain a holistic view of what happened before, during, and after an incident.

3.

A Vision for the Post-DLP World

Lightweight and Streamlined, for Rapid ROI

Time to value is of critical importance for IT and security teams

As we explained in detail earlier, DLPs are difficult to deploy and fine-tune and their agents are heavy on the endpoint, leading to bluescreens, crashes, and failures that make it hard to get work done.

A modern data loss prevention strategy needs to be lightweight, with minimal impact on endpoints. It all starts with deployment. A tool like ObserveIT has a silent install and does not require a reboot to get going, meaning it takes just a few days to completely deploy—vs. up to two years with a traditional DLP.

Additionally, as compared to a kernel-based DLP agent, **ObserveIT runs in user mode with little to no impact on the end user.** In most cases, users won't even realize ObserveIT is there, given its 1% CPU impact to end users and ability to run in full stealth mode. The lightweight agent resolves performance issues, which means that users won't be looking for ways around it (and, as we mentioned earlier, it's much more difficult to bypass than a traditional DLP.)

ObserveIT altogether eliminates time-consuming troubleshooting and maintenance processes that go hand-in-hand with DLP, meaning you can realize a rapid return on investment, rather than sinking years of administrators' time and energy into an incomplete DLP deployment.

Time to value is a key metric for IT and security teams, since they are often seen as cost centers by the larger business. **ObserveIT is able to complete a standard proof of concept in an hour**, with a full pilot taking no more than one to two weeks before administrators are able to realize the value of deployment.

3.

A Vision for the Post-DLP World

Decreased Time to Detect and Remediate Incidents

When addressing a data loss incident, **contextual insights** are essential for investigation and remediation

Finally, as we have touched on briefly above, DLPs fall behind when it comes to actually remediating a data loss incident. By their very nature, they are not able to provide context or investigational capabilities. In practice, while a DLP might alert you to an incident, it won't help you do anything about it.

To actually address a data loss incident, user activity-centric detection and investigation tools are necessary. A tool like ObserveIT provides the sort of context that is necessary to rapidly detect and remediate incidents, driving down mean times to resolution. ObserveIT reduces incident response times, often even catching an insider-caused incident in progress (which can slip right past DLPs), because it is laser-focused on actual indicators of compromise.

Moreover, because ObserveIT is easily integrated into a broader security ecosystem, it decreases security teams' workloads by providing necessary context when it's time to conduct forensics. Combing through log files from a DLP can only slow down incident response times, and in today's climate of frequent and business-endangering breaches, that kind of lost time is difficult to afford.

4. Building A Realistic Data Loss Prevention Strategy

Data loss is not a systems problem—**it's a people problem**

To sum it up, today's security and IT teams are looking for a new way to stop data loss because current DLP solutions have proven time and time again to be ineffective. Many teams have also recognized that complete data loss prevention may not even be attainable, which calls into question the value of investing in a traditional data loss prevention solution. At ObserveIT, we believe complete data loss prevention is an unrealistic expectation and that modern security teams are—and should be—shifting away from prevention to detection and response.

Data loss is, at its core, a people problem—not a systems problem. This means the best strategy to identify, stop, and remediate data loss incidents is one that puts user activity at its center.

Proactive security organizations recognize that DLPs are failing for all of the reasons that we have explored in this paper. They may help you check compliance boxes, but they aren't able to protect against insider threats and other common causes of data loss, nor are they sufficient to the tasks of investigation or response. The way forward is to adopt a new security paradigm altogether, one that is user-centric, holistic, and streamlined. Only when organizations begin to invest in strategies that take today's enormous and complex technological landscape fully into account will we begin to see a decrease in data loss.

Ready to bring your data loss prevention strategy into the modern era?

Test Drive ObserveIT Today