Overcoming Enterprise Data Protection Challenges

paloalto® NETWORKS

Table of Contents

Data Protection for the Modern Enterprise

Data has evolved rapidly in recent years. The volume, velocity, and movement of data outside typical corporate boundaries, as a consequence of cloud computing and remote working, have irrevocably changed the data landscape. As a result, data protection strategies are difficult to execute and often ineffective due to the fragmented and manual nature of legacy data protection solutions.

As painful as they are, these legacy solutions are better than nothing. After all, suffering a data breach or compliance penalty can severely harm a business. Organizations continue to utilize their existing solutions, spending extra time, money, and effort to solve a complex problem.

A cloud-delivered enterprise DLP service easily scales for effective, consistent data protection across every network, cloud, and user.

What organizations need is a data protection solution built for today's modern data—a modern architecture that is easy to deploy across the entire organization, that consistently discovers and safeguards all sensitive data no matter where it lives or flows. This e-book explains how a consolidated data loss prevention (DLP) solution can make data protection easier to manage and ensure your data remains secure.

Data Protection Requirements

Today's resource-constrained organizations need a modern DLP solution that can do it all, from safeguarding against external threats to maintaining compliance, protecting intellectual property (IP), stopping malicious outsiders, and preventing user errors.

Safeguard Against External Threats

Data protection and security are not one and the same. For example, anti-malware, firewalls, and intrusion prevention systems (IPS) protect data indirectly by preventing intruders or malware from entering a network. Organizations need a modern DLP solution that explicitly addresses the risk of a data breach as well as monitors and stops unsafe data movement and sharing.

Maintain Regulatory Compliance

Data privacy and compliance requirements are growing increasingly complex as industries, governments, and standard-setting bodies establish their own criteria for protecting regulated data. Regulatory bodies raise the stakes with fines and other penalties that can have a significant impact on an organization. A modern DLP solution must facilitate the organization's regulatory compliance efforts—not add to the burden.

Protect Intellectual Property

No doubt your customers' data is valuable; however, so is your IP. A modern DLP solution must apply the same protective rigor to your copyrights, patents, trademarks, and trade secrets that it does to sensitive or personally identifiable information (PII).

Stop Malicious Insiders

Users with privileged access present a significant risk to an organization. They can abuse their access to steal data or share their access credentials with unauthorized individuals. This type of risky activity is difficult to spot because access appears to be coming from an authorized source with a legitimate use case. A modern DLP solution must help organizations identify the activities that are affecting sensitive data and stop malicious insiders from putting that data at risk.

Prevent User Mistakes

Malicious actors are not always the source of data loss. In fact, well-meaning employees often engage in behaviors that inadvertently put corporate data at risk—for example, sharing confidential documents openly on cloud applications or transmitting corporate secrets via personal email accounts. A modern DLP solution must account for unintentional data exposure as well as educate employees on corporate data security policies as a means to mitigate careless behavior and minimize the risk of data loss over time.

Data Protection Challenges

Addressing these multiple requirements with a traditional data protection solution is difficult. Making it even more challenging is the diversity of sensitive data.

Data is everywhere. It's in your data center, on users' laptops and smartphones, and of course, increasingly stored and used in the cloud. That said, even the cloud isn't a single place. People use a variety of software-as-a-service (SaaS) applications, and organizations often utilize various public cloud platforms to store and share sensitive data. It's not uncommon for an organization to run a shadow IT report and discover myriad unsanctioned cloud applications in use.

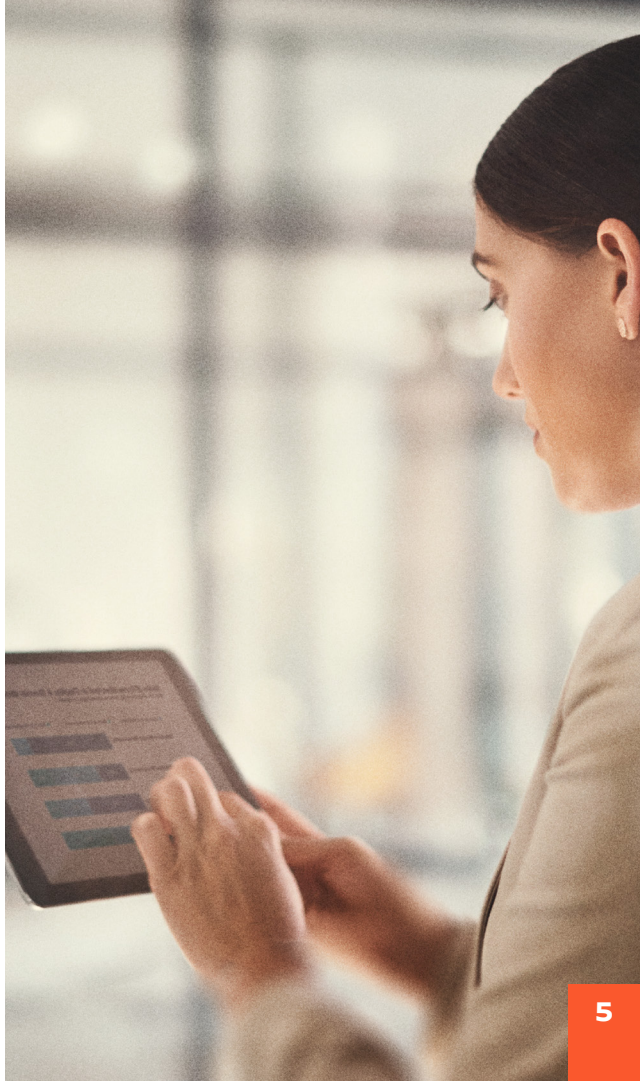
With remote work becoming the new normal, sensitive data is even more susceptible to flowing outside the typical IT-managed premises of an organization. Today, home offices have become a legion of remote sites, leaving IT teams without visibility or control over how employees use or store sensitive and personal data.

According to Gartner, the year-over-year data security spend in 2020 is expected to grow by 7.2%. Can legacy DLP approaches champion the growing need for innovative data security?

Left with new and unexpected challenges, how can IT teams protect this data?

Data is shared and transmitted across many different channels. It is constantly on the move. From mail servers, file sharing apps, cloud email, social media, USB drives, and Bluetooth to mobile phones tethered to laptops, the options for transmitting data are endless, and many of them are outside of IT's purview. Organizations need a way to monitor the transfer of data both within and outside of the organization.

Bottom line: without visibility into your sensitive data, protecting it becomes very challenging.



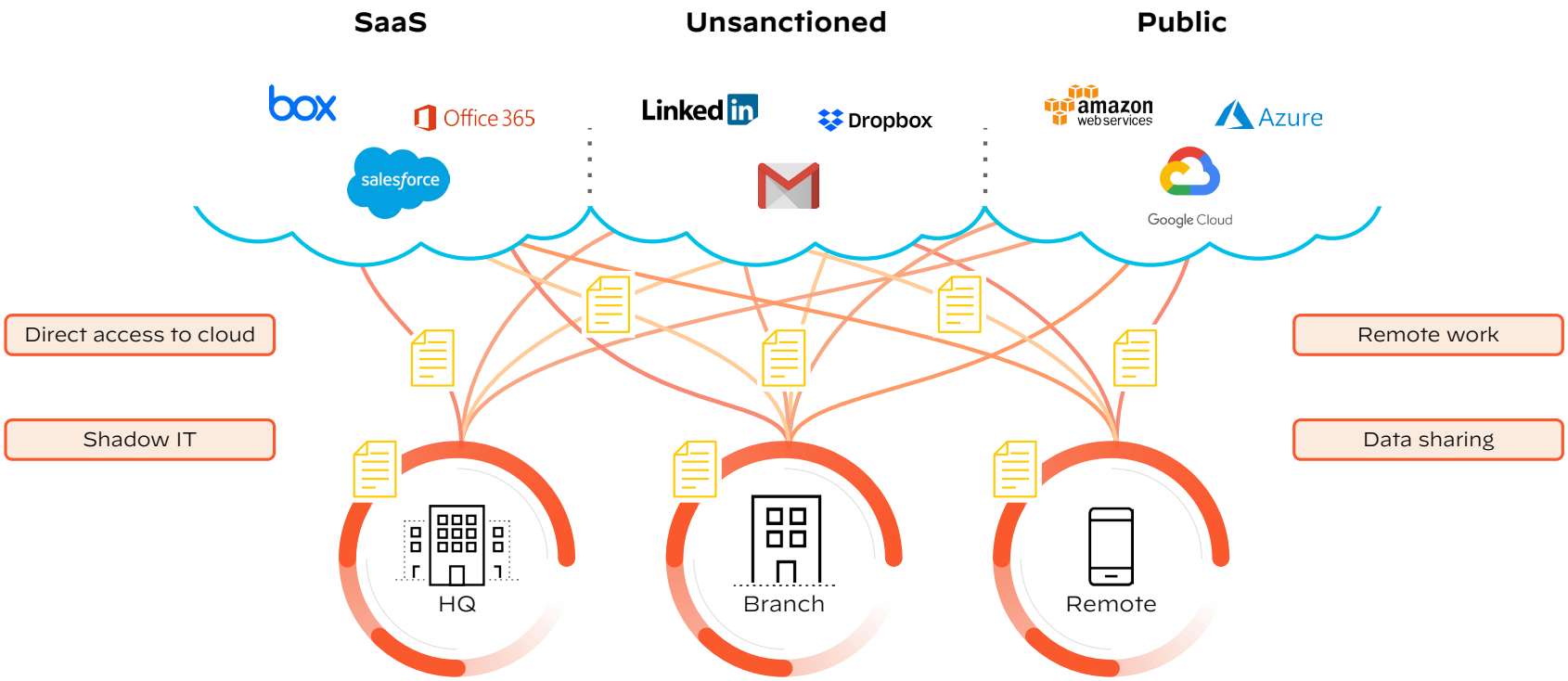


Figure 1: The modern, highly distributed enterprise

One-Size Legacy Data Protection Solutions Don't Fit All

No single DLP solution fits the needs of every enterprise. Security providers must offer customers both the ability to tune policies and the flexibility to adapt configurations and deployments to meet their specific needs. Such processes are usually lengthy, ongoing, and resource-intensive. The consequence of this complexity is that DLP solutions are only suitable for the largest enterprises, which can afford significant investments in time, people, and money. As for the majority of organizations, legacy DLP solutions are inapplicable or provide minimal protection because their extensive capabilities are too complex to use and maintain.

That doesn't stop providers from trying. Let's take a closer look at three common data protection solutions available today and their shortfalls.

Data Protection Option No. 1: Legacy DLP

Legacy DLP solutions are based on technology that was created more than a decade ago and hasn't evolved much since. In fact, newer functionalities have been built on top of old engines that are unsuitable for modern enterprises. Most of these solutions were built and still run on-premises, so IT organizations are forced to maintain the infrastructure and bear its cost. They are also constantly charged for add-ons and must continuously fine-tune the solution manually to reduce myriad false alerts and address newer use cases. Most recently, to embrace the cloud adoption, some legacy DLP technology providers simply performed a "lift and shift," essentially transferring the problems from the customers' premises to the cloud.

There's a lot involved in the setup and maintenance of legacy DLP solutions. Creating and fine-tuning policies requires manual processes that cost the organization time and money. Manual processes also introduce the risk of human error.

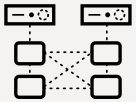
To further complicate matters, protecting the various repositories and channels requires bolt-on solutions such as on-premises scanners, repository agents, and cloud API scanners, adding to the operational overhead needed to maintain the solution.

Protecting data through transmission channels and protocols requires bolt-on solutions as well, including:

- On-premises proxy
- On-premises MTA
- Cloud proxy
- Cloud MTA
- Agents
- Plugins
- Document repositories

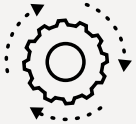
Enterprise DLP provides very granular configuration options, but data detection and classification must be fine-tuned manually.

The downside of maintaining a legacy DLP solution:



Multiple components that are complex to deploy and manage

Inconsistent and difficult scaling



Lengthy and taxing software updates

High total cost of ownership (TCO)

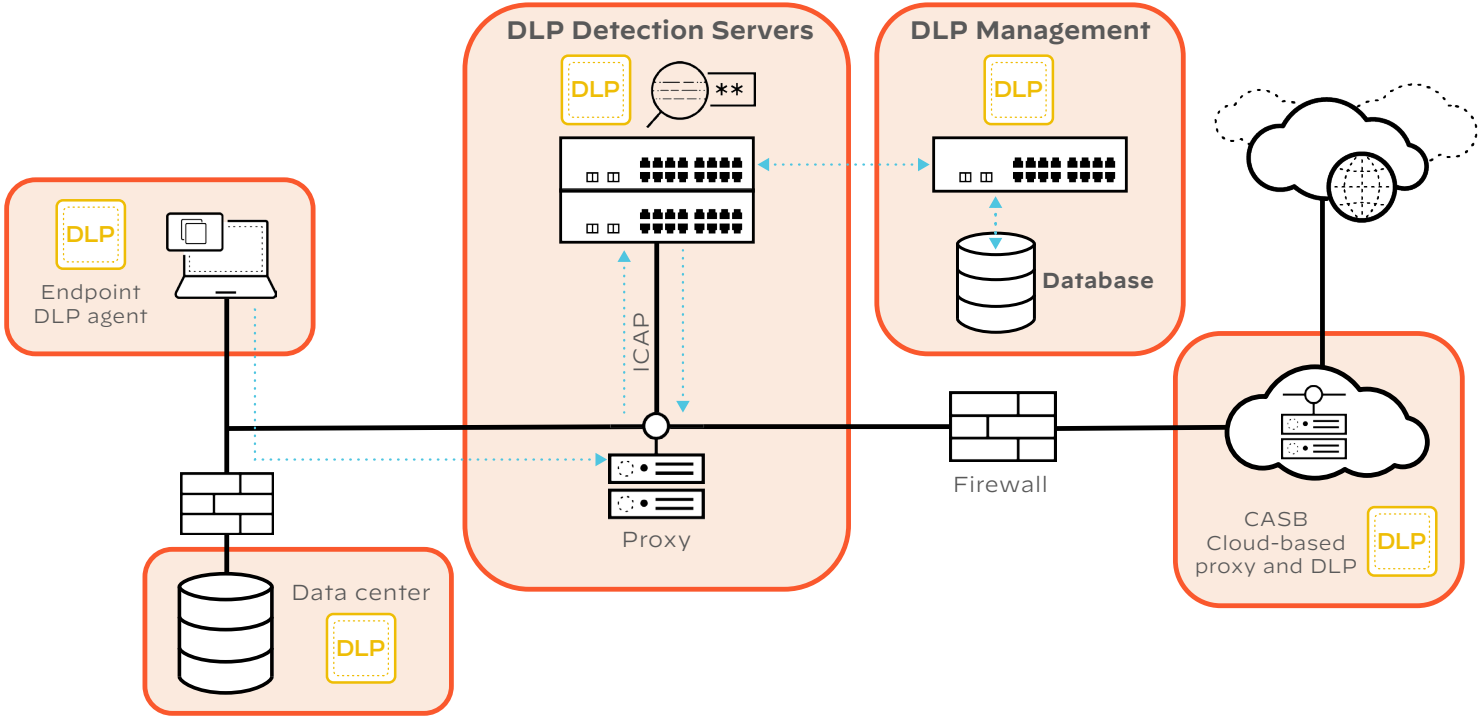


Figure 2: Complex DLP architecture—no longer sustainable

Data Protection Option No. 2: Embedded DLP

Given the difficulty of maintaining a legacy DLP solution, some data protection providers and even service providers have attempted to simplify their solutions (and succeeded, to some extent) by tightening their focus. Instead of trying to protect every channel or control point and every data repository, DLP providers began embedding data protection in single security control points, or channels, such as email, web, endpoint, and cloud apps. This certainly made their job easier. However, the one—and only—benefit that embedded DLP solutions offer to customers is a reduced barrier to adoption, resulting from a lower initial cost.

Unfortunately, the benefit is overshadowed by a significant problem—or dozens of them, depending on how you look at it. With embedded DLP covering only one data channel, organizations still have dozens more to protect, and it only takes one hole to sink the boat.

With embedded DLP covering only one data channel, organizations still have dozens more to protect, and it only takes one hole to sink the boat.

Data Protection Option No. 3: Multiple Embedded DLP Solutions

Organizations that deploy one embedded DLP solution have little choice but to deploy another ... and another, and another ... until all the data channels and repositories are protected.

Enabling DLP through disparate security control points from different vendors means having to deal with different DLP approaches. It takes a great amount of work to fine-tune disjointed policies and align them for a consistent approach to data protection. Specifically, each solution has its own management console, policy language, and data classification system. None of the solutions "talk" to each other, requiring organizations to manually connect data in order to gather accurate reporting. With the addition of each new embedded DLP solution, the risk of human error increases.

The adoption of multiple embedded DLP solutions from different providers can be an administrative nightmare!

Each solution has its own management console, its own policy language, and its own data classification system.

Cloud Enterprise DLP to the Rescue

It's time for a new approach. Organizations need a fresh solution that meets their data security and compliance requirements without complexity and overcomes the challenges of protecting data in the modern distributed enterprise.

But how?

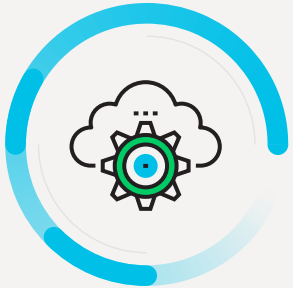
A modern cloud-delivered DLP solution is more than a product. It's a comprehensive strategy that transforms how, when, and where DLP is employed. It provides organizations with four key benefits:

1. High efficacy—ensures new protections and updates are applied the instant they are released with "zero delay," unlike legacy solutions that require multiple manual steps and take months to apply.

2. Comprehensive coverage—discovers, monitors, and protects all sensitive data across physical and virtual networks and clouds—including SaaS at rest, SaaS inline, and cloud native IaaS—and every user, whether on campus, at branch locations, or working remotely.

3. Easy deployment—serves as a single cloud service activated by a license in all existing Next-Generation Firewall and Prisma® Access control points for easy deployment designed to scale across the enterprise in minutes, not months.

4. Cost-effective—natively integrates into all existing control points to lower your TCO by three times more compared to legacy products. There's no need for additional proxies, servers, or databases—prevent data loss with just a cloud subscription.



Cloud-delivered DLP takes a comprehensive approach to data protection—one that makes all sensitive and confidential data easier to manage and easier to secure, no matter where it lives or where it flows.

Enterprise DLP, Simplified by Palo Alto Networks

Enterprise DLP by Palo Alto Networks is the industry's most comprehensive cloud-delivered enterprise DLP. It discovers, monitors, and protects sensitive data—such as customer and employee PII and your organization's proprietary IP—across every network, cloud, and user. The solution is designed to offer consistent data protection at scale automatically, everywhere, through a unified cloud service.

Our solution natively integrates with your existing Palo Alto Networks Next-Generation Firewall, Prisma SaaS, and Prisma Cloud to easily enable data protection and compliance throughout your entire enterprise in minutes, not months. Cloud-delivered architecture applied new protections and product updates the instant they are released, ensuring effective data protection and zero-delay updates, compared to months for legacy vendors anchored by on-premises infrastructure and manual software provisioning. Policies are created once and instantly applied to sensitive data—at rest, in motion, or in use—wherever the data resides. Thanks to advanced supervised machine learning, policy tuning and incident response workflows are extremely simple.

Our Enterprise DLP is simple to adopt, use, and maintain. You won't have to bring in additional deployments of software, proxies, consoles, or IT resources—**lowering your total cost of ownership by three times more compared to legacy products!**

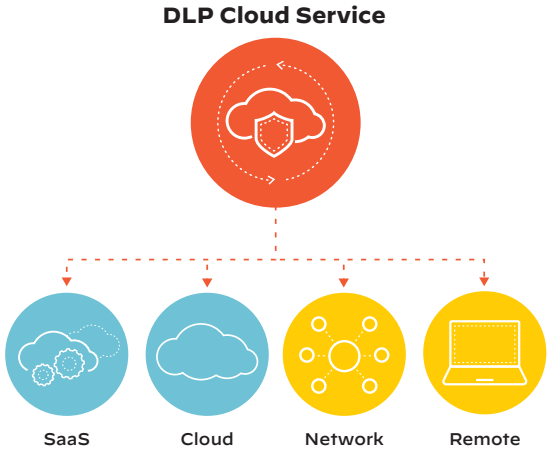


Figure 3: One cloud-delivered DLP service for easy adoption, consistent protection, and scalability

Conclusion

Traditional DLP solutions were not designed with workforce mobility and the cloud landscape in mind. As enterprises continue on the path to digital transformation in the foreseeable future, problems with complexity, administrative effort, and partial protection of sensitive data will only become exacerbated.

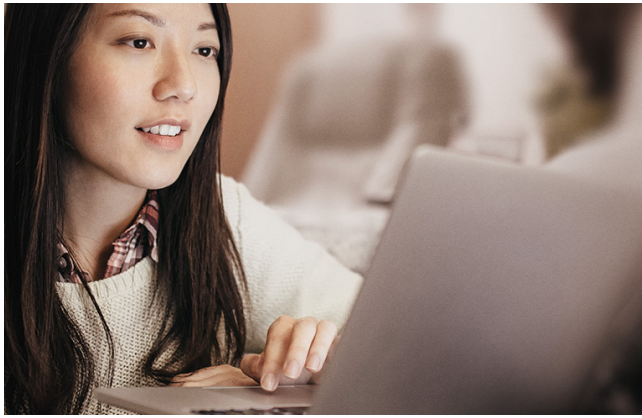
A modern cloud-delivered DLP solution enables a more comprehensive and effective data protection approach. When natively integrated with Next-Generation Firewalls or delivered as part of a secure access service edge (SASE), it enables your organization to continuously and consistently protect all sensitive data across networks, clouds, and users regardless of location.

As your organization continues its cloud transformation journey, consider not only how a modern firewall-attached DLP solution can help meet your data protection needs, but also how a SASE solution can provide a holistic view of your entire network from a single unified, cloud-delivered service.

Next Steps

Find out how a modern enterprise DLP solution can protect and secure your company data, no matter where it flows or where it is located.

Learn more →



paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com