Enterprise Data Loss Prevention

Preventing the Risks of Data Loss and Noncompliance in Highly Distributed Modern Enterprises

Every organization must protect its reputation from the threat of data breaches. In the modern world, keeping sensitive data, such as personally identifiable information (PII) and intellectual property (IP), safe and private is more challenging than ever. New trends and data usage models affect data visibility and control. As enterprises adopt cloud-based services and their users become more mobile—working from home and utilizing public connections while embracing new data-sharing models—sensitive data becomes more vulnerable to theft as well as prone to both intentional and unintentional exposure.

Preventing threats is one aspect, but organizations also need to explicitly address the risk of a data breach by monitoring and stopping unsafe movements of data that is highly sensitive.

Business Benefits

- Comprehensive coverage to discover, monitor, and protect all sensitive data across every network, cloud, and user.
- High data protection efficacy with persistent protection and zero-delay updates provided by cloud-delivered DLP.
- Easy deployment, natively integrated into existing control points, enabled throughout the entire enterprise in minutes.
- The most cost-effective enterprise DLP, with the lowest TCO compared to legacy products.

While the number of data breaches rises, so does the number of data privacy and compliance requirements. Most recently, the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) have raised the stakes with fines that can have a significant impact on any business.

Current data protection solutions are complex to deploy, hard to manage, limited in coverage, and lacking in reliable features.

Organizations need an innovative data protection solution for their modern networks—one that supports their cloud and network transformations, minimizes the risk of data breaches across every threat vector, and helps regulate unsafe and noncompliant data exposure and sharing practices.

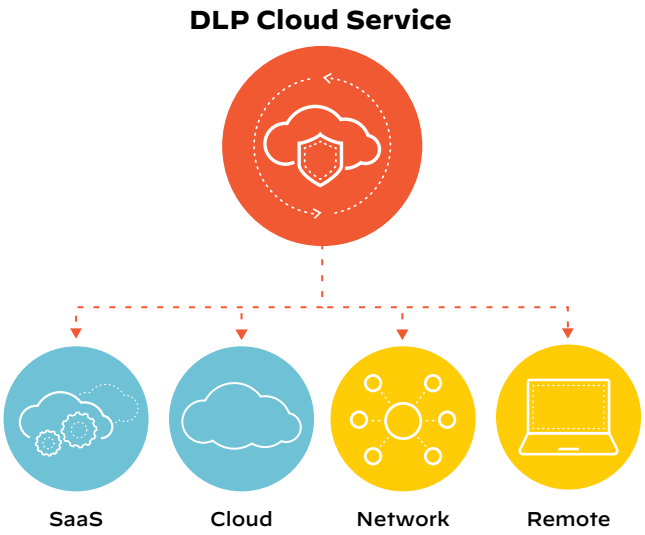

Figure 1: One cloud-delivered DLP service for easy adoption, consistent protection, and scalability

Key Capabilities

Data Security Everywhere, with a Cloud-Delivered Architecture

Enterprise DLP by Palo Alto Networks is the industry's most comprehensive cloud-delivered enterprise data loss prevention solution that discovers, monitors, and protects sensitive data across every network, cloud, and user. A single cloud service and predefined policies deliver data privacy and compliance easily and consistently, whether on-premises, across remote workforces, or in the cloud. Natively integrated with an organization's existing security control points, Enterprise DLP lowers TCO by three times more compared to legacy DLP products by simplifying deployment and maintenance as well as eliminating the need for additional infrastructure (e.g., server deployments, proxies, software, databases, consoles, and appliances).

Customers get reliable discovery of their sensitive data, comprehensive control and consistent protection everywhere data is, whether it's at rest or in motion.

Consistent Policy Delivered by a Single DLP Engine

Implementing comprehensive DLP across an entire organization often requires customers to author and manually maintain policies in each environment, such as endpoints, networks, and clouds. Inconsistent policies produce incomplete protection, security blind spots, and shadow IT while demanding time-consuming policy management cycles.

The Palo Alto Networks Enterprise DLP engine is centralized in the cloud, so data protection policies and configurations can be defined anywhere and automatically applied to all control points, wherever the data is. There is no need to reinvent the wheel every time your organization adds branch offices or users, adopts new software-as-a-service (SaaS) applications, or embraces multi-cloud infrastructure. Existing cloud-only data protection solutions are too limited in coverage, producing an ineffective leakage prevention.

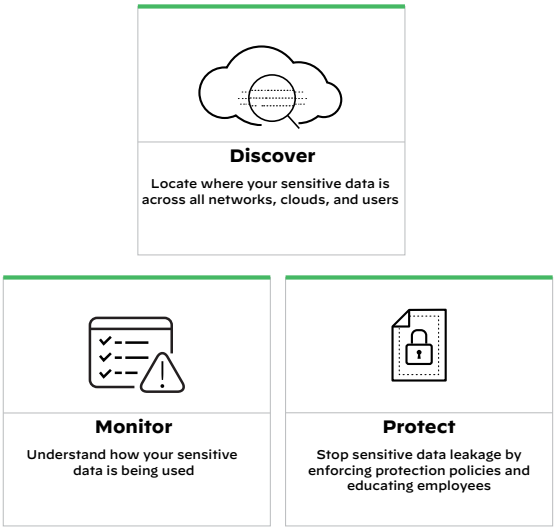

Figure 2: Fundamental DLP capabilities

Easy to Deploy, Update, and Scale

Many organizations face the reality that legacy DLP has become too complex to deploy and manage, inconsistent at scale, expensive, and resource-intensive—and therefore impractical to operate and sustain. This is because legacy DLP solutions are anchored by their on-premises infrastructure and scale using a costly bolt-on approach.

Palo Alto Networks Enterprise DLP is delivered from the cloud across network inline, SaaS at rest, SaaS inline, infrastructure as a service (IaaS), branch offices, and remote workforces. It doesn't need proxies, ICAP and additional infrastructure because it's natively integrated as a service into the Palo Alto Networks existing control points. Unlike legacy DLP solutions, it simply deploys and scales across the entire enterprise in minutes, not months. The cloud-delivered architecture of Palo Alto Networks Enterprise DLP also ensures that new protections and product updates are applied the instant they are released.

Comprehensive Data Protection

Today's cloud landscape forces organizations to maintain control of their data in SaaS applications as well as public and private clouds. Various security offerings may already provide some of the protection capabilities they need, but as an organization adopts more cloud services, adds branch offices, and embraces new remote workforce models, a piecemeal security approach may see it juggling multiple siloed solutions and disjointed policies that cause protection gaps and complexity. Settling for half measures doesn't pay off.

Palo Alto Networks delivers a comprehensive data protection solution broadly covering every network and web transmission for all their users regardless of their location, for their multiple SaaS applications, and public clouds consistently while eliminating blind spots across on-premises and multicloud environments.

For Physical Networks

With business communication spread over an exhausting number of web apps, the exit points for sensitive information are innumerable. Embedded in a Next-Generation Firewall (NGFW) as a cloud-delivered service that inspects web traffic over HTTP and HTTPS, Enterprise DLP automatically detects sensitive content in motion via machine learning-based data classification, hundreds of data patterns, and business context. It monitors transmissions of this content across the network and conditionally protects it from being leaked to the web—all without disrupting business users.

For Virtual Networks

Organizations worldwide are executing digital transformation initiatives through network architectures that incorporate multiple public clouds and on-premises virtualized data centers. Enterprise DLP in Palo Alto Networks VM-Series Virtual NGFWs automatically discovers, monitors, and protects sensitive data in motion, and it does so consistently across on-premises, hybrid, and multicloud environments.

For SASE and Mobile Workforces

Digital transformation is driving cloud adoption and user mobility. Modern users expect a convenient "work from anywhere" experience. However, corporate data becomes more vulnerable and difficult to track outside the managed premises. Enterprise DLP in Palo Alto Networks Prisma® Access automatically discovers, monitors, and protects sensitive data in motion across branch offices and mobile users. It's a core service of the secure access service edge (SASE) that consistently extends data protection and compliance outside physical premises, allowing organizations to stay ahead of their digital transformation.

For SaaS Applications

To adapt to the new hybrid work, organizations have embraced the convenience of Software-as-a-Service (SaaS) applications like Microsoft 365® and Salesforce®. Particularly, they have become increasingly dependent on collaboration apps like Slack®, Teams®, Zoom®, Jira® and Confluence™ where confidential information is unstructured and difficult to protect. Our Enterprise DLP service in

Figure 3: Examples of sanctioned apps

SaaS Security automatically discovers sensitive files, emails and messages across cloud applications, uncovers data loss blind spots, and minimizes data loss risk by enabling rich protective actions.

DLP detection as a service in SaaS Security ensures optimal performance for consistent data classification directly in the cloud, eliminating the inefficiencies incurred in legacy solutions when shuttling content between cloud and on-premises DLP.

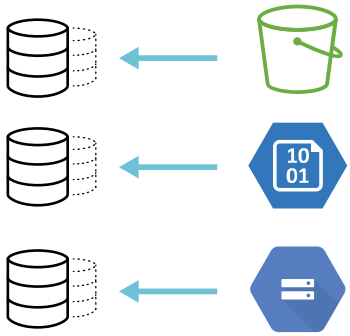

Figure 4: Examples of public clouds

For IaaS and PaaS

The near-limitless capacity offered by cloud storage services has enabled organizations to collect massive amounts of data. Cloud native environments require an integrated, automated way to identify and protect sensitive data as well as extend compliance and data privacy. Enterprise DLP in Prisma Cloud discovers, monitors, and protects sensitive data at rest in public cloud storage, such as Amazon S3 buckets. We offer Enterprise DLP in Prisma Cloud as Prisma Cloud Data Security in combination with our WildFire® malware prevention service.

Highly Reliable Detection

In data protection, automatic discovery of sensitive data drives response actions on policy violations—so it needs to be accurate. Inaccurate detection produces false positives, unsustainable incident triaging work, and disruption of normal business processes. Content similarities need advanced detection techniques that account for context as well. A modern DLP approach also needs to adapt to data flowing through modern collaboration apps like Slack, Teams and Zoom, where users communicate with short and unstructured messages leveraging more screen captures rather than traditional files to quickly convey ideas and information.

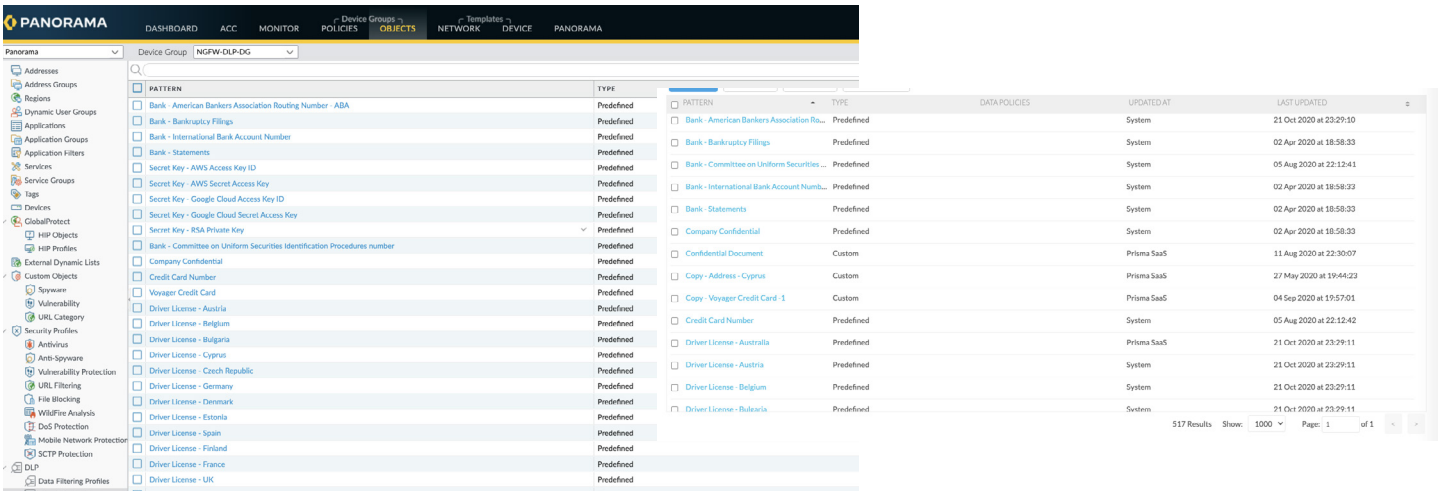

Figure 5: Predefined and customizable data identification

Palo Alto Networks Enterprise DLP automatically discovers sensitive content, both structured and unstructured, via a combination of detection methods. It leverages machine learning-based data classification and an extensive number of described data identifiers using regular expressions or keywords (e.g., credit card or ID numbers, financial records, GDPR, other data privacy- and compliance-related information) and applies customizable data profiles and Boolean logic to scan for collective types of data. Type of exposure (e.g., public or internal), confidence levels, and precise context criteria (e.g., number of occurrences and pattern logic) reduce incidents and inaccurate detection. Exact data matching (EDM) is an advanced data fingerprinting method to detect specific sensitive data, like account numbers, addresses, and

other personal information by looking for content matches on large data sources. Most importantly, the solution is able to automatically identify sensitive information even within the context of unstructured users' conversations on collaboration apps like Slack, thanks to deep learning, natural language processing, and AI models, ensuring high accuracy and fewer false positives. Advanced optical character recognition (OCR) finds sensitive content in PDFs, images, and screenshots. Automated incident workflows with policy-based response actions include user alerts and auto-remediation. Detection of flexible document properties, such as third-party data tagging, augments the identification of sensitive data.

Achieve unparalleled protection of all sensitive data with more automated detection engines, more control points, and content-aware technologies.

Use Cases

Prevent Data Breaches

Palo Alto Networks Enterprise DLP addresses the risk of a data breach by identifying sensitive information in various file types as well as monitoring, preventing, and governing unsafe movement and sharing violations with respect to that information.

Assist with Regulatory Compliance

Data privacy and compliance requirements are growing as industries, governments, and standard-setting bodies establish criteria for protecting information. Palo Alto Networks Enterprise DLP assists compliance efforts with tailored policies for GDPR, PCI DSS, HIPAA, CCPA, and more.

Protect Intellectual Property

Your IP is valuable, but it can be difficult to protect. Unstructured IP—source code, for instance—is difficult for many DLP solutions to detect. Palo Alto Networks Enterprise DLP applies the same protective rigor to your IP, such as copyrights, patents, trademarks, and trade secrets, as it does to other sensitive data or PII.

Stop Malicious Insiders

In the wrong hands, privileged access presents a significant risk. Insider data theft activities are difficult to spot because they come from authorized sources with legitimate-looking use cases. Palo Alto Networks Enterprise DLP helps organizations identify malicious insiders and stop them from putting data at risk.

Avoid Mistakes from Well-Meaning Employees

Malicious activity isn't the only cause of data loss. It can also happen when employees make mistakes. In fact, well-meaning employees often inadvertently put corporate data at risk. Palo Alto Networks Enterprise DLP accounts for unintentional data exposure and educates employees on corporate policies to mitigate careless behavior and minimize the risk of data loss over time.

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 for 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 a Next-Generation Firewall or delivered as part of a SASE, it enables organizations to continuously and consistently protect all sensitive data across network, cloud, 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.

Visit us online to learn more about how Enterprise DLP can protect and secure your company data, no matter where it is located.

Table 1: Palo Alto Networks Enterprise DLP Features and Capabilities	
Service integrated across network in-line, SaaS at-rest, SaaS in-line, IaaS, branch offices, and remote workforces	Extensive set of predefined industry-standard data identifiers and weighted regular expressions
Cloud-delivered architecture ensures new protections and product updates are applied the instant they are released	Machine learning-based data classification, automated deep learning, natural language processing, and AI models
Consistent protection enforced by a single cloud engine for data in-motion and at-rest	Exact data matching (EDM) and optical character recognition (OCR) for detection of structured and unstructured data
Natively integrated into existing Palo Alto Networks control points; no need for ICAP, proxies, and additional infrastructure	Multiple confidence levels and proximity analysis for high detection accuracy
Configure once, and automatically sync policy everywhere the service is enabled	Flexible document properties for identification of third-party data classification tags
Out-of-the-box compliance templates like GDPR, CCPA, GLBA, financial regulations, etc.	Support for advanced Boolean operators for policy tuning
Single cloud service activated by a license automatically enforces policies at scale in all the existing control points	SOC 2 Type II certification

Table 2: Privacy and Licensing Summary	
Privacy	
Trust and Privacy	Palo Alto Networks has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. You can find further information in our privacy datasheets.
Licensing and Requirements	
Requirements	Palo Alto Networks Next-Generation Firewalls require PAN-OS 10.0.2 or newer versions and are managed by Panorama. Prisma Access running 9.0.4 or newer versions. No prerequisites for the other products.
Supported Next-Generation Firewalls	All models of PA-Series and VM-Series Firewalls except CN-Series

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