paloalto NETWORKS

PRISMA™
BY PALO ALTO NETWORKS

Enterprise Data Loss Prevention

Addressing the Risks of Data Loss and Noncompliance in Modern Enterprises

Every organization must protect its reputation from the threat of data breaches. Unfortunately, keeping sensitive data, such as personally identifiable information (PII) and intellectual property (IP), safe and private can be challenging. Especially as modern enterprises adopt cloud-based services and embrace new data-sharing models, their data becomes more vulnerable to theft and prone to both intentional and unintentional exposure.

Highlights

- **Consistent data protection policy** across networks, clouds, and users—one cloud DLP engine delivers a policy everywhere sensitive data lives and moves.
- **Accurate discovery and protection** of sensitive data using automatic classification, context, and machine learning to mitigate the risk of accidental exposure while enhancing data privacy and compliance.
- **Simple adoption and management** embedding the cloud DLP engine in existing security controls to eliminate resource-intensive deployments and complex configurations.

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 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 transformation, minimizes the risk of data breaches across every threat vector, and helps regulate unsafe and noncompliant data exposure and sharing practices.

Data Security Everywhere, with a Service-Delivered Architecture

Palo Alto Networks Data Loss Prevention (DLP) provides innovative cloud-delivered data protection for a complete enterprise solution spanning clouds, networks, and data. Integrated as a service in an organization's existing security control points, it is easy to enable, eliminating the complexity of server deployments, on-premises databases, and appliances.

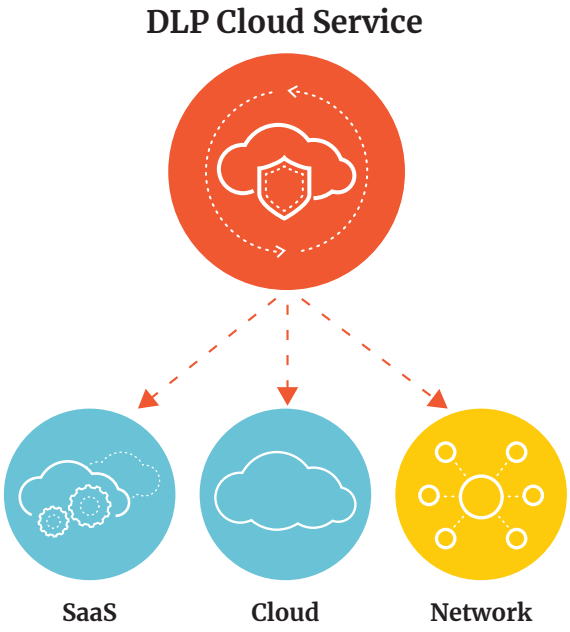

Figure 1: One cloud DLP service for easy adoption, consistent protection, and scalability

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

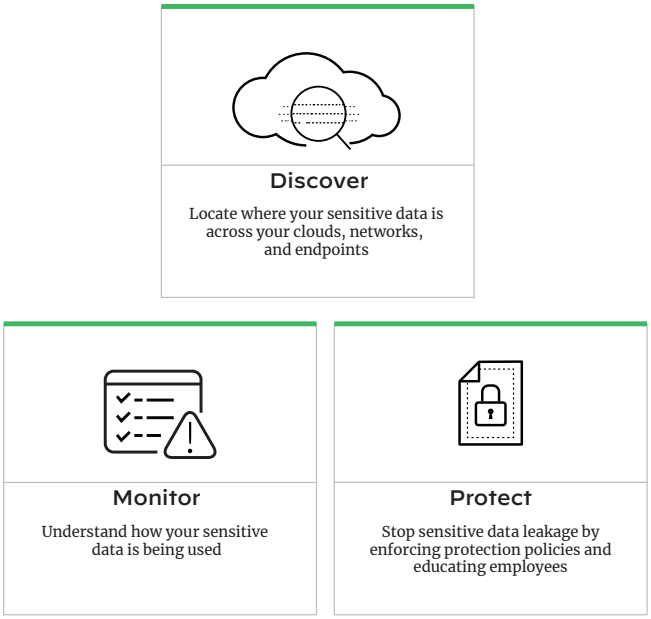

Figure 2: Fundamental DLP capabilities

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.

Complete Cloud 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 apps, 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 for the cloud, broadly covering multiple SaaS applications, web transmissions, and public clouds consistently while eliminating blind spots in multi-cloud environments.

Web

With business communications in a growing number of web apps, the exit points for sensitive information are innumerable. Shadow IT can be a serious issue when employees use untrusted apps to transfer or process data. DLP embedded in Prisma™ Access by Palo Alto Networks is a cloud service that inspects outbound web traffic sent over HTTP and selectively HTTPS, including traffic from branch offices and mobile users. It automatically detects sensitive content and conditionally protects it against being leaked to the web without disrupting users. Corporate policy-compliant transmissions are allowed, and shadow IT is safely controlled.

SaaS

With cloud adoption, corporate sensitive data is increasingly stored and created in cloud applications such as Office 365®, Slack®, Salesforce®, G Suite®, and Box. DLP in Prisma SaaS allows organizations to automatically discover sensitive files and emails in cloud apps, uncovering data loss blind spots and minimizing data loss risk by enabling effective protections, such as quarantining and reducing sharing permissions. Automatic notification for each violation helps educate users on corporate data policies over time. DLP in Prisma SaaS ensures optimal performance for data classification directly in the cloud, eliminating latencies incurred when shuttling content between the cloud and on-premises DLP.

Figure 3: Examples of sanctioned apps

IaaS

As organizations store and move sensitive content in infrastructure as a service (IaaS), they need a way to govern and protect it to stay compliant and prevent data breaches. Palo Alto Networks DLP cloud service lets organizations track and protect confidential information consistently in Amazon S3, Microsoft Azure® Storage, and Google Cloud® Storage with machine learning-assisted data classification.

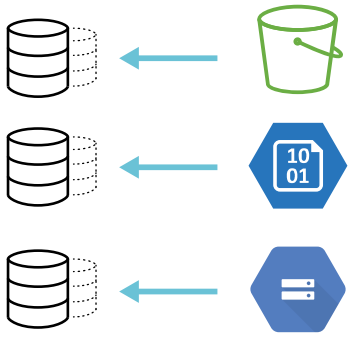

Figure 4: Examples of public clouds

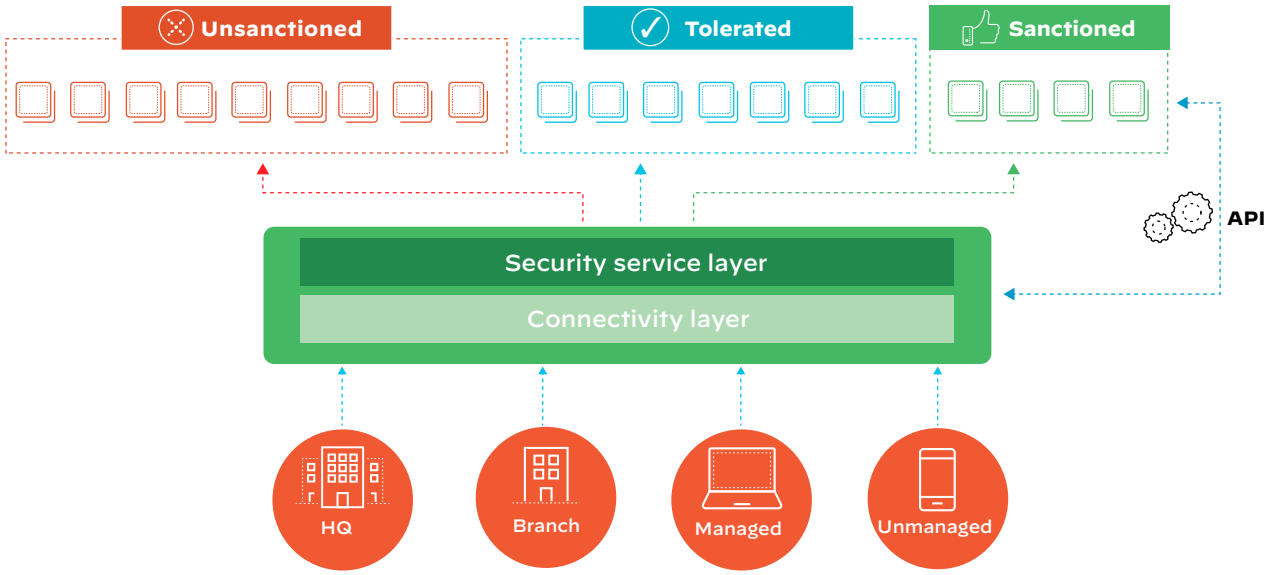

Figure 5: Network traffic flows to unsanctioned, tolerated, and sanctioned sites

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.

Palo Alto Networks DLP provides a single engine for accurate detection and consistent policy for sensitive data, both at rest and in motion. It automatically detects sensitive content via machine learning-based data classification and hundreds of data patterns using regular expressions or keywords (e.g., credit card or ID numbers, financial records) and uses data profiles and Boolean logic to scan for collective types of data. Type of exposure (e.g., public or internal) and precise context criteria (e.g., number of occurrences and pattern logic) reduce incidents and inaccurate detection. Advanced machine learning simplifies data classification.

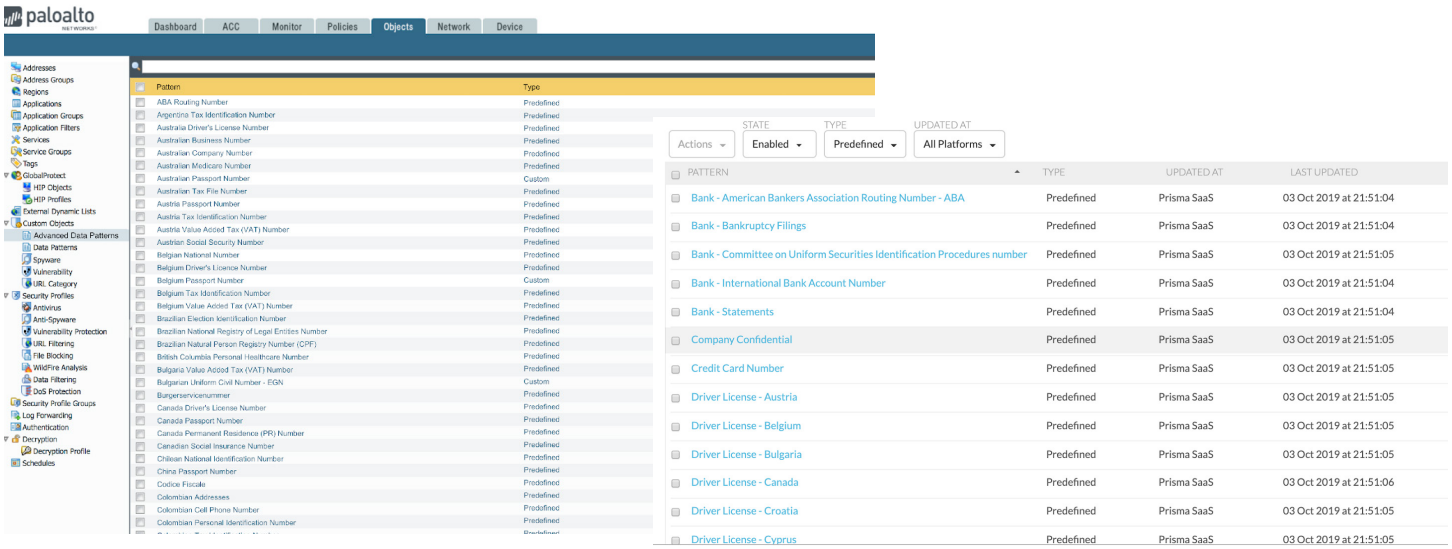

Figure 6: Predefined and customizable data identification

Use Cases

Prevent Data Breaches

Palo Alto Networks 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 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 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 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 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 solutions were not designed with mobility and the cloud in mind. As enterprises continue on the path to digital transformation, problems with complexity, administrative effort, and incomplete protection will become exacerbated.

Enterprise cloud DLP enables a more effective data protection approach. When delivered as part of a secure access service edge (SASE) model, DLP enables organizations to continuously and consistently protect all endpoints, users, and data, wherever they are. As your organization continues its cloud transformation journey, consider not only how DLP can help solve 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 platform.

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

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