Enterprise Data Loss Prevention

Data Loss Prevention (DLP) for the Modern Enterprise

Organizations face the complex challenge of securing data across hybrid work environments that expand the attack surface, with 58% of Americans now working from home.[1] The adoption of SaaS and public cloud has made legacy DLP inadequate, with both careless users and malicious actors a threat to enterprise data. Organizations struggle to comply with global regulations, protect business innovation, and prevent sensitive data leakage, all while transitioning to the cloud. Gaining visibility and control in the modern cloud environment across people, devices, and networks without juggling multiple vendors is a challenge.

Business Benefits

- **Comprehensive coverage** to discover, monitor, and protect all sensitive data across every network, cloud, and user
- **Simplified operations** to write and consistently enforce one policy throughout multiple layers of the security stack
- **High data protection** efficacy with persistent protection and zero-delay updates via cloud-delivered DLP

1. "Americans are embracing flexible work—and they want more of it," McKinsey & Company, June 23, 2022.

Challenges

- Inconsistent policies across multiple environments (endpoints, networks, and clouds) result in incomplete protection and time-consuming policy management cycles.
- A piecemeal security approach with multiple vendors across SaaS applications and public and private clouds results in siloed solutions and disjointed policies that cause protection gaps and complexity.
- Exit points for sensitive information are innumerable, with business communication spread over an exhausting number of web apps.
- Digital transformation initiatives through network architectures with multiple public clouds and on-premises virtualized data centers make data protection more complex to manage.
- Balancing the convenience of software-as-a-service (SaaS) applications like Microsoft 365 and Salesforce and collaboration apps like Slack, Teams, and Zoom with the difficulty of protecting unstructured confidential information.
- The near-limitless capacity offered by cloud storage services has enabled organizations to collect massive amounts of data. This can make identifying and protecting sensitive data and ensuring compliance and data privacy difficult.
- Legacy solutions rely on pre-defined compliance-oriented data patterns that lack the context to understand intellectual property, and typical fingerprinting-based solutions provide limited detection capability and cumbersome workflows.
- Companies are focused on stopping data as it's about to leave the boundary. This misses an opportunity to identify data at risk of loss or exposure before a data loss incident actually occurs.

Simplify Day 2 Operations with Cloud-Delivered Enterprise DLP

Palo Alto Networks Enterprise DLP discovers, monitors, and protects sensitive data across every network, cloud, and user. No more stitching together multiple DLP policies across various tools to solve for individual use cases. Our 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 stack, our Enterprise DLP solution allows one policy to be written and consistently enforced across multiple layers in the security stack, simplifying daily operations.

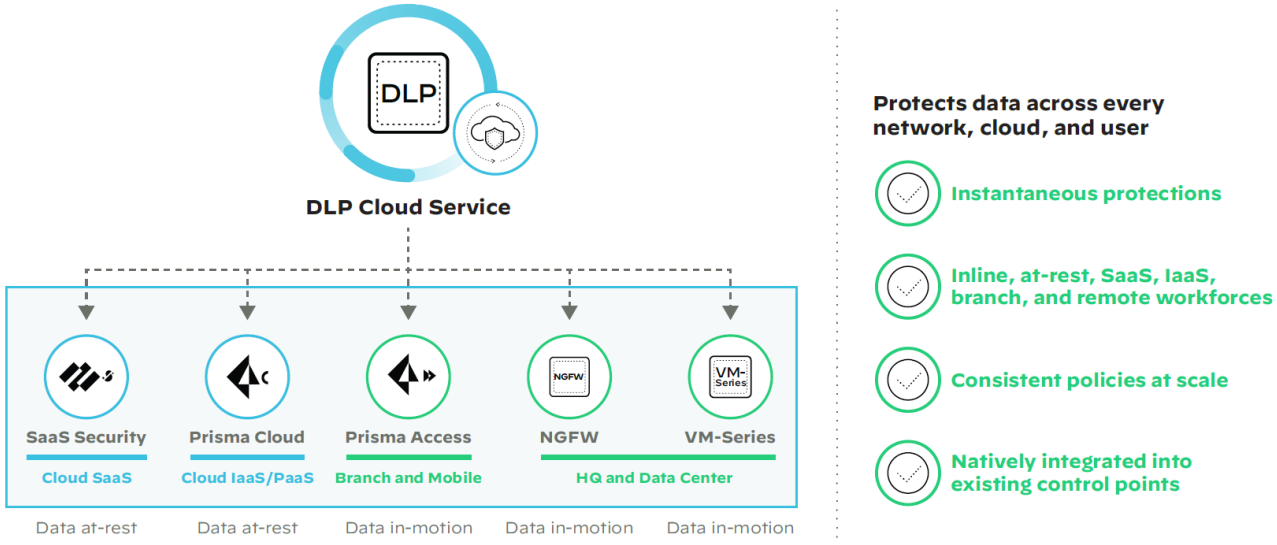

Figure 1: Comprehensive cloud-delivered Enterprise DLP

Minimize the risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise, with two times greater coverage of any cloud-delivered enterprise DLP.

Easy to Deploy, Update, and Scale

Our Enterprise DLP deploys and scales across the entire enterprise in minutes, not months, because it's natively integrated into our existing firewalls. Delivered from the cloud across network inline, SaaS at rest, SaaS inline, and infrastructure as a service (IaaS), we ensure that new protections and product updates are applied instantaneously across the security stack.

Highly Reliable Detection

Automatically identify sensitive information within unstructured conversations on collaboration apps like Slack with our advanced optical character recognition (OCR). Purposely built for DLP, OCR better preserves the context of documents to find sensitive content in PDFs, images, and screenshots compared to standardized OCR engines.

Holistically detect documents and document types based on each unique structure and fingerprint with our Deep Neural Net (DNN) models. Our advanced machine learning-based methods focus on data security over compliance and include detection of ID cards, credit card images, legal documents, and financial documents, among others. This goes above and beyond traditional DLP, which relies on fixed patterns and regular expressions to detect specific information.

Reduce SOC team loads and make end users a part of the process with security orchestration, which allows users to fix issues and seek exemptions seamlessly. With XSOAR integration, end users can remediate mistakes and seek one-time exemptions through an automated workflow, allowing SOC teams to focus on what matters the most.

Comprehensive Data Protection

Our comprehensive DLP solution covers every network and web transmission for all users, regardless of their location. It protects multiple SaaS applications and public clouds while eliminating blind spots across on-premises and multicloud environments.

- **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—all without disrupting business users.
- **Enterprise DLP in our VM-Series Virtual NGFWs** automatically discovers, monitors, and protects sensitive data in motion consistently across on-premises, hybrid, and multicloud environments.
- **Enterprise DLP in Prisma Access** automatically discovers, monitors, and protects sensitive data in motion across branch offices and mobile users. Natively integrated into secure access service edge (SASE), it allows organizations to stay ahead of their digital transformation.
- **Natively integrated into our Next-Gen CASB** and greatly expanded to address more contemporary data loss scenarios, including the growing threat of sensitive data being shared within collaboration apps such as Slack or Teams.
- **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.
- **Email DLP** identifies sensitive data using machine learning, protects data when sent to varying domains, and ensures data safety regardless of the device or email client. It provides organizations with consistent data security, leveraging extensive data detection methods, and offers global insights into data risks.
- **Data Security for Generative AI Apps** includes comprehensive app usage visibility, specific SaaS application controls, and advanced data security employing ML for data classification and leakage prevention.

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

Taking a Shift-Left Approach

Enterprise DLP takes a "shift left" approach to data security for SaaS, by providing continuous monitoring of data security posture, enabling data security administrators to take a proactive approach to securing data at risk. By taking a shift left approach for Data Security, organizations get end-to-end visibility into where data is most at risk with a unified Data Risk Explorer that enables users to drill down into sensitive data impact and breach likelihood across the organization based on location, data profiles, applications, instances, and control points. In addition, we are making it even easier to accurately identify the sensitive data specific to your business with the power of AI and ML. Our DLP classifiers now feature over 100+ predefined document type detectors and leverage the latest LLM technology to help further drive unparalleled accuracy. In addition to our new built-in ML-based document classifiers, administrators can now train custom ML models with their unique and proprietary documents to help ensure that our DLP is able to accurately identify and protect their most sensitive data. This capability can be used to discover and protect financial, legal, scientific, and business documents such as pay stubs, employment contracts, legal intake forms, and more that are unique to your organization. Customers can confidently rely on best-in-class data detection standards such as EDM, OCR, IDM, ML, and Natural Language Processing classifiers to reduce the workload on security teams by alerting end users to data incidents in real time with user-led remediation.

Table 1: Palo Alto Networks Enterprise DLP Features and Capabilities

Protect All Data, Wherever It Resides	• Service integrated across network inline, SaaS at-rest, SaaS inline, IaaS, branch offices, and remote workforces • Consistent protection enforced by a single cloud engine for data in-motion and at-rest
Cloud-Delivered Scalability	• Cloud-delivered architecture ensures new protections and product updates are applied the instant they are released
Operational Simplicity	• Natively integrated into existing Palo Alto Networks control points; no need for ICAP, proxies, and additional infrastructure • Configure once; automatically sync policy everywhere the service is enabled • Out-of-the-box compliance templates like GDPR, CCPA, GLBA, financial regulations, etc. • Single cloud service activated by a license automatically enforces policies at scale in all the existing control points
Best-in-Class Detection	• Extensive set of predefined industry-standard data identifiers and weighted regular expressions • Machine learning-based data classification, automated deep learning, natural language processing, and AI models • Exact data matching (EDM) and OCR for detection of structured and unstructured data • Multiple confidence levels and proximity analysis for high detection accuracy
Advanced Controls	• Flexible document properties for identification of third-party data classification tags • Support for advanced Boolean operators for policy tuning
Certifications	• 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	Enterprise DLP is compatible with Palo Alto Networks Next-Generation Firewalls requiring 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.

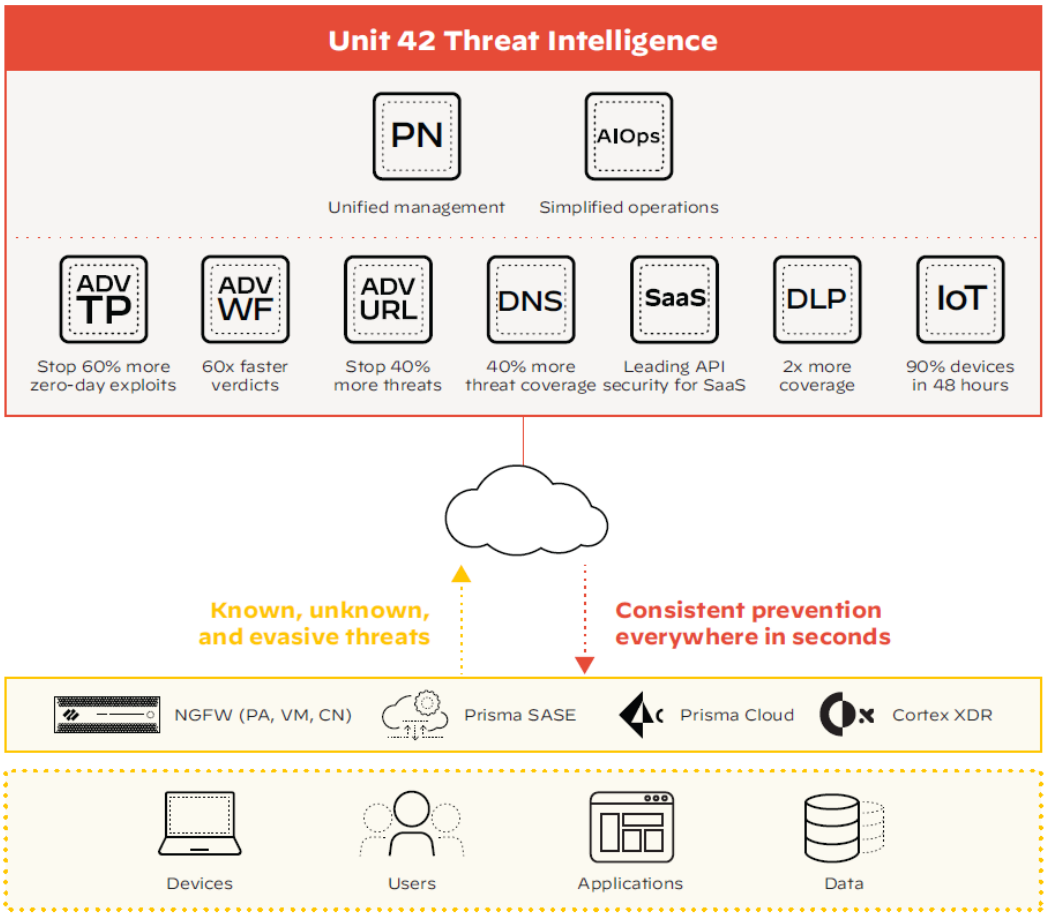

Figure 2: Palo Alto Networks Cloud-Delivered Security Services

The Power of Palo Alto Networks Security Subscriptions

Today, cyberattacks have increased in volume and sophistication, using advanced techniques to bypass network security devices and tools. This challenges organizations to protect their networks without increasing workloads for security teams or hindering business productivity. Seamlessly integrated with the industry's first ML-Powered NGFW platform, our Cloud-Delivered Security Services coordinate intelligence and provide protections across all attack vectors, providing best-inclass functionality while eliminating the coverage gaps disparate network security tools create. Take advantage of market-leading capabilities with the consistent experience of a platform, and secure your organization against even the most advanced and evasive threats. Benefit from Enterprise DLP or any of the following security subscriptions:

- **Advanced Threat Prevention:** Stop known exploits, malware, spyware, and command-and-control (C2) threats while utilizing industry-first prevention of zero-day attacks. Prevent 60% more unknown injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.
- **Advanced WildFire malware prevention:** Ensure files are safe by automatically preventing known, unknown, and highly evasive malware 60X faster with the industry's largest threat intelligence and malware prevention engine.
- **Advanced URL Filtering:** Ensure safe access to the internet and prevent 40% more web-based attacks with the industry's first real-time prevention of known and unknown threats, stopping 88% of malicious URLs at least 48 hours before other vendors.
- **DNS Security:** Gain 40% more threat coverage and stop 85% of malware that abuses DNS for command and control and data theft without requiring changes to your infrastructure.
- **Enterprise DLP:** Minimize the risk of a data breach, stop out-of-policy data transfers, and enable-compliance consistently across your enterprise, with 2X greater coverage than any cloud-delivered enterprise DLP.
- **SaaS Security:** The industry's only Next-Generation CASB natively integrated into the Palo Alto Networks SASE offers proactive SaaS visibility, comprehensive protection against misconfigurations, real-time data protection, and best-in-class security.
- **IoT Security:** Safeguard every "thing" and implement Zero Trust device security 20X faster with the industry's smartest security for smart devices.
- **AIOps:** AIOps for NGFW redefines firewall operational experience by empowering security teams to proactively strengthen security posture and resolve firewall disruptions.

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