Trellix

Trellix Data Loss Prevention

Key Advantages.

- Single console
- Encrypts sensitive data
- Pre-production rule tuning
- Educates users on best practices
- Covers many cloud applications (via partners)
- World class service & support
- On-prem or SaaS-based

Trellix DLP Suite of Products

- Trellix DLP – Discover
- Trellix DLP – Endpoint
- Trellix DLP – Monitor
- Trellix DLP – Prevent
- Drive Encryption
- File & Removable Media Protection

Do you know exactly what sensitive data your organization has, and where it resides? Are you losing intellectual property, financial data, customer information and more, without even knowing it, possibly right now? Such data loss is not necessarily the work of hackers; your employees also leak data, inadvertently or intentionally. Trellix offers a Data Loss Prevention (DLP) solution that protects against external and internal threats and helps maintain compliance with various regulatory frameworks.

Discover and Classify Your Data

The first step to protect your data: find where it resides and classify it. That's not an easy task. A typical enterprise has petabytes of data, scattered between laptops, shared file servers, document repositories, file transfer locations, and private and public clouds. Moreover, sensitive data comes in both structured and unstructured formats, the latter being harder to define (design files, for example).

Trellix DLP scans your data, wherever it resides, and classifies it using more than 300 content types. Classification methods include automatic fingerprinting, exact data match, integration with external classification tools, and manual classification.

Set and Enforce Policies

Once you've found the sensitive data, Trellix DLP helps define policies (rules) to protect it. In addition to outright blocking of actions (which can hinder business more often than not), Trellix provides numerous customizable actions that inform the user they violate a policy yet allow the user to provide a reason and continue, knowing both violation and reason are logged. You can also encrypt

sensitive data, for example on laptops or cloud repositories, so even if files leak – no one can access the data. After setting policies, Trellix DLP will routinely scan all accessible resources, to find and report policy violations. Scanning, tracking, and reporting is done in real time on data-at-rest, data-in-use, and data-in-motion, across your entire network. This gives you full visibility on data

that travels between your users and the external world. By doing that, and generating incidents when DLP policies are violated, Trellix DLP protects against data loss.

Creating the right policies is a challenging task. You want rules that prevent data leaks, yet without hindering users' work. You also want to prevent false

incidents that overload your data security team. Trellix DLP provides more than 150 pre-built rules to help you start. It also provides our unique Capture technology, which enables testing and tuning your rules against all your historical data. Capture also helps with classification tuning, as well as supporting your compliance efforts by aiding in forensic after-the-fact investigation, as it saves everything that happened on your network.

Central Monitoring and Incident Management

Trellix ePO software enables all DLP activities through a single pane-of-glass: full data mapping and classification, policy setting, monitoring, incident handling, and full centralized management. Our unique technology shows the security team what they should focus on, enabling a deep dive into every aspect of the overall DLP platform. This single console omits the need to switch between multiple consoles and views, saves time, and makes sure no incident goes unnoticed.

Trellix ePO is available either on-prem or as a SaaS-based option.

Compliance Enforcement and User Education

A Verizon study found that 82% of data breaches in 2022 involved human error. There's also intentional insider threat, for example disgruntled employees or those considering a move to your competition.

Enforcing compliance on employees is getting harder. Users interact with a growing number of data repositories, both on-prem and in the cloud. They may inadvertently violate policies regarding the handling of sensitive data, or intentionally try to steal your data.
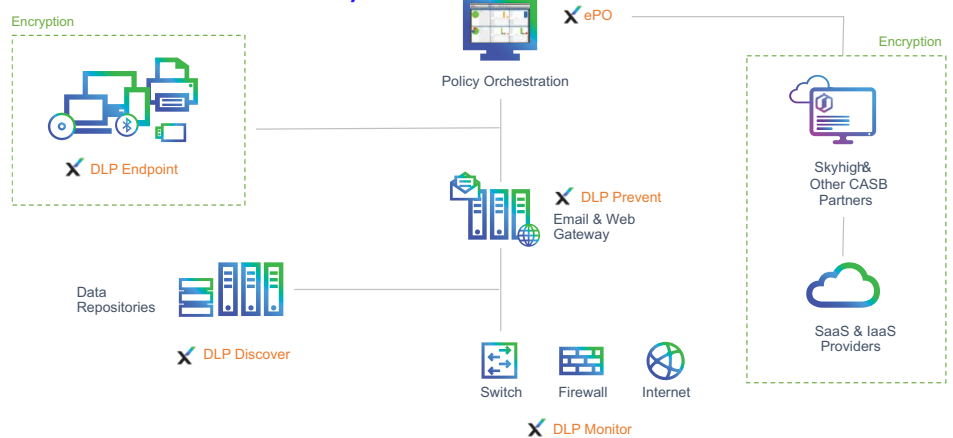
Trellix DLP not only stops insider threat, but also ensures compliance by educating your users. Every time a user violates a policy – and their action is blocked – they get a pop-up screen explaining what they did

Service and Support to Guarantee Your Success

Data loss is painful for any organization. Moreover, implementing DLP technology is a challenging task. Gartner says that 35% of DLP implementations fail. One of the main reasons: DLP is not an 'install and forget' solution. DLP needs constant attention and tuning. As your business evolves, new data is created, classification changes (today's sensitive data may be public next week), and rules should be modified. DLP must constantly be adjusted for updated business needs.

Trellix guarantees your DLP implementation is successful through our world class Customer Success and Professional Services teams. Our data security experts help you implement Trellix DLP, train your people on using it, and accompany you along your journey – to guarantee your success.

Trellix Data Security

072022-05