Checklist:
Five signs you need to add DLP to your MSP practice

Why should service providers care about data loss prevention (DLP)?

For years, organizations have had little success protecting sensitive data from unauthorized access and exfiltration via external attacks or insider risks such as IT misconfigurations and human error. This has left them exposed to consequences like embarrassing headlines, damaged customer and partner trust, equity losses, and regulatory sanctions.

With the rise of behavior-based data loss prevention (DLP) technologies, MSPs can now effortlessly launch and manage DLP services with minimal efforts-to-value to reduce the risks of data leakage for clients.

Now is the time to capitalize on this trend and ensure your clients sleep better at night knowing their data is protected and their regulatory compliance is intact.

> "80% of global organizations report they are likely to experience a data breach that impacts customer data in the next 12 months."

Source: Cyber Risk Index Report, 2021, Ponemon Institute

Check the five signs that you need to add DLP to your practice

1 Clients' employees have access to sensitive data via their endpoints (e.g., data subject to regulations)

It doesn't matter if your clients store their sensitive data in the cloud, if it's accessible via employees' workstations — it can easily be leaked out through them via peripheral devices or network channels such as email and instant messengers.

More than 80% of data breaches are perpetrated with a financial motive, according to the Verizon Data Breach Investigation Report, 2022. Due to this, the primary data that is targeted in attacks is of high value — such as data that is subject to regulations, trade secrets or intellectual property data that can be leveraged for financial gain.

If clients' employees create, store or work with such data on their endpoints, you need to ensure it's protected against leaking to unauthorized parties to save them from severe financial, regulatory and reputational risks.

2 You are looking for new revenue sources to grow your practice

In the Acronis Pulse of the MSP 2021 Report, we can see that MSPs expect their primary revenue income for the coming years to be from cybersecurity. However, with the majority of service providers offering some form of managed security services, competition is becoming a primary challenge in the industry.

The rise of behavior-based DLP technologies enables you to differentiate your portfolio with DLP services that were previously unavailable for MSPs and smaller organizations due to high complexity, service delivery costs, and slow time to value because of the need to map policies to ever-changing business processes that are specific to each client.

With behavior-based DLP technologies, you can find new revenue sources and provide an attractive DLP service offering for organizations of all sizes, thereby reducing the risks of clients' data ending up with unauthorized parties.

3 You have clients in highly regulated industries (e.g., healthcare, BFSI, government)

In case your clients operate with or store personally identifiable information (PII), patient health information (PHI), cardholder data, or any other form of sensitive data in highly regulated industries, they will require a higher a level of data protection than just backup.

The majority of regulations, such as GDPR, HIPAA and PCI-DSS require the reporting of data breaches and data leaks within a strict time frame and could lead to severe fines for clients in the event of sensitive data leakage.

Data loss prevention solutions are the only technology capable of monitoring data flows inside the organization and preventing data leaks while raising the visibility and enabling investigations of DLP events.

4 You have clients that are more prone to attacks and data leak risks

Historically, there have been industries with greater security vulnerabilities that also store valuable sensitive data, making them a high value target of cyberattacks. Examples of such industries include education, healthcare and other public sectors where data accessibility is required, but at the same time, you need efficient protection for this data so it won't leak to unauthorized parties.

Behavior-based DLP technologies enable you to provide a highly competitive DLP service for an affordable price to protect such organizations against noncompliance and data leakage risks.

5 You have clients that are considering/paying for cyber insurance to reduce liability

Let's face it — cyber insurance is among the hottest topics in the cybersecurity space in recent years. Clients are turning to cyber insurers to limit their business's liability in case of data breaches.

The cost of cyber insurance depends upon several factors, including the business's annual revenue, its industry, the type and amount of data held, and the level of security. You should consider adding DLP to your service stack to cover data safeguard requirements for cyber insurance and minimize cost for clients.

Advanced DLP

The Advanced DLP for Acronis Cyber Protect Cloud helps your clients sleep better at night knowing that their sensitive data is protected against leaks to unauthorized parties. Its unique behavior-based technology enables the creation and continuous extension of DLP policies based on the specifics of each client and eases your service launch with never-seen-before simplicity and minimal efforts-to-value.

Acronis

Learn more at
www.acronis.com