Acronis

WHITE PAPER

Launching and scaling DLP services: A guide for MSPs

For years, businesses of all sizes have not been able to tackle the risks of data leakage, despite increased awareness, security protocols, and regulations. In fact, they're actually on the rise: According to the 2021 Year End Report: Data Breach QuickView by Risk Based Security, more than 22 billion records were exposed, making it the second highest year for the amount of confidential data compromised since 2005. The overwhelming majority of these records were exposed due to data leakage. A data leak is defined a breach of security in which confidential, sensitive or protected data is accidentally or deliberately released to an untrusted environment or unauthorized users either outside or inside the organization.

So what leads to data leakage? There are two main causes:

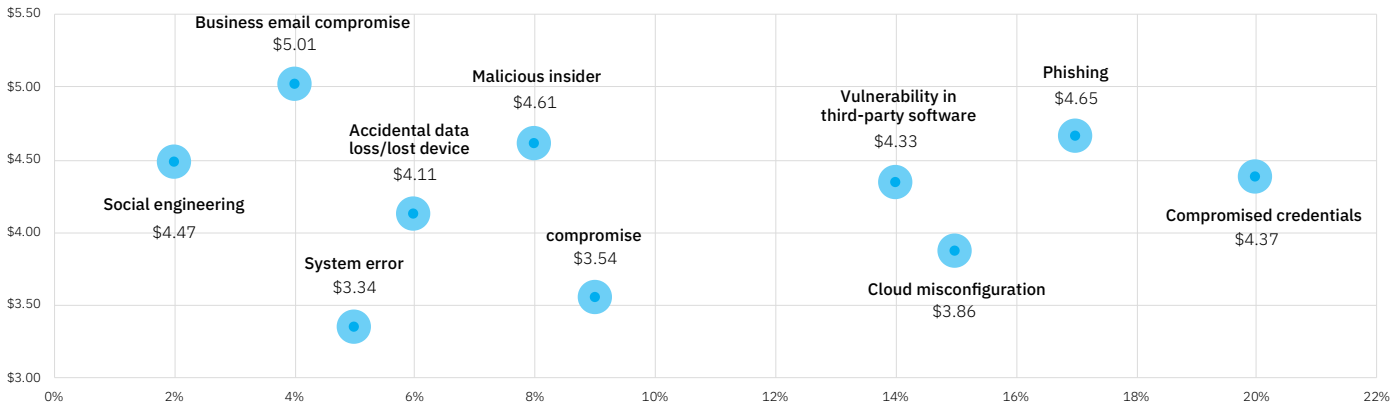
1. External cyberthreats

As defined by the MITRE ATT&CK framework, data exfiltration is among the last tactics that malicious adversaries carry out during an attack. The motive of actors in more than 80% of data breaches is financial gain, according to the Verizon 2022 Data Breach Investigation Report.

That's why sensitive data is the primary target in a majority of attacks. Once malicious adversaries establish access to the corporate environment, they can try to exfiltrate data via numerous channels. As attacks grow in complexity and are increasingly able to bypass security layers, the risks for organizations' data are exponentially growing.

2. Internal risks

While anti-malware and other endpoint security technologies are able to detect and stop external attacks, other risks for organizations' data — insider-related ones — are gaining momentum. One common example is end users unknowingly releasing data to unauthorized parties (e.g., by forwarding an email). This can occur due to accidental employee mistakes, IT misconfigurations, or through malicious insiders — all of which can pose a severe threat to organizations — leading to the costliest data breaches.



It's worth noting that although some organizations underestimate the impact of internal risks, the 2021 Cost of Data Breach Report by the Ponemon Institute clearly states that approximately a third of data breaches involve insiders.

What's the impact of data leaks on businesses?

Data leakage poses a severe risk for business. The exfiltration of sensitive data to unauthorized parties leads to:

- **Noncompliance with regulations** — The storage, access to, and protection of sensitive data such as employee and customer personally identifiable information (PII), protected health information (PHI), or cardholder data, are strictly regulated by local and international regulations including GDPR, CCPA, HIPAA, PCI-DSS, etc. Some regulations, such as GDPR, even require breaches to be reported within a strict timeframe. In the case of a regulated data breach report delay, organizations can face large fines and might even lose their compliance certifications.
- **Financial damage** — Once data gets leaked, in addition to the regulatory fines that MSP clients might be facing, service providers may also be exposed to the threat of financial damage as a result of liability for clients' security that may lead to litigation. Additionally, the exfiltration of trade secrets or intellectual property might cause additional financial losses for companies and even destabilize their market position.
- **Reputational risks** — Ending up in the embarrassing data breach headlines can be detrimental for businesses. This could not only lead to customer churn for your clients, but could also cripple their existing partnerships and ability to acquire new customers. Your clients' data leakage may also affect your reputation and business.

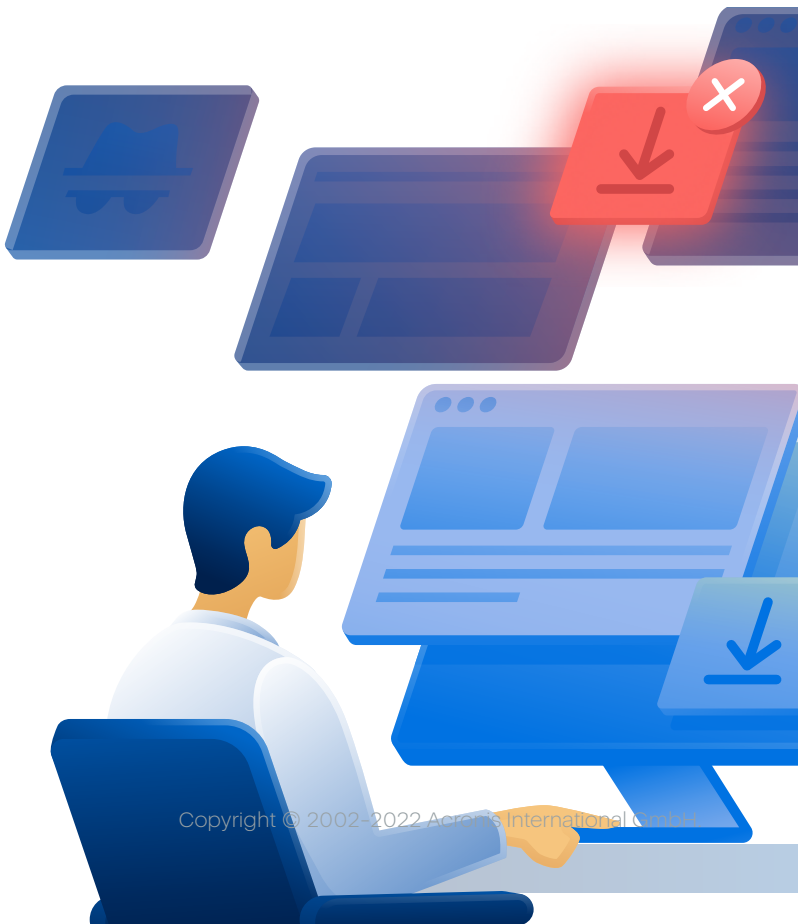
What is data loss prevention?

Data loss prevention is a long-established category of security solutions, representing systems of integrated information security technologies that detect and prevent unauthorized use, transmission and storage of confidential, sensitive data.

DLP solutions do this by applying a combination of data flow controls and content analysis methods. Such technologies enforce business-acceptable data use and handling policies across the organization that prevent exfiltration of sensitive data to unauthorized recipients (both internal and external).

While data protection is primarily associated with backup and disaster recovery, there are other essential technologies such as DLP, notarization, and encryption that secure sensitive information against a wider variety of threats, including data leakage.

DLP is the only technology capable of providing visibility and control into the sensitive data flowing and stored across an organization to prevent its leakage to unauthorized entities.



States of data and how different functional DLPs protect them

There are **three main states** in which data can reside within an organization:

- **Data-in-use:** Data being used or transferred in local channels (e.g., peripherals, removable storage) or via applications on endpoint computers. An example of such data would be files that are being transferred from an endpoint computer to an USB drive.
- **Data-in-motion:** This term refers to data that is moving or being transferred between computer systems. For example, data that is being transferred from a local file storage to a cloud storage, or data that is transferred from an endpoint computer to another endpoint via instant messenger or email is considered data-in-motion.
- **Data-at-rest:** This describes data that is being stored locally or in a network and is currently not being accessed or transferred. An example of data at rest is data that is stored in network shares or on-premises servers.

It's important to note that data frequently and continuously changes its state, although some data may remain in a single state for the entire lifecycle of an endpoint. Understanding the different states of data, their specifics and differences can help clients to handle their organizational data more securely and protect it against leakage.

Respectively, there are three main "functional" DLP types dedicated to protecting each of the states of data:

- **Data-in-use DLP**
- **Data-in-motion DLP**
- **Data-at-rest DLP**

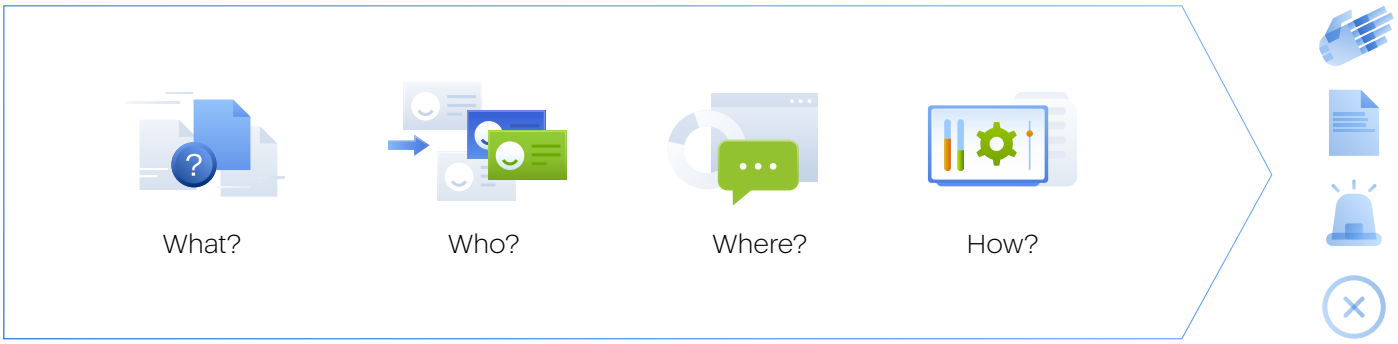
It's worth mentioning that there're other technologies that can address different data risks (e.g., accessibility, privacy risks) such as identity management or encryption. However, DLP is the only technology capable of protecting data across multiple states with the solemn purpose of preventing data leakage while providing visibility into data flows.

DLP controls: Content vs. context

Each data flow in an organization has its context and content. The context refers to environmental factors such as the users involved in a data flow, the channels being used, the direction of the flow, etc. The content describes the actual type/category of information being transferred — e.g., patient health records, employee PII, etc.

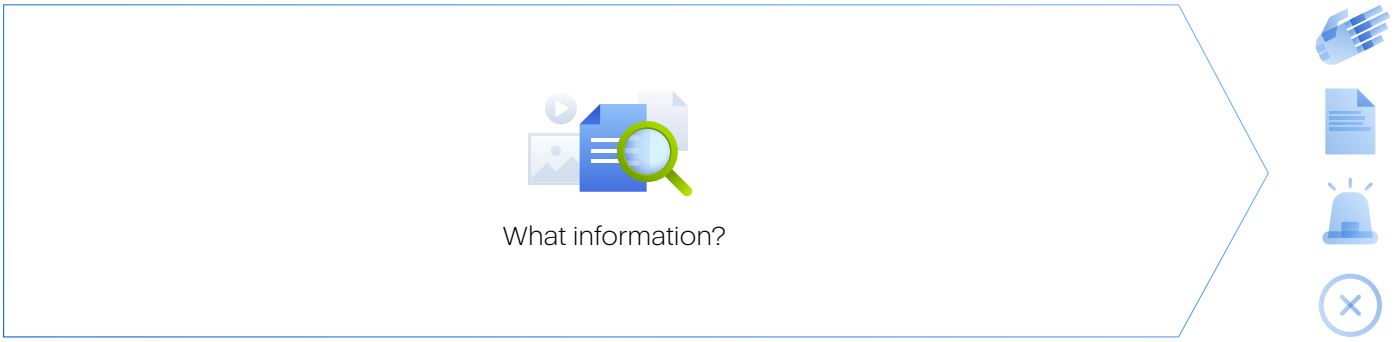
Efficient DLP solutions should implement controls over data flows based both on their context and content:

- **Context-aware DLP controls** — Control data transfer operations based on the operation's context using attributes such as involved users, used channels, transferred data direction, destination, time, etc.



Example: Policies that allow copying data (what) by users (who) to encrypted USB devices (where) and block copying data to unencrypted USB devices.

- **Content-aware DLP controls** — Deeper control over data flows is based on the type and sensitivity of the actual information (content) being transferred.

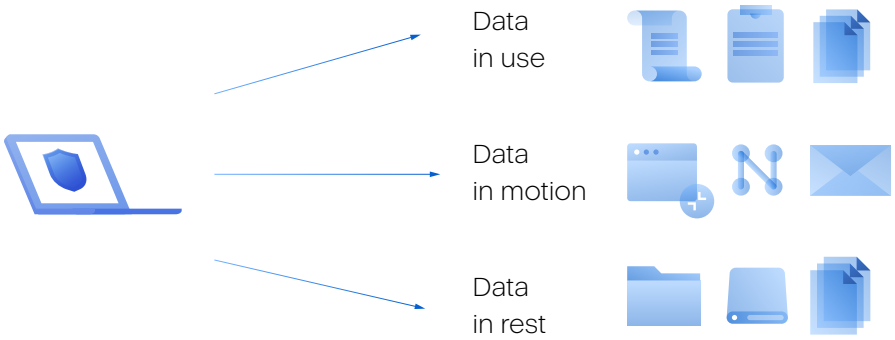


Example: Documents containing HIPAA-related information (what information) are prohibited from being copied to any USB device.

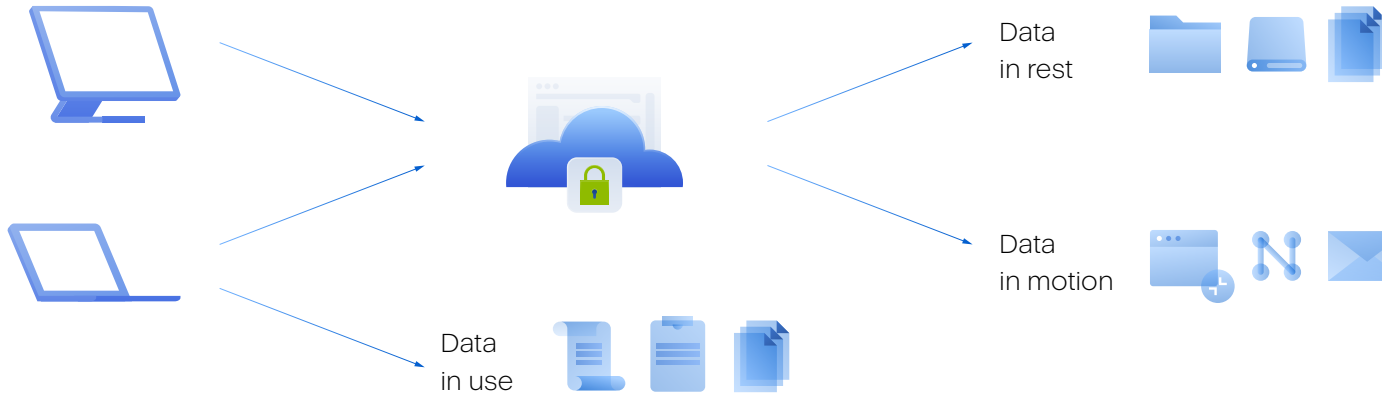
DLP architecture types

There're three main types of DLPs based on the ways they're deployed and operate:

- **Endpoint DLPs** — Solutions that use DLP agents on endpoint computers and prevent data-in-use, data-in-motion, and data-at-rest leakage from these computers, regardless whether they are used inside the corporate network or on the internet.



- **Network / cloud DLPs** — Solutions with only network-resident components, including hardware / virtual DLP gateways and servers that protect data in motion or data at rest on computers located in the corporate network, preventing data leakage to unauthorized recipients and destinations outside the corporate network.



- **Hybrid DLPs** — Solutions that utilize both network and endpoint DLP components to perform all functions of both endpoint and network DLP architectures.

What's worth remembering is that network DLPs can not protect data in use due to their architecture and control only data leakage to unauthorized parties outside of the corporate network, while endpoint and hybrid DLPs can protect data in all states and prevent leakage to both internal and external unauthorized parties.

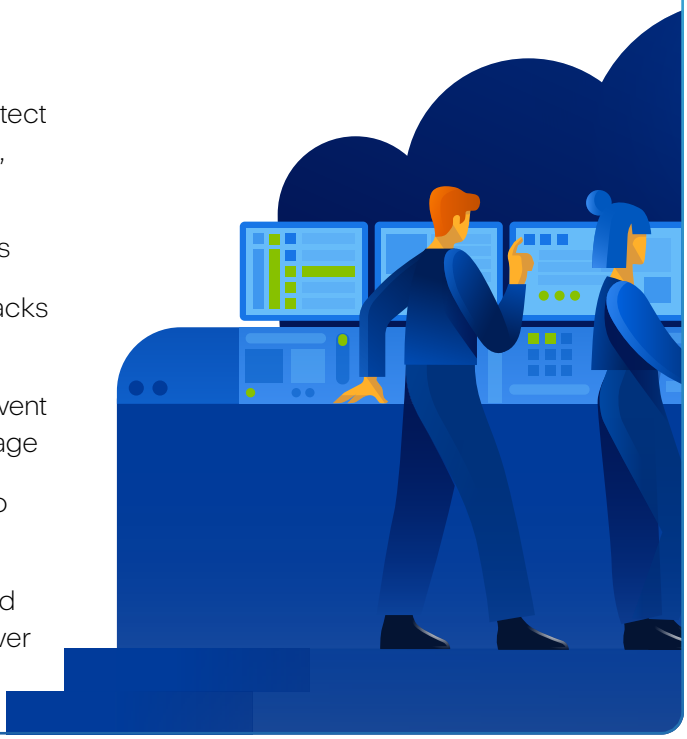
For the purpose of this guide, we will be focused on launching, running and scaling a DLP service based on the endpoint DLP architecture.

Why clients need DLP

According to the Ponemon Institute 2021 Cost of Data Breach report, the global average total cost of a data breach is $4.24 million, which is 10% higher than it was in 2020. As we see the cost of data breaches rising, the actual average time to identify and contain a breach is 287 days — which speaks to the huge risks your clients face before the breach is contained. These risks can lead to financial, reputational, and compliance costs.

The main ways in which you'll be able to reduce risks for clients with a DLP service are by:

- **Helping achieve compliance** with regulations and protect regulated information – PII (GDPR, CCPA), PHI (HIPAA), payment card information (PCI DSS), etc.
- **Protecting clients'** intellectual property and trade secrets
- **Minimizing risk** of data exfiltration by malware and attacks due to social engineering
- **Strengthening remote work** and BYOD security and prevent the transfer of sensitive data to private cloud-based storage
- **Preventing data leakage** caused by employees due to accidental mistakes, negligence or misconduct
- **Enabling rapid response** to data leakage incidents and post-breach investigations with continuous visibility over DLP events



DLP service delivery flow

Before going into more details on how to launch, run and scale a DLP service, it's important to note first that due to ther specifics, DLP services have a concrete delivery flow which includes the following steps:

- **DLP agent deployment:** Deciding which endpoints should be provisioned with DLP services with the purpose of ensuring thorough protection for company data and deploying DLP agents on these endpoints are among the first steps in your service delivery process. Keep in mind that it is recommended to have DLP agents provisioned to all workloads where sensitive data is created, stored or used. If such workloads remain unprotected, they create potential data leakage gaps in the corporate IT security system.

- **DLP policy creation:** Another initial step is to create the DLP policies that ensure the proper data use and handling policies to prevent data leakage. Keep in mind that based on the DLP technology used, this step can precede deployment. **What's important to note** is that DLP policies are not universal — they're always client-specific — because different organizations have different internal processes, fall under different regulations, and have different data access and sharing needs. Due to these specifics of DLP policy creation, traditional DLP solutions that require manual policy management present significant complexity and cost barriers to being used by service providers for building DLP services.
- **DLP policy validation**: An important step following the creation of initial DLP policies is to validate them with clients to ensure these policies fit the business requirements — as MSPs are not able to acquire such deep understanding of each client's business specifics. The more complex and "technical" the visual representation of the policy, the more time and expertise is required by clients to validate it.
- **DLP policy enforcement and management:** When DLP policies are validated with the client, they can then be enforced to start protecting sensitive business data against leakage. Keep in mind that DLP technologies control sensitive data flows of an organization, blocking any unauthorized ones. However, businesses constantly evolve, new processes are being introduced, new data regulations arise and old ones can be changed. Due to this, the initial DLP policies must be continuously adjusted to ever-changing business needs, in order to ensure no new essential data flows are blocked, while all data leakage attempts are prevented. This could be achieved either through manual policy fine-tuning or automatic methods of adaptive policy adjustment.
- **Reporting on DLP service value:** Ongoing reporting of blocked sensitive data transfers and DLP-related end-user actions to demonstrate the value of DLP services helps boost customer retention and illustrates risk reduction to clients who are not aware of their data leakage problems.

MSP challenges with current DLP solutions

DLP is a mature, enterprise-focused market with long-established players that the wider market — such as service providers and their SMB clients — has struggled to adopt, due to the need for continuous, deep understanding and mapping of business specifics to DLP controls, knowledge of regulatory requirements, and understanding of data compliance needed to operate such technologies. This has caused the DLP industry to focus predominantly on large organizations that can afford costly in-house expertise dedicated to DLP management.

The main challenges that MSPs face when it comes to implementing and running a DLP service are:

- **Running a DLP service is costly and complex** — Due to the fact that traditional DLP solutions require complex, manual processes for initial policy creation and follow-up adjustments, the time and efforts-to-value required to implement an efficient DLP across clients, make the service too costly. Moreover, this complexity requires hiring DLP experts — a task much more difficult and expensive than hiring general IT security specialists.

- **Efficient DLP requires client-specific policies** — As mentioned above, the business processes and data sensitivity of any organization are unique and ever changing, requiring ongoing DLP policy adjustment to business specifics. However, MSPs lack and can't acquire and continuously maintain such deep understanding of each client's business processes. This becomes a barrier posing a significant scalability challenge for MSPs with traditional DLP technologies.
- **Misconfigured DLP policies can disrupt business continuity** — On the one hand, manual DLP policy creation and configuration are error prone due to complexity and granularity. On the other hand, DLP technologies block any unauthorized data flows. The fusion of this complexity and the DLP preventing capabilities can disrupt essential business processes by mistakenly blocking data flows necessary for the business if DLP policies are misconfigured or new business processes are not consistently mapped to these policies.
- **Employees are the clients' weakest link** — No matter that DLP technologies are hardly accessible to MSPs and their clients; human error and external attacks targeting employees are the primary causes of data leaks. Even if service providers are able to limit the risk of external threats with other endpoint protection layers, they will be the ones held responsible if users unknowingly release sensitive data, causing a data breach.
- **Clients can be unaware of the data leakage problem** — Due to historically difficult access to DLP, the data leakage problem is something that clients might be unaware of. Launching a DLP service means that service providers would need to also educate clients on the data leakage risks they're facing, and the fact that DLP is the only technology capable of addressing those risks that pose significant threats for organizations of any size.

New trends and technologies on the market, such as automatic, behavior-based policy creation, extension and monitoring are tackling the challenges of rapidly changing DLP rules to match constantly evolving business procedures, in addition to regulatory requirements. These new capabilities are effectively democratizing the DLP market and making it accessible to service providers and their clients. Now is a great time to think of extending your portfolio with DLP services.

Planning and launching a DLP service

The first step in planning and launching a DLP service is verifying whether your clients actually need DLP.

Clients require a DLP service to reduce their data leakage risks in case they possess some or all of the following indicators:

- Create, store or work on their workloads with sensitive data that is subject to regulations
- Have trade secrets or intellectual property that needs to be protected against leakage
- Are operating in highly regulated industries
- Have suffered a data breach and want to secure their environment and reduce risks
- Have / need compliance certifications
- Are paying / considering cyber insurance to reduce their liabilities
- Lack dedicated security staff and expertise

In addition, clients in the following industries have historically demonstrated greater interest in DLP:

- Banking and financial services
- Healthcare
- Legal
- IT and telecommunications
- Government and the public sector
- Manufacturing
- Retail and logistics
- Education
- Energetics

In the event you have clients exhibiting these indicators or operating in the aforementioned industries, it's a good time to consider adding DLP to your service portfolio to meet their rapidly growing needs for reducing data leakage risks and strengthening regulatory compliance.

Planning your services and cost estimation

The three major factors that determine your service price are labor costs, product costs and the desired margin. This is how each can affect your price quote:

- **Labor costs:** The complexity of the solution chosen will determine the time your service technicians spend on provisioning and managing the service, as well as the required level of their IT security expertise.
- **Product costs:** DLPs, historically utilized by larger enterprises, involve high costs which make them unaffordable to small and medium-sized businesses. If your clients are mainly SMBs, you need to choose a solution that will not make the service too costly for them.
- **Desired margin:** The average MSP brings in gross margins as high as 50% on remotely delivered services sold under the recurring-revenue model.

Running a DLP service with Acronis Advanced DLP pack

Acronis offers a behavior-based DLP that automatically creates and continuously maintains the consistency of client-specific policies, without requiring months to deploy, teams to maintain or a Ph.D. in privacy law to understand.

With Acronis Advanced DLP pack, you can provide clients with comprehensive DLP protection for data in motion and data in use with a never-seen-before level of simplicity, enabling you to:

- **Unlock new profitability opportunities by** extending your portfolio to attract more clients and increase your revenue per client with DLP services that were previously available only to enterprises.
- **Minimize efforts-to-value** easily adding DLP to your practice without increasing your management complexity, costs and headcount.
- **Mitigate security risks for clients** by preventing sensitive data leakage.
- **Strengthen client regulatory compliance** with out-of-the-box data classification templates for common regulatory frameworks, including GDPR, HIPAA, and PCI DSS.
- **Simplify service provisioning and management** by automating DLP service provisioning, initial policy configuration and follow-up adjustments.
- **Ensure client-specific DLP policies at any scale** by automatically aligning DLP policies with ever-changing business specifics with behavior-based technology — thereby ensuring easy policy validation with clients prior to enforcement.
- **React faster to DLP events** and simplify DLP service operations, policy maintenance, IT security audits, and incident investigations with centralized, policy-based audit logging and security alerting.

Acronis Advanced DLP pack

The Advanced DLP pack 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