



E-Book

# Gaining Competitive Advantage: Own the Data Security Conversation

**Bill Falk**

President of Go-to-Market, Actifile

September 2024





## State of the Managed Security Services Market

Many MSPs want to be in the Managed Security Services (MSS) market, and with good reason. MSSPs have been enjoying a lane with 15% compound annual growth rate (CAGR) over the last several years—a rate that is expected to continue unabated clear through 2030, reaching a market size of over \$75B. This makes it one of the fastest growing sectors for IT service providers overall.

However, MSPs moving into security services understand there are significant hurdles to clear. There are specialized resources to integrate tech investments for specific capabilities like intrusion detection, event management, and stricter standards of compliance and reporting when dealing with a company's sensitive data.

To compensate for the tech and skills gaps, MSPs are investing in 3rd party solutions to take their managed security offerings to market. IT Harvest Dashboards counts over 3,700 cybersecurity vendors bringing over 8,000 products to market. Typically, they will combine multiple solutions and vendors to create a specialized offering that aligns with their target market.

To gain competitive advantage and grow revenue in security services, IT service providers must deliver value-added security services that go beyond table stakes.

Just as critical are differentiated value propositions and sales approaches. Accelerating time to close requires a powerful strategy that sets your organization apart from other service providers that potential clients may be evaluating.

How can MSPs enter this space with confidence, and how can MSSPs expand their revenue without significant investments?

Actifile offers a pathway for MSPs and MSSPs to deploy data security as a strategic advantage through its **Dynamic Data Security Platform**, enabling them to get started quickly and provide a next-level cybersecurity and compliance solution.

## Strategic Advantage #1: Unlock New Markets

It starts with understanding and responding to data risk. Actifile Dynamic Data Security is key to opening new markets through a comprehensive yet manageable data security solution.

Dynamic Data Security is a process based on assessing risk—generating a complete picture of an organization's data risk landscape—and using that understanding to create intelligent security rules that allow for automated protection in a way that scales throughout the network seamlessly.

Dynamic Data Security provides MSPs and MSSPs a powerful offering for their clients:

**Visibility into their entire data risk**—through a continuous and automated risk assessment, all sensitive data on the network, across endpoints, servers, and cloud file repositories is quickly located, identified, and categorized by data type without using intrusive methodologies. Additionally, the system will automatically assign monetary risk values to all the data.

Armed with a full picture of their data risk exposure, IT admins and business decision-makers can make intelligent, informed decisions about data access and security levels. These rules are applied instantly to existing data and when new data files and records enter the network. The ability to automatically encrypt any data, anywhere, provides a completely secure option in the face of rapidly evolving cyberthreats. The encryption and decryption processes are transparent (invisible encryption) to end users, providing the optimum level of protection while enabling business efficiency.

For example, admins can apply distinct levels of security protocols based on whether a file or record is classified as high risk (credit card records) or low risk (external marketing content). If it is high risk and of critical importance, admins can apply encryption policy so that only users equipped with Actifile can view the unencrypted content, with no latency or need for usernames and passwords.

Even if the sensitive data is stolen in a breach, bad actors will not be able to read the encrypted content, eliminating the risk. Beyond protecting data from internal and external threats, encryption also helps with compliance, placing the organization in safe harbor according to all privacy regulations.



**Ability to “set and forget” dynamic security and encryption rules** based on user, data type, and application, instantly, instead of enduring months-long configurations that quickly become outdated by business demands.

Actifile offloads the heavy solution management associated with traditional Data Loss Prevention (DLP) and encryption technologies. By automating data discovery, setting rules, and nearly eliminating configuration and maintenance headaches, service providers can confidently offer cybersecurity services that reduce their risk of exposure by +90%, within hours, without sacrificing productivity at the end user level.

## Strategic Advantage #2: Accelerate Revenue Growth

*Turn Risk into Revenue Through the Power of Quantification*



The IT service provider landscape is crowded—10,000 MSSPs by some estimates and roughly 40,000 MSPs all wanting a part of the growing security services market. So, how can you differentiate yourself?

By becoming a trusted advisor. Talking about reducing a company’s monetary risk immediately initiates a consultative conversation by bringing the concepts of cybersecurity, data security, and levels of risk to a new level.

Data breaches are costly. The IBM Cost of a Data Breach Report 2023 found the global average impact of a data breach to be a staggering **\$4.45M per incident**, and the total addressable market to combat these breaches for vendors and service providers has reached \$2T. Traditionally, it has been challenging to illustrate the risk to potential clients. When the company's stakes are unknown, it can be hard to justify adding another expense to protect against a potentially non-existent threat.

*Putting a monetary value to risk changes the sales conversation*

One of the most powerful sales tools to fuel these conversions is the monetary risk a company is faced with. The monetary value is derived from industry standards and data types, the FAIR Institute’s risk analysis framework model, and Actifile’s proprietary technology.

### Actifile's solution presents:

- The client's sensitive data types, data flows, and potential vulnerabilities
- The potential cost of a breach based on the value of their data
- The location of all sensitive data types, on and off the network perimeter, no matter how long it has been, or whom it was shared with

Clients receive a rude awakening when confronted with their financial exposure, driving them to take immediate action.



Organizations rarely see this complete picture of their threat landscape, let alone understand the total amount of their financial exposure.

The value proposition for robust data security becomes crystal clear. It gives the client a tangible number that they can use to justify the investment in data security.

By quantifying the exact financial risk hanging over a company, you can dramatically accelerate the sales process. You position yourself as a proactive problem solver, opening a trusted advisor relationship with clients that helps expand your footprint.

Actifile equips you with the tools and expertise to have these value-added conversations with your clients, that include both their data security needs and also their business and financial risks.

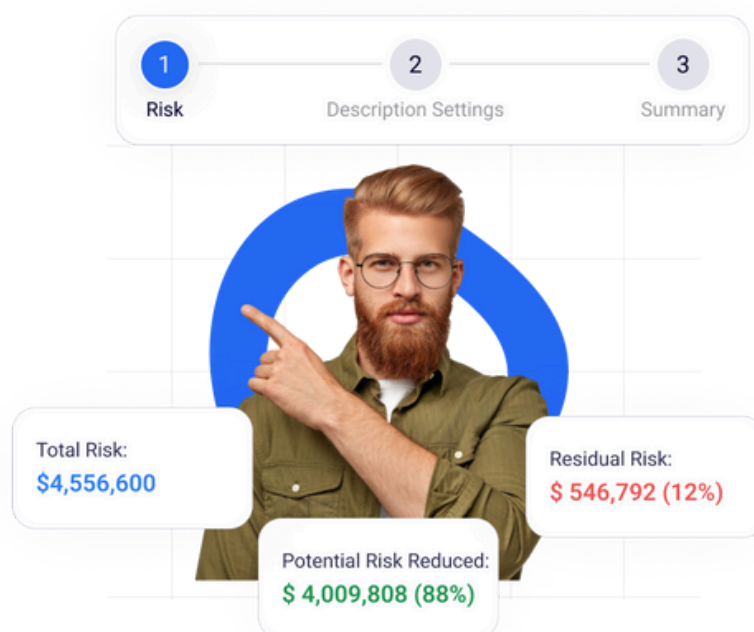
## Strategic Advantage #3: Roll Out New Compliance Services

Intertwined with the security equation is compliance. A growing industry in its own right, the Compliance Management Software market forecasting a projected 11% CAGR from 2021-2028, reaching an expected \$75B. MSPs can benefit greatly by extending their security services to include compliance management and reporting.

Every organization that deals with sensitive data needs to (a) maintain regulatory compliance with the relevant data security frameworks that govern their specific data types, such as HIPAA, GDPR, CCPA, CMMC, PCI, etc., and (b) prove they are in compliance through regular reporting. Neither activity is a one-time event. Both require ongoing processes to ensure that the sensitive data is properly protected.

It is important to recognize security does not equal compliance. While security frameworks define how to protect systems, networks, and sensitive data, privacy compliance defines what sensitive data is and provides general guidance on how to protect it.

Both security and compliance have impacts on a company's reputation, their standing with regulatory agencies, business efficiency, and ethical posture. Companies that fail to meet compliance guidelines may be fined or censured by governing bodies. Security and compliance certainly overlap and influence each other. Becoming compliant involves implementing systems to encrypt, mask, and restrict access to data, which are also important parts of security. Further, non-intrusive data classification is essential to maintaining compliance.



Understanding what data should be retained or deleted is a perfect use case: deleting certain records after a certain amount of time is a key GDPR requirement, but it's also a key part of security operations. Data often finds its heaviest use during the first few weeks of its lifecycle, then is shelved indefinitely, a vulnerability just sitting there waiting to be compromised.

In the past, traditional enterprise DLP solutions would require numerous rules to be developed to guard data across its entire lifecycle. And these would have to be applied differently based on data type, regulations, and business needs.

Now, Actifile's intelligent data forensics can show when that data was accessed and used, and when it is no longer useful. Automatic actions can be taken, based on set guidelines like CCPA, GDPR, or any other government standard, to ensure that the relevant data is properly protected. These actions can be configured once and dynamically applied to new data records as they enter the network.

MSPs and MSSPs can set up Actifile on a client's network and bring all their data processes into alignment with security guidelines in several hours. The solution's continuous monitoring and assessment of all data—including data passed through shadow IT apps—generates an audit trail that records changes to the data.

Actifile similarly streamlines the reporting process. Service providers can easily generate detailed reports to demonstrate compliance with industry regulations, and help clients achieve a proactive security posture.

## Ready to See Actifile in Action?

Dynamic Data Security is a competitive advantage for MSPs and MSSPs that is easily tailored to their client's IT, operations, compliance, and security needs. The ability to protect a company's sensitive data in a matter of hours is something that no other cybersecurity solution can provide.

**[Click here to watch an on-demand demo](#)** and see how Actifile can empower you to offer a comprehensive, data-centric approach to security, propelling your business and your clients' cybersecurity to new heights.



## Effortlessly Safeguard Sensitive Data. Everywhere.

Watch the Platform in Action

