
Ignite
TECHNOLOGY
BROADCOM
Symantec
by Broadcom Software
BROADCOM
Automic
SYMANTEC DLP + AUTOMIC
IF YOUR SECURITY ISN'T AUTOMATED, YOUR DATA ISN'T FULLY PROTECTED
DLP protects your data, automation protects your business.
VISIT IGNITE-TEC.COM

Detection Without Action Leaves Critical Gaps

Modern enterprises have never had more visibility into their data. Your investment in Symantec Data Loss Prevention (DLP) gives you a clear understanding of where sensitive information lives, how it moves, and when it's at risk.

But in today's environment, defined by cloud adoption, distributed workforces, regulatory pressure and fast-moving threats, visibility alone is no longer enough. The security gap isn't in what your DLP platform detects. It's in the time and effort required to act on that detection. Every minute between identifying a data-risk event and resolving it represents exposure: exposure to breach, to insider misuse, to misconfiguration, to non-compliance, and to reputational harm. Traditional, human-driven remediation cannot match the speed at which data moves or threats evolve.

This is why business leaders are pairing Symantec DLP with automation that transforms DLP investments into an always-on, zero-touch protection engine, one that executes remediation instantly, consistently and in full alignment with governance and compliance requirements. It eliminates the delays, inconsistencies and manual dependencies that make traditional DLP response difficult to scale and hard to audit.

The result is a modernised data-security operating model where:

- Incidents are resolved at machine speed.
- Response is standardised across cloud, endpoint, SaaS and identity systems.
- Audit evidence is generated automatically and reliably.
- Security teams are freed from repetitive manual work.
- Your organisation's risk window is dramatically reduced.

You've already invested in the right detection capability, now it's time to ensure every detection leads to immediate, effective action.

The Strategic Challenge: Visibility Is No Longer Enough

Modern organisations have made significant progress in strengthening data protection. Symantec DLP has given you the visibility and intelligence needed to understand where sensitive data lives, how it's used, and when it's at risk. This foundation is essential, but in today's environment, it is no longer sufficient on its own.

Data now moves across cloud platforms, SaaS applications, remote endpoints, shared repositories, and hybrid infrastructure faster than traditional security processes can respond. While DLP has become highly effective at detecting policy violations and high-risk events, the real challenge lies in what happens after detection. In most organisations, the response to DLP events still relies on:

- Manual investigation and triage
- Remediation steps executed in different tools
- Variable levels of expertise
- Limited out-of-hours coverage
- Documentation that varies from case to case

These human-dependent processes introduce delays, inconsistencies, and exposure windows that adversaries, insiders, and misconfigurations can exploit, even when detection is immediate. This isn't a limitation of the DLP technology itself, but a natural consequence of relying on manual workflows in an environment where data, threats, and compliance obligations move at speed.

The strategic challenge is clear: DLP tells you what's happening, but without automated, reliable, real-time action, risk remains.

Closing this gap requires modernising the response layer, ensuring that the moment a high-risk event is detected, the organisation can act with the same speed, consistency and assurance as the technology that identified it. This is where integrating Symantec DLP with automation becomes transformative, it closes the last-mile protection gap and turns detection into immediate, effective defence.

The Real Security Gap: The "Last Mile" Between Detection and Response

Even with the strength and sophistication of Symantec DLP, organisations still face a fundamental challenge: data protection breaks down in the space between detection and response. DLP excels at identifying risky behaviour, spotting sensitive data in the wrong place, flagging unusual user actions, and surfacing policy violations with remarkable accuracy.

But once those incidents are detected, the responsibility shifts from technology to people, that is where risk re-enters the equation.

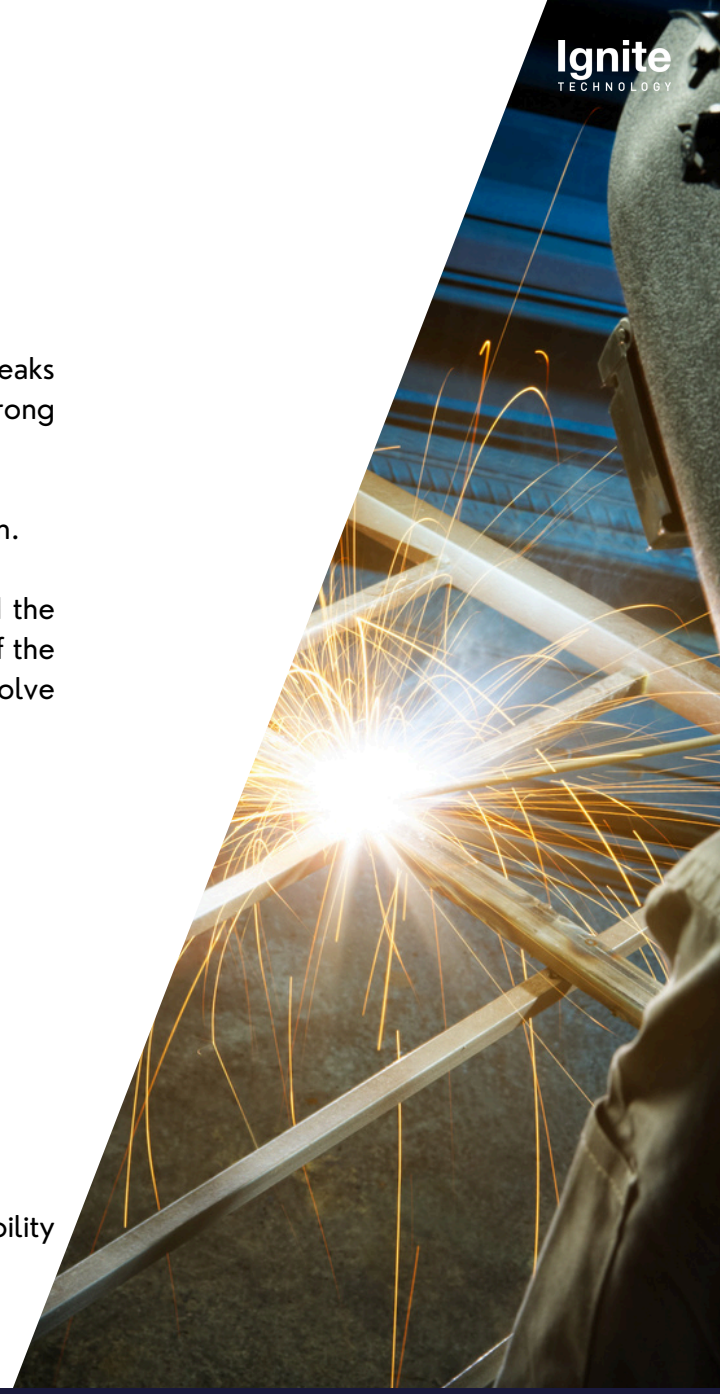
In most organisations, resolving DLP events depends on manual workflows where every handoff introduces time, variability, and the potential for human error. This reliance on manual intervention creates an unavoidable security gap, one that exists not because of the technology, but because of the operating model surrounding it. In a world where data moves instantly and threats evolve continuously, human-paced remediation simply cannot keep up.

Key limitations of manual response include:

- Delayed action when incidents occur outside business hours
- Inconsistent execution across teams, systems, and regions
- Competing priorities that slow down remediation
- Dependence on expertise that isn't always available
- Increased audit pressure when documentation varies between analysts
- Exposure windows that remain open long after detection

The result is a modern paradox where you can know about a risk immediately and still remain vulnerable.

This is the real security gap facing today's enterprises, a gap not in detection capability, but in the speed, consistency and reliability of the response. And it's this gap that must be closed to achieve true, end-to-end data protection.



Automic is the Logical Extension of Your DLP Investment

To fully realise the value of DLP and to close the protection gap that still exists between identifying a risk and resolving it, organisations need a response layer that operates with the same speed, precision and consistency as the detection engine itself.

This is why automation is the logical next step - it doesn't replace or compete with Symantec DLP; it elevates it.

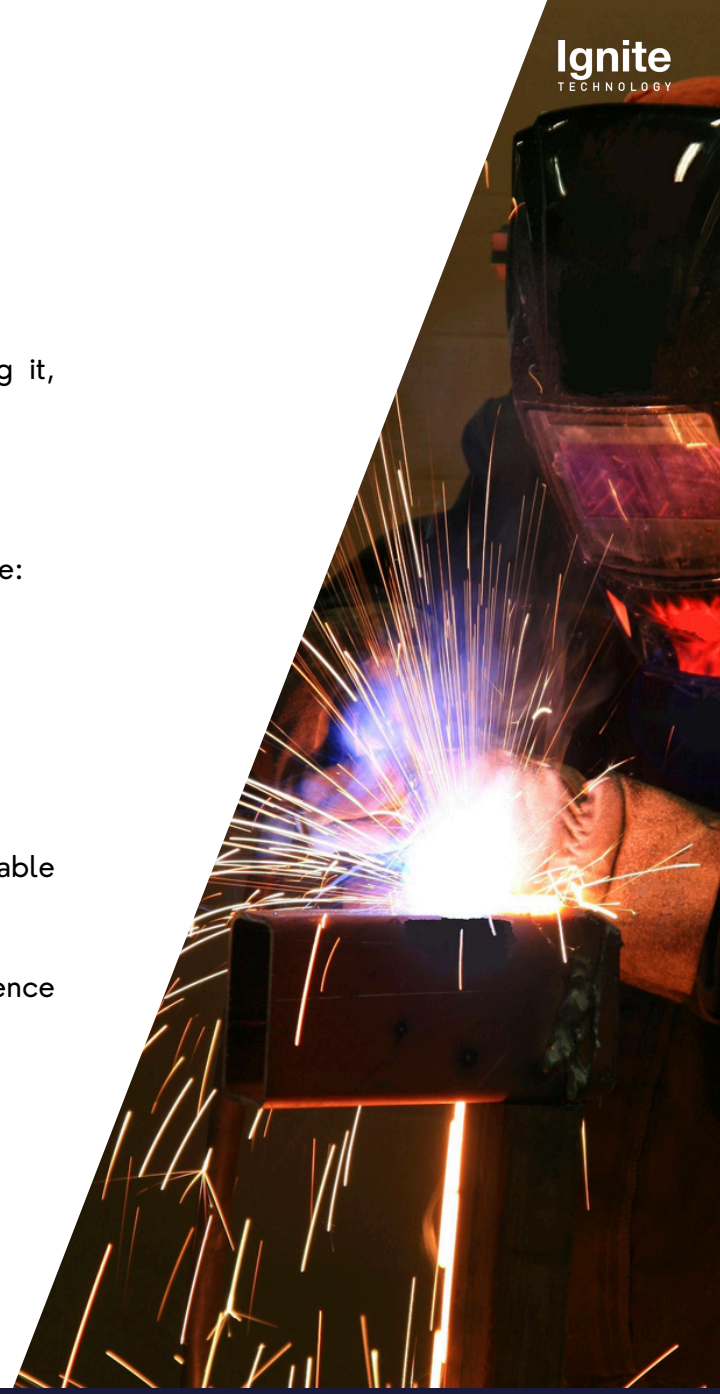
Where DLP surfaces risk, automation ensures the right actions happen, immediately, automatically and without operational variance:

- Every DLP alert becomes a trigger for orchestrated, zero-touch remediation.
- Actions occur at machine speed, not human speed, significantly reducing your exposure window.
- Processes are standardised, removing the inconsistency that manual response inevitably introduces.
- Evidence is captured automatically, strengthening your compliance posture.
- Your security team is freed from repetitive work and can focus on higher-value activity.

In other words, automation transforms DLP from a visibility platform into a complete detection-to-resolution capability, one capable of protecting sensitive data across cloud, hybrid and endpoint environments without relying on human intervention.

This integration represents a structural uplift in how the organisation handles data risk, it delivers a level of responsiveness, resilience and operational assurance that simply cannot be achieved with manual processes.

Together, they form a modern data-security architecture that is built not just to see risk, but to eliminate it.



High-Value Use Cases with Symantec DLP + Automation

1. Automatically Secure Misconfigured Cloud Storage
Automation revokes public access, corrects permissions, tags resources, and initiates governance workflows, enabling immediate containment of cloud misconfigurations, one of the leading causes of modern data breaches, without waiting for humans to react.

2. Respond Instantly to Insider Risk and Endpoint Behaviours
High-risk behaviours trigger automated safeguards, disabling accounts, killing specific processes, isolating devices, or notifying HR and security leaders instantly. Leading to a stronger internal defence posture, with zero dependence on response time or staffing.

3. Neutralise Compromised Accounts in Real Time
Executing enforcement automatically, resetting credentials, terminating sessions across SaaS platforms, and enforcing MFA revalidation, where account compromise becomes a contained event, not a breach pathway.

4. Enforce Enterprise-Wide Data Governance Consistently
Remediation becomes standardised. Every department and system responds to DLP events the same way, following the same governance, every time. IT leaders gain predictable, repeatable control across the entire organisation, no drift and no exceptions.

5. Strengthen Audit, Compliance and Operational Assurance
Every action, every remediation step, permission change, or enforcement process is automatically logged, timestamped and auditable. This means audit readiness improves dramatically, and compliance risk is substantially reduced with minimal effort.

6. Scale Security Operations Without Additional Headcount
Automation takes on the high-volume, repetitive work, enabling your security teams to focus on strategic initiatives rather than constant manual remediation, giving you a modern, scalable security operating model that grows with the business.

The Business Case: Higher Value, Lower Cost, Reduced Risk

Six key areas where automation is the ROI multiplier for your existing DLP investment include:

1. Dramatically Reduced Data-Security Risk

Every minute between detection and response increases the likelihood of data loss, insider misuse or regulatory breach. Automating DLP closes this exposure window, ensuring a materially lower probability of data-security incidents and less time managing fallout.

2. Lower Operational Cost Through Intelligent Automation

Manual remediation consumes valuable time and increases organisational dependency on specialist expertise, automation provides a more efficient operating model that scales without increasing staffing cost.

3. Strong Compliance and Audit Readiness

Regulators expect accuracy, consistency and evidence, however, manual remediation, with its inevitable variation and documentation gaps, makes this increasingly difficult. Automation provides a stronger, more defensible compliance posture with reduced effort.

4. Greater Resilience Across Hybrid, Cloud and Distributed Environments

Automation brings predictability and standardisation to every DLP-driven action, across every platform and region, providing a more resilient, modernised security model, one that performs the same way everywhere, every time.

5. Full Realisation of Your Symantec DLP Investment

The true value of DLP is only realised when risks are resolved instantly and consistently, enabling a maximum return on an investment you've already made, without replacing or restructuring your existing security stack.

6. A Future-Ready Security Operating Model

Move from reactive workflows to a predictable, automated, always-on security posture that supports long-term digital strategy, achieving a scalable, future-proofed approach to data protection.

In Conclusion
From Visibility to Security

Modern security demands more than visibility, it demands certainty, consistency, and speed. The organisations thriving in this landscape are those that have recognised a simple truth: real protection begins when detection triggers immediate, reliable action.

By integrating Symantec DLP with Automic Automation, you eliminate the delays, variability and operational strain that manual remediation introduces. You gain a response layer that works at machine speed, enforces your governance model consistently, and strengthens your regulatory posture by design.

The result is a data-security operating model that is:

- **Faster**, because response is instantaneous.
- **Safer**, because exposure windows vanish.
- **More resilient**, because actions are standardised.
- **More efficient**, because teams focus on what matters.
- **Future-ready**, because automation scales as your business does.

Your DLP platform gives you the insight, automation gives you the impact. Together, they form a modern, proactive, enterprise-grade defence capability, one that enables your organisation not only to identify risk, but to eliminate it with confidence.

This is the evolution of data protection, and Ignite is here to help you lead it.

Click here to get in touch with our automation specialists


Ignite
TECHNOLOGY
BROADCOM®
FOR MORE INFORMATION, VISIT IGNITE-TEC.COM
CONTACT US
BROADCOM
Automic