

## USE CASE

# Data Protection



Data loss prevention (DLP) systems have been used in enterprises for years as blanket data protection, but traditional DLP systems are time intensive, expensive and dated. Complex DLP can't keep pace with today's evolving threat landscape and business environments that rely on distributed systems, cloud technology, encryption and mobile devices.

## THE CHALLENGE

Traditional DLP systems are designed and priced for enterprise environments that can afford and staff them, making them virtually inaccessible to small and mid-sized enterprise. Yet smaller businesses face the same data protection challenges as their larger peers, especially when it comes to digital transformation, data proliferation and increasing pressure to protect their sensitive data from risk.

Underfunded and short-staffed small enterprises arguably face greater risk than large enterprises as a single data breach or non-compliance fine can put them out of business. As a result, small enterprise security and IT teams are forced to prioritize investments and programs that map to incident response and ever-increasing regulatory requirements. Most teams spend their time on reactive activities rather than proactive strategies that can better mitigate risk and help them understand where their critical data exists.

## Risks of Insufficient Data Protection:



Poorly Protected Data



Breach Liability



Regulatory Non-compliance



Increased Cyber Risk



Data Loss



Incomplete Data Inventory



Increased Operational Risks



Reputational Risk

# Use the CaveLO platform to underpin your data protection strategy.



## Here's how:

**1** Continuously align your business to industry best practices like the CIS Benchmarks, a set of recommendations and controls that focus on the secure configuration of multiple systems across business environments.

**2** Customizable settings make it easy for your employees to use your systems securely, and harder to violate your data policies.

**3** Real-time data discovery and classification means you'll always have an up-to-date inventory of the critical data that exists across all of your systems.

[LEARN MORE](#)

## THE SOLUTION

Data protection is achieved when all of the layers that make up a business's infrastructure are addressed. Those layers (including servers, hardware, applications, endpoints and cloud services) all contain sensitive company data. By combining security best practices with automated solutions designed to meet modern use cases, small enterprises can get greater visibility across all layers of the infrastructure and the vulnerabilities that might put them at risk. Right-sized data protection delivers:

- ✓ Richer threat intelligence
- ✓ Faster time to respond to threats
- ✓ Improved threat detection across the security tech stack
- ✓ Demonstratable processes required for compliance purposes
- ✓ Third party reassurance

