



**Data
Protection**

Solutions Guide



CAVELO

How to Use This Guide

Data protection can be an overwhelming topic for IT teams. If you're an IT or security leader at a mid-sized organization, you know how complex the practice of cybersecurity has become, especially when you have limited time and resources to manage it. Yet as complex as cybersecurity is, data protection boils down to having good security hygiene and baseline processes in place to guard your data.

We all know that cyber-attacks are on the rise, but did you know that most breaches can be traced back to system misconfigurations? Unfortunately, unchecked and unintentional human mistakes and oversights expose highly sensitive data, leaving your systems vulnerable to attack.

Security strategy used to focus on your network's perimeter and legacy solutions to protect your business's "castle walls". But cloud adoption, a reliance on endpoints and our distributed workforces mean that the traditional perimeter doesn't exist anymore. Best practices and good hygiene are key to hardening your overall security posture while helping you align to the many data privacy and security standards that apply to your business.

This guide is designed to help you organize and prioritize data security and best practices planning; it navigates new and emerging use cases, details industry best practice frameworks and provides a solutions comparison to help you source an approach that's right-sized for your business and its unique security requirements.



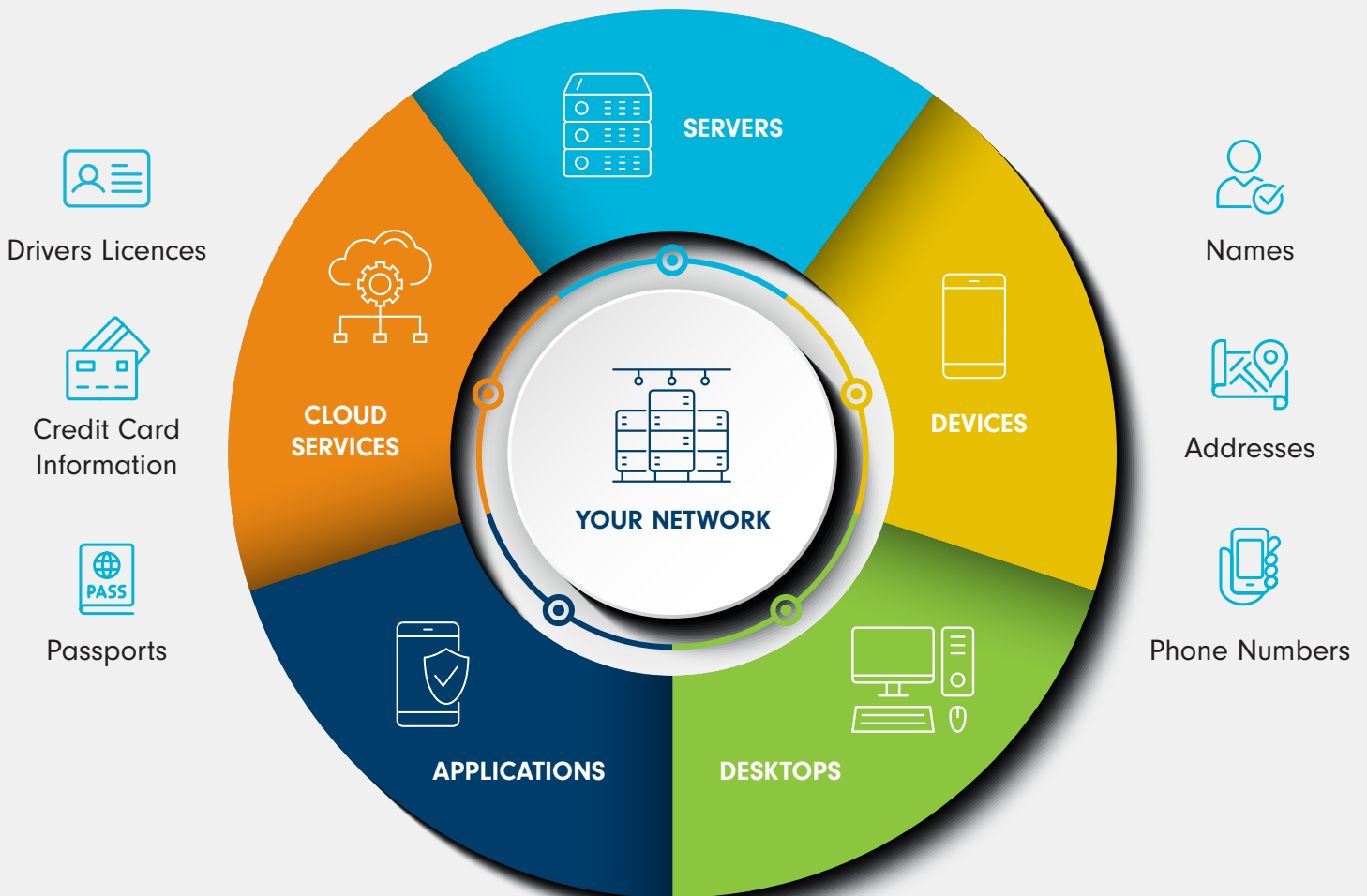
New & Emerging Application Use Cases	4
Data Loss Prevention (DLP).....	5
Data Discovery	6
Data Protection	7
Data Privacy and Compliance.....	8
Managed Service Provider (MSP) Third-party Audit.....	9
Incident Response	10
Understanding Industry Best Practices.....	11
Evolving Your Organization’s Security Maturity.....	13
Solution Comparison Guide	15
The Cavelo Platform.....	16
Overview	16
Platform Architecture.....	16
Getting Started.....	17

New and Emerging Application Use Cases

Your organization's use cases are evolving – your strategy should, too

It's no surprise that the data that lives on your network grows every day. As you add new servers, applications, devices and endpoints your data can move to potentially unsafe or unsecure locations.

Knowing where your data lives is important for many reasons; we're covering top-of-mind use cases (many of which you're probably navigating today) to explore why.



Data Loss Prevention

Traditional data loss prevention (DLP) technology is often mistaken for data loss prevention strategy; DLP technology is used by enterprises as a tool to protect company data and prevent it from getting lost or stolen. On the other hand, DLP strategy focuses on a broader approach and frameworks that include policies and procedures, network controls and more technical pieces like tools and technology.

The Challenge

Companies use a combination of DLP strategy and DLP technology to mitigate data loss. Larger enterprises with a high level of security maturity are able to institute layers of policies and procedures, controls, technology, and dedicated in-house expertise to run it all. Smaller businesses lack the same level of security maturity and budget that their larger peers have, and often turn to DLP software providers or large cloud service providers who offer some level of DLP controls as part of all-in-one licencing agreements. Yet without a DLP strategy, knowing how to implement those controls can be confusing, so teams won't use the controls at all – or worse, assume that their service providers are operating them on their behalf.

The Solution

A data loss prevention strategy starts with knowing what data exists on every endpoint across the network. With full visibility, businesses can establish a comprehensive data inventory, and better identify the tools they need to encrypt and protect sensitive company data, all by data type. From an auditing perspective, an up-to-date data map helps businesses demonstrate alignment to data security, privacy policies and data protection controls. Data loss prevention provides:

- Visibility to data in motion, not just data at rest
- Faster time to respond to data risk
- Demonstratable actions, policies and controls to achieve compliance
- Up-to-date data inventory supporting incident response requirements

Risks of data loss prevention strategy and technology gaps

• Poorly protected data	• Increased cyber risk	• Increased Operational Risks
• Breach Liability	• Data Loss	• Reputational Risk
• Regulatory Non-compliance	• Incomplete data inventory	

Data Discovery

The practice of data discovery and classification varies widely and focuses on the unique types of information a business needs to track (like intellectual property, financial data or sensitive customer information), and the business’s individual industry requirements. Classification methods and outcomes vary too; while larger organizations have embraced data loss prevention (DLP) technology, smaller organizations with limited budget and internal resourcing rely on manual methods to keep track of their data.

The Challenge

Small and midsized businesses face ever-increasing regulatory pressure, data privacy requirements and cyber risk. They’re held to the same standards as larger companies and are expected to maintain up-to-date data inventories in accordance with data privacy and security regulations. Many businesses, especially utilities and municipalities, rely on manual data classification techniques like folder structures and meta data tagging. But those methods are prone to error, can’t scale and lack diligence, making the process next to impossible to audit and difficult to enforce.

On the other hand, larger companies have embraced DLP technology to provide classification capabilities and visibility to data leaving the network. However, the inline data suppression capabilities they offer are usually based on whitelisting and blacklisting, and push notifications after the data has left the network, rather than while it’s in motion and recoverable.

“We generate data faster than we can catalogue or classify it. However, at the same time we are mandated by the Ontario Energy Board to know what and where all of our data is. We have no solution for this but even if we did Cavelo’s platform has completely automated work that would probably take up to an entire FTE.”

— Mark Dillion, Waterloo Hydro

The Solution

Businesses need to rethink the way they’re managing data classification. Manual classification methods and unstructured data (databases) can’t keep pace with shifting use cases, escalating cyber risk and increasing regulatory pressures. DLP technologies are an improvement but come with limited functionality and lack real-time visibility. By adopting automated data discovery and classification solutions organizations can:

- Get control of their data
- Track and classify all data by type
- Better identify organizational risk based on data types and sensitivity
- Institute data integrity and access controls
- Understand the value of the business’s information to better mitigate risk and align to compliance requirements

Risks of limited and manual data discovery & classification capabilities

• Poorly protected data	• Out-of-date data	• Increased Operational Risks
• Breach Liability	• Data Loss	• Reputational Risk
• Regulatory Non-compliance	• Data Privacy Risks	

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. While suited for larger businesses, legacy and on-premises DLP technology can't service smaller organizations because of its cost. 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.

"Like many other businesses, moving operations to the cloud and managing a remote workforce makes data visibility and tracking a larger priority for overall data security. The Cavelo platform gives us complete visibility to sensitive data, so we can better protect it – all in line with industry compliance and security best practices."

– Dave Boyle, Guelph Hydro

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 businesses. 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.

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

Risks of insufficient data protection

• Poorly protected data	• Increased cyber risk	• Increased Operational Risks
• Breach Liability	• Data Loss	• Reputational Risk
• Regulatory Non-compliance	• Incomplete data inventory	

Data Privacy & Regulatory Compliance

Over the last decade global, regional and industry regulators have put frameworks, regulations and laws in place to protect citizen data and hold organizations accountable as custodians of personally identifiable information (PII). The introduction of the General Data Protection Regulation (GDPR) set a benchmark for data protection and data privacy requirements that continue to be replicated at regional, provincial and state levels.

All businesses are held to the same standard when it comes to compliance requirements and are expected to adopt a compliance mindset, but many small and mid-sized businesses lag behind their larger peers when it comes to implementing controls to achieve compliance.

The Challenge

Smaller enterprises are able to pivot and adapt to changing regulatory requirements faster than larger enterprises but designating a full-time resource to time-intensive data privacy programs isn't realistic for resource-strapped companies. As a result, the responsibility is usually divvied up between general counsel, product management or other roles that take on compliance-related tasks.

In smaller organizations data access and inventory is a problem. Limited controls mean too many people have access to sensitive data, while inconsistent data inventories make it hard to keep track of what data types are collected and who can access them.

Compliance is a mandatory requirement, not an optional exercise, so without appropriate policies and processes in place companies can fail compliance audits and face costly fines.

“Cavelo provides visibility into insights on where data exists both inside and outside the network, how it's classified and the value of the data. The platform allows security and compliance professionals to identify risks related to data exposure and drive decision making to ensure the security of their data.”

— Ben Tercha

The Solution

Cybersecurity and data privacy go hand in hand. Adopting a privacy-first mindset starts with understanding the basics of the data privacy regulations that apply to the organization. Every framework outlines pillars that define data rules, restrictions and controls. By understanding what types of data your business has, why your organization collects it and how data is used can help to:

- Establish data privacy and compliance programs
- Understand compliance requirements
- Instill a privacy-first culture across the organization
- Achieve compliance
- Provide customer reassurance

Risks of non-compliance

• Data Loss	• Data Privacy Risks	• Fines
• Breach Liability	• Reputational Risk	• Legal Action
• Regulatory Non-compliance	• Gaps in Policies and Procedures	• Penalties

Managed Service Provider (MSP) Third-Party Audit

When it comes to cybersecurity, organizations and their service providers are equally responsible for measures and cyber defenses that protect shared data. Attackers commonly use service and technology companies as access points to larger corporate targets, so instituting appropriate controls has never been more important for providers and their customers.

“Deployment was simple and the platform itself is easy to operate and easy to explain to team members. Managed Service Providers (MSPs) don’t have the expertise nor the skillset to manually manage data security. MSPs using other solutions underuse product features and miss out on value because they don’t know how to operate the product.”

– Vinod Paul

The Challenge

Organizations hire speciality firms to conduct MSP third-party audits. The audits support due diligence questionnaires (DDQs) that companies operating in regulated industries need, while also ensuring alignment to broader regulatory laws like the General Data Protection Regulation (GDPR) and state-level acts like the California Consumer Privacy Act (CCPA). Third-party audits are becoming more routine, yet they lack standardization and often vary depending on the firm conducting the audit or the customer requesting it.

Increased frequency and a lack of standardization makes completing audits and fulfilling requirements challenging for MSPs and vendors. In many cases several MSP employees support the audit, each handling a different section. The process is time consuming, and a lack of central expertise can create confusion, misalignment or worse – failed certification.

The Solution

Audit requirements will continue to vary depending on industry or individual regulatory requirements, but by centralizing and automating audit management capabilities MSP teams can:

- Standardize third-party audit processes
- Reduce staffing requirements to fulfill audit requirements
- Significantly reduce the time it takes to complete individual audits
- Achieve third-party audit certification
- Gain competitive advantage
- Meet growing audit requirements in highly regulated industries

Risks of audit misalignment, non-completion and failed certification

• Regulatory Non-compliance	• Competitive Disadvantage	• Reputational Risk
• Penalties	• Lost business	

Incident Response

Incident response is a playbook and process that businesses follow to manage a cyber incident or data breach. It's the first step to incident recovery. But like many cybersecurity functions, incident response capabilities vary widely depending on how established a business is and its level of security maturity.

The Challenge

Large enterprises with ample resources have well-staffed teams that monitor and react to cyber incidents. Team members specialize in the operations, legal and communications functions businesses need to react and handle incidents from incident discovery to public disclosure. Unlike large enterprises, midsize companies lack a dedicated budget, staff and in many cases, the foundational processes required to respond to cyber incidents. As a result, they're often caught off guard when an incident happens and struggle to respond, or resort to external support, losing precious time.

Cyber incidents happen on a regular basis and target businesses large and small. All companies need an incident response plan in place to be able to respond to incidents as they happen, limit damage and minimize downtime.

The Solution

Traditional incident response is a reactive process to repair any damage caused by a cyber incident. All of the processes, tools and technology used in incident response plans are designed to identify what happened and what data was compromised. The proliferation of data across company networks makes it harder for businesses to understand what data types they have, who has access to data and how their data is used. Without an accurate data inventory identifying whether data was accessed or compromised can be a frustrating and drawn-out process.

All businesses need to adopt a proactive approach to incident response that starts by discovering, classifying and tracking sensitive data that's used and stored within the organization. Ensuring an up-to-date data inventory supports:

- The creation of an incident response plan that's specific to your organization, its data types, unique regulatory drivers and reporting requirements
- Full visibility and an accurate inventory of sensitive data within the organization
- Ongoing reporting requirements
- Confidence in your team's ability to respond to and manage cyber incidents
- In-house or third-party forensics investigations
- Faster time to event mitigation
- Reputation management

Risks of limited or non-existent incident response capabilities

• Regulatory non-compliance	• Data loss	• Costly data recovery fines
• Reputational risk	• System downtime	• Financial losses due to ransoms
• Legal action	• Lost production time	


Understanding Industry Best Practices

To know where you need to go, you need to understand where you are.

A one-size-fits all cybersecurity solution just won't work, and that's because all businesses are unique in terms of their industry, size, regulatory requirements and overall security maturity. As a mid-sized organization, you're racing to implement the processes and controls that will help your business rank higher on the security maturity scale. But – what is security maturity, and where does your organization fit within its definition?

The National Institute of Standards and Technology (NIST) [cybersecurity framework](#) is arguably the most recognized and universal framework available, which is why the Cavelo platform aligns to the framework's classification and reporting guidance. The first iteration of the NIST cybersecurity framework was introduced in 2018, with a [data privacy framework](#) following two years later.

The frameworks are a companion to NIST's cybersecurity maturity model, a series of maturity tiers designed to help organizations identify where they fit in terms of their security processes and posture.



NIST Cybersecurity Framework CSF Tiers

Tier 4: Adaptive

Risk Management Process – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators

Integrated Risk Management Program – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.

Tier 3: Repeatable

Risk Management Process – Practices are formally approved and expressed as policy.

Integrated Risk Management Program – There is an organization wide approach to manage cybersecurity risk.

External Participation – There is an organization wide approach to manage cybersecurity risk.

Tier 2: Risk Informed

Risk Management Process – Risk management practices are approved by management but may not be established as organizational-wide policy.

Integrated Risk Management Program – There is an awareness, but an organizational approach has not been established.

External Participation – Generally, organization understands its role in larger ecosystem with respect to either its own dependencies or dependents, but not both.

Tier 1: Partial

Risk Management Process – Organizational cybersecurity risk management practices are not formalized.

Integrated Risk Management Program – Limited awareness of cybersecurity risk at organizational level.

External Participation – Organization does not understand role in larger ecosystem with respect to its dependencies or dependents.

Evolve Your Organization's Security Maturity

Implement initiatives that strengthen your organization's security maturity

Data protection, security maturity and regulatory compliance go hand in hand. A variety of initiatives can help teams align to best practices while building on their security maturity. But if you're a resource-strapped team, it's simply impossible to do everything at once. By aligning core initiatives to the purposes they serve in elevating your security maturity, you and your team can break down larger cybersecurity pieces into more manageable parts that you can build over time.

Understanding your data supports many downstream security considerations and helps keep your team's efforts more focused, practical and cost effective. Knowing what types of data you have, who has access to it and how it's used provides data-driven evidence that better supports decision making and demonstrates to stakeholders and auditors that you're taking appropriate steps to protect your business's sensitive data – and the privacy of your customers.



Achieving Security Maturity

The following chart breaks down core initiatives across three levels that when wholly implemented support a lighter compliance lift - and a hardened security posture.

Initiative	Function as it supports security maturity		
	Level 1: Basic	Level 2: Advanced	Level 3: Expert
Multi-factor Authentication Verifying systems access	Enable where possible	Required for core systems	Requirement for all systems
Data Discovery & Classification Understanding your data	Basic understanding of your data	Organization-level policy automation	Department-level policy automation
Data Backups & Recovery Basic incident readiness	Enable where possible	Requirement for core systems	Required for all systems
CIS Benchmarks Endpoint configuration best practices	Awareness and proactive planning	Implementing core components of the plan	Striving to be at least 80% compliance
Vulnerability Assessments Endpoint security best practices	Awareness and proactive planning	Patching criticals monthly	Patching criticals weekly
Incident Response Formal Planning	Awareness and proactive planning	Testing core systems quarterly	Testing all systems quarterly
Identity & Access Management Knowing who has access to your data		Core system focus	All systems focus
Encryption & Data Obfuscation Considering at rest data security		Protecting data from an operational perspective	Protecting data from a liability perspective
Secure Network Topology Hardening your network		Least privilege access model focus	Implementing zero trust networking
Penetration Testing Testing network and systems strength		Executing annually	Executing quarterly
Regulatory & Compliance Management Up-market business readiness		"Checking the boxes"	Ensuring strong internal operating competencies
Intrusion Detection & Prevention Permissions automation			Implementing software process controls
Data Loss Prevention (DLP) Data movement permissions			Implementing data process control
SIEM Log Aggregation Collecting log records from systems and services			"Checking the box"
Threat Activity Analysis (Threat Hunting) Analyzing log records from systems and services			Internally owning event detection and response
Managed Detection & Response (MDR) Managed security services			Externally owned event detection and response

Technologies and Solutions Selection

Today thousands of cybersecurity products and services span roughly 26 technology categories. As a mid-sized business, knowing where to start is overwhelming, especially when you have limited time to vet solutions, a limited budget, and limited bandwidth to manage it all.

The industry's current categories span capabilities that address the many layers that exist within modern IT infrastructure. This table captures the most common security capabilities and matches how the industry's most talked about technologies meet them.

Controls & Capabilities	CYBERSECURITY TECHNOLOGY SOLUTIONS					
	Asset Management Software	Data Loss Protection Software	Data Classification Software	EDR	XDR	Cavelo
Inventory & Enterprise Asset Control	•		•			•
Inventory & Control of Software Assets	•		•			•
Data Discovery			•			•
Data Protection		•		•	•	•
Secure Configuration of Enterprise Assets and Software	•	•		•	•	•
Account Management						
Access Control Management		•				•
Continuous Vulnerability Management						•
Network Infrastructure Management						•
Malware Defenses				•	•	•
Data Recovery						
Network Infrastructure Management						•
Network Monitoring and Defense						•
Security Awareness and Skills Training						
Service Provider Management						•
Application Software Security				•	•	
Incident Response				•	•	•
Penetration Testing						

The Cavelo Platform

When it comes to data discovery, classification and protection your team has to work with the limited resources you have, like spreadsheets or disparate toolsets. Cavelo is a simple platform designed to help you and your team get a handle on your company's sensitive data, so you can protect it - all through a single pane of glass.

The platform's key pillars and service integrations gives you the ability to customize its dashboard and features to match your unique business requirements and regulatory frameworks.



The Cavelo platform offers pricing that's easy on your budget, and right-sized for your business

Depending on the type of business you are and the industry you operate in your data protection and compliance requirements will vary. That's why the Cavelo platform is offered as a right-sized platform that can meet your needs today and scale with your business, regardless of how many data sources, cloud applications and endpoints connect to the network. Our pricing model is simple and starts based on the number of data sources you've got on your network..

Try before you buy

We're confident the Cavelo platform will change the way you think about data discovery and protection, and compliance reporting, which is why we offer a no strings attached 30-day free trial and affordable monthly subscription packages.

How it works

Getting started is simple - the Cavelo Discover Platform downloads in minutes, installing its lightweight agent for turnkey set-up and onboarding.



Want to give it a try?

Our solutions team would be happy to chat through your data protection requirements and help you decide if Cavelo is right for your business.

[GET STARTED TODAY](#)



CAVELO

Cavelo helps businesses proactively reduce cybersecurity risk and achieve compliance with automated data discovery, classification and reporting. Its cloud compatible data protection platform continuously scans, identifies, classifies and reports on sensitive data across the organization, simplifying compliance reporting and risk remediation. To learn more visit www.cavelo.com and follow @Cavelo_Inc.

www.cavelo.com

