

# Data Protection

## *Solutions Guide*



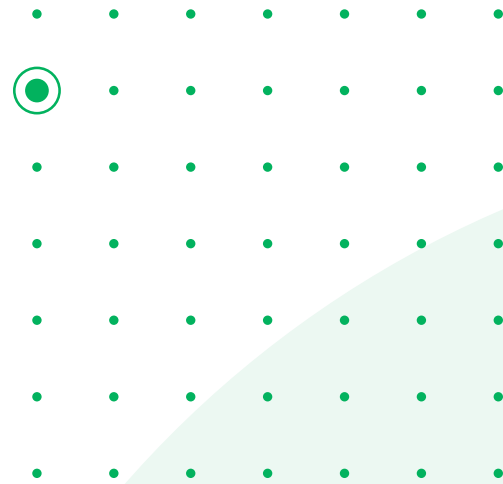
# How to Use This Guide

Data protection can be an overwhelming topic for IT teams. If you're an IT or security leader at a midsized 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.



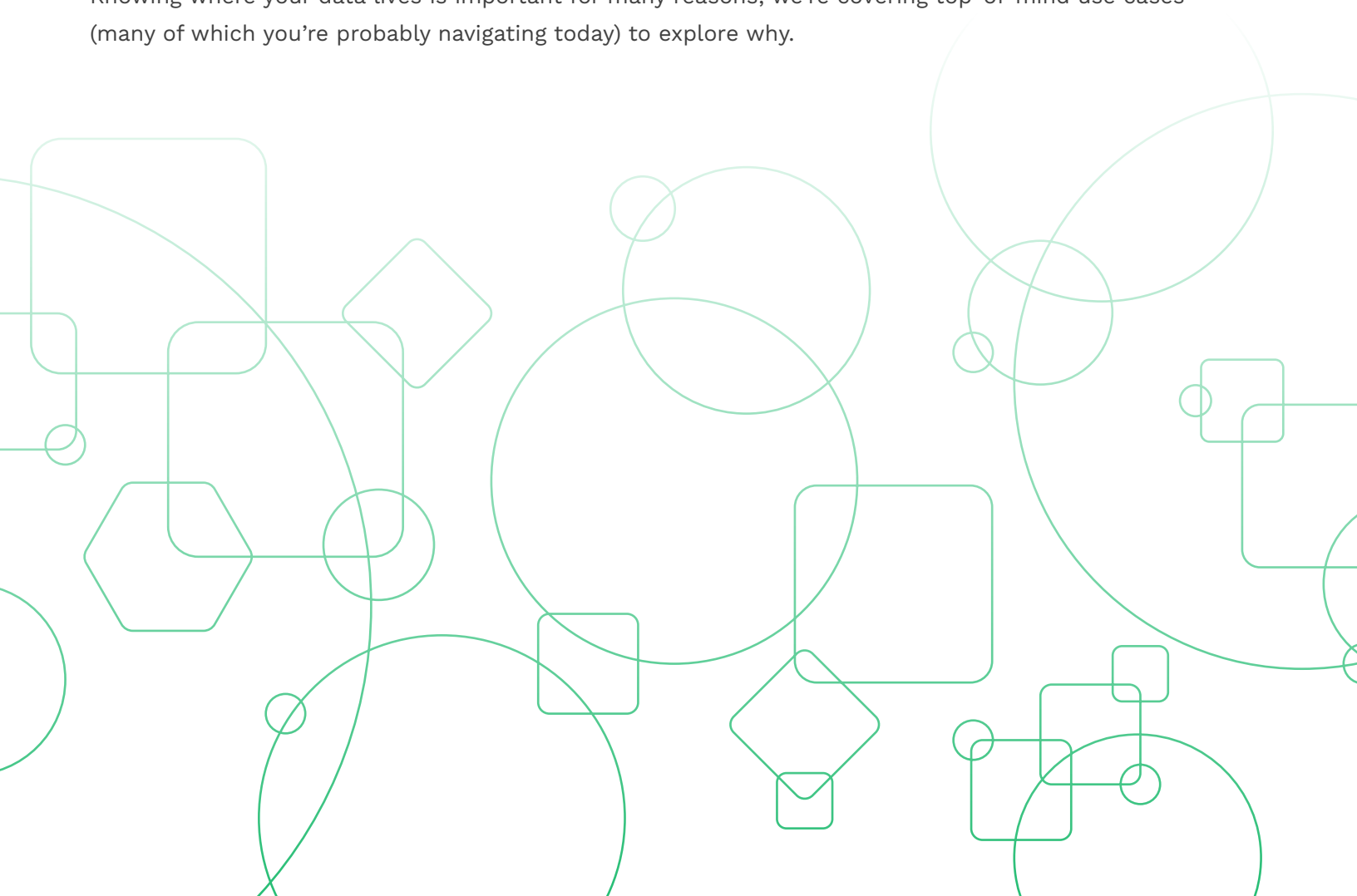
# Table of Contents

<b>New and Emerging Application Use Cases</b> .....	<b>4</b>
Use Cases from Cavelo.com .....	<b>5</b>
<b>Understanding Industry Best Practices</b> .....	<b>6</b>
<b>NIST Cybersecurity Framework CSF Tiers</b> .....	<b>7</b>
<b>Evolve Your Organization's Security Maturity</b> .....	<b>8</b>
Achieving Security Maturity .....	<b>9</b>
<b>Technologies and Solutions</b> .....	<b>11</b>
<b>The Cavelo Platform</b> .....	<b>12</b>

# 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.



# Use Cases from Cavelo.com



[Read on Cavelo.com](#) →

## CAASM

Swap costly spend and multiple data protection technologies for a simple, single pane of glass.



[Read on Cavelo.com](#) →

## Data Discovery

Meet shifting regulatory requirements and security use cases head-on with optimized data discovery.



[Read on Cavelo.com](#) →

## Data Loss Prevention

Get the visibility you need to protect your data and align to compliance requirements.



[Read on Cavelo.com](#) →

## Data Permissions

Strengthen your business's data access processes and get a wider view of your threat landscape.



[Read on Cavelo.com](#) →

## Data Protection

Institute industry best practices and align to compliance requirements.



[Read on Cavelo.com](#) →

## Compliance Reporting

Implement the policies and procedures your team needs to navigate routine audits.



[Read on Cavelo.com](#) →

## Incident Response

Understand the types of data your organization has and maintain an up-to-date inventory with Cavelo.



[Read on Cavelo.com](#) →

## MSP Third-Party Audit

Centralize and simplify audit management capabilities with Cavelo.

# 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.

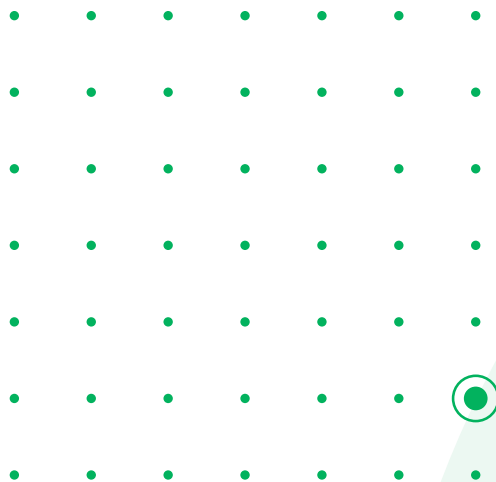
**External Participation** – Organization does not understand role in larger ecosystem with respect to its dependencies or dependents.

# 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

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

*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 Dillon**


Vice President of Information Technology  
**Waterloo North Hydro**



# Technologies and Solutions

Today thousands of cybersecurity products and services span roughly 26 technology categories. As a midsized 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.

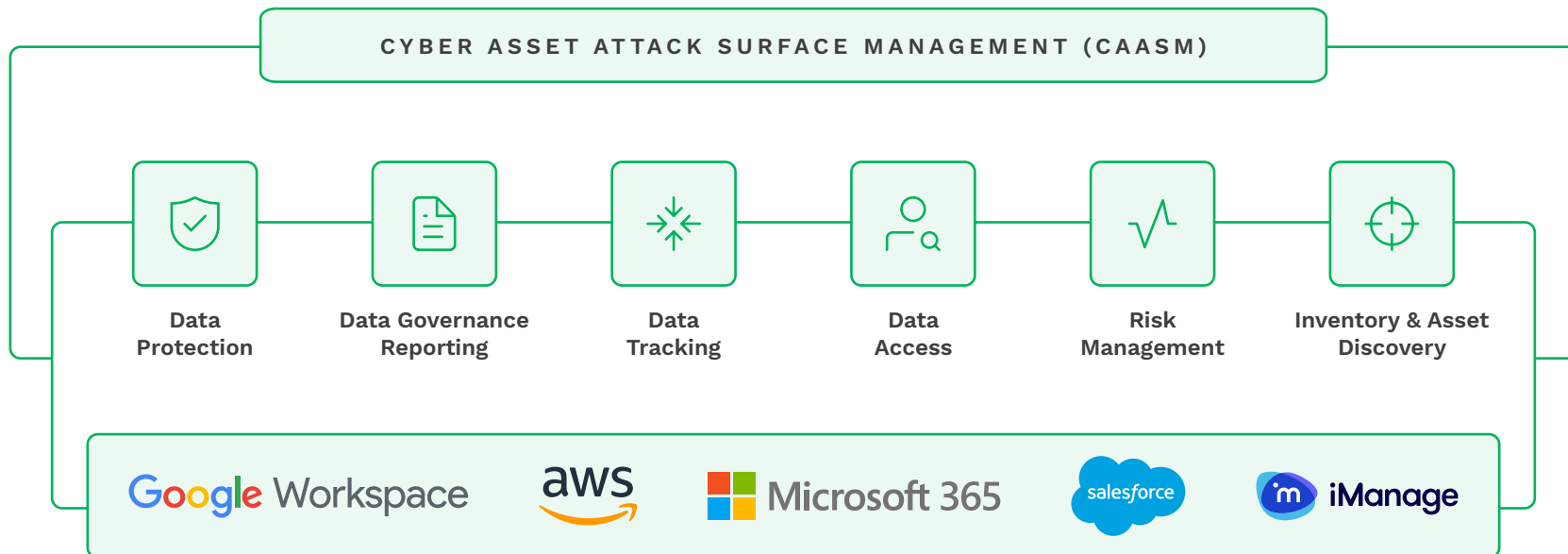
Controls and Capabilities	Popular Tech Categories					Attack Surface Management			
	Asset Management Software	Data Loss Protection Software	Data Classification Software	EDR	XDR	DRPS	CAASM	EASM	
Inventory & Enterprise Asset Control	✓	x	✓	x	x		✓	✓	✓
Inventory & Control of Software Assets	✓	x	✓	x	x		✓	✓	✓
Data Discovery	x	x	✓	x	x		x	x	✓
Data Loss Prevention	x	✓	x	✓	✓		✓	✓	✓
Secure Configuration of Enterprise Assets & Software	✓	✓	x	✓	✓		✓	✓	✓
Account Management	x	x	x	x	x		x	x	✓
Access Control Management	x	✓	x	x	x		x	x	✓
Continuous Vulnerability Management	x	x	x	x	x		x	✓	✓
Network Infrastructure Management	x	x	x	x	x		x	x	✓
Malware Defenses	x	x	x	✓	✓		x	x	✓
Network Monitoring and Defense	x	x	x	x	x		x	✓	✓
Service Provider Management	x	x	x	x	x		x	✓	✓
Application Software Security	x	x	x	✓	✓		✓	✓	x
Incident Response	x	x	x	✓	✓		x	x	✓

# Consolidate costly spend and multiple security technologies with Cyber Asset Attack Surface Management (CAASM) from Cavelo

As your business adds new digital assets (hardware and software), your overall attack surface grows, increasing cyber risk and the chance of a data leak or security breach.

Data is your business’s most critical asset. Getting visibility to the digital assets and sensitive data that’s used, stored, and shared across the tools and technologies you use is mission critical when it comes to aligning to security best practices, achieving compliance and keeping your data safe from risks.

Powered by machine learning, the Cavelo platform continuously scans your company’s cloud applications, cloud hosted servers and on-premises servers and desktops to identify, classify, track, protect and report on sensitive data.









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

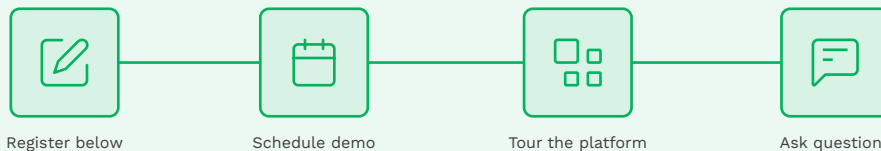
Depending on the type of business you are and the industry you operate in your data protection and compliance requirements will vary. That's why the Cavelo platform is offered as a right-sized platform that can meet your needs today and scale with your business, regardless of how many assets, data sources,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

Our pricing model is simple and based on the number of data sources and employees your business has.

### Seeing is believing. Within hours of deploying Cavelo, you'll see:

- 
**ROI**  
 Get valuable data that you can take to your leadership or decision makers.
- 
**Competitive review**  
 We're not shy! Compare us to the software or tools you're using today.
- 
**Immediate value**  
 Let your team members test it too to make sure Cavelo is right for you!
- 
**Use case vetting**  
 Test the product against all of the use cases your team handles.
- 
**Full functionality**  
 Access full platform functionality and our team of experts who can help you along the way.
- 
**Real reports**  
 Run reports (even in trial) that you can review and share with your team.

### Get started with a live demo



We're confident the Cavelo platform will change the way you think about data discovery, data protection, and compliance reporting. Book a 20-minute demo with our team of experts to learn about managing your company's digital assets and sensitive data, all through a single pane of glass.

Request a demo