constellation

a partnership between

nuwave & ALLENDEVAUX & COMPANY

"Together we aim to solve data protection challenges, increase security for businesses, and provide high value services for as little as one headcount a month."

www.nuwave.com

About Constellation

Constellation provides the best place for businesses to find all the privacy, security, and full-service compliance needs **in one place without juggling between the service providers**.

The platform provides million-dollar valued **services attainable for any size organization**.

Businesses can find the end-to-end services from ISO implementations to Data Protection services, all in one place.

Global Challenge

93% of company networks can be penetrated by hackers[1] with a 243-day average to detect the event and 84 days to contain it.[2]

Businesses and their customers are at risk to cyber threats and hackers and require adequate defenses.

Businesses can't keep up with constant compliance changes across various geographies, especially without third-party help.

There is a lack of customizable compliance and privacy solutions. Businesses are forced to pay for more than they need.

Your business loses out on growth when you're not in compliance with new regulations.

[1] Positive Technologies. (2021). *Positive Technologies: Cybercriminals Can Penetrate 93% of Local Company Networks, and Trigger 71% of Events Deemed 'Unacceptable' For Their Businesses.* Retrieved from https://www.ptsecurity.com/ww-en/about/news/positive-technologies-cybercriminals-can-penetrate-93-of-local-company-networks-and-trigger-71-of-events-deemed-unacceptable-for-their-businesses/

[2] IBM. (2022). *Cost of a Data Breach 2022 Report.* Retrieved from https://www.ibm.com/downloads/cas/3R8N1DZJ, page 18.

It Won’t Happen to Me

It’s not if, it’s when. Everyone thinks that they’re unlikely to be the victim of a cyber-attack until it hits close to home, it could be anyone.

Data breaches are **at an all-time high** and new ransomware attacks are on the rise. The need for stable security is more urgent than ever.

The estimated **annual cost of cybercrime in 2022 was $8.44 trillion USD.**[1] In the United States the average cost of a data breach was $9.44 million in 2022[2].

[1] Statista. (2022). *Estimated cost of cybercrime worldwide from 2016 to 2027*. Retrieved from https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide/

[2] Statista. (2022). *Average cost of a data breach in the United States from 2006 to 2022*. Retrieved from https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/

The Reality of Today

Australia's largest health insurer, **Medibank, was victim of a $10M (USD) ransomware attack**. The overall cost of this breach, according to Bloomberg Intelligence analysts, will likely **cost the company an estimated $640 million (USD)**.

Customers Whose Data Was Leaked:

9.7 Million

500,000 Confirmed Unlawful Record Retrievals

Sheehan, M. (2022, November 20). *Medibank hackers release 1,500 more sensitive medical records.* Sydney Morning Herald, Retrieved from https://www.smh.com.au/business/companies/medibank-hackers-release-1500-more-sensitive-medical-records-20221120-p5bzpk.html

The Reality of Today

A gargantuan leak involving **200 hundred million Twitter users was unveiled in January 2022**. 5 million users had leaked email addresses, names, and phone numbers. 195 million users had their emails were leaked.

Affected People:

5 Million (Account Info)

195 Million (Emails)

Newman, L. (2023, January 6) *What Twitter's 200 Million-User Email Leak Actually Means*. WIRED. Retrieved from https://www.wired.com/story/twitter-leak-200-million-user-email-addresses/

The Reality of Today

LastPass, a password management service, recently had a large data breach involving compromised accounts and leaked credentials. Now customers are left with a mess and abandoning the service.

Affected Accounts:

33 Million

Page, C. & Whittaker, Z. (2022). *It's all in the (lack of) details: 2022's badly handled data breaches.* TechCrunch. Retrieved From https://techcrunch.com/2022/12/27/ badly-handled-data-breaches-2022/

Service Offerings

ISO Implementations

Incident Management

Internal Audits

Data Protection as-a-Service

How Can You Get Started?

1

Start an Informal Conversation.

2

Discovery of your organisation's current state.

3

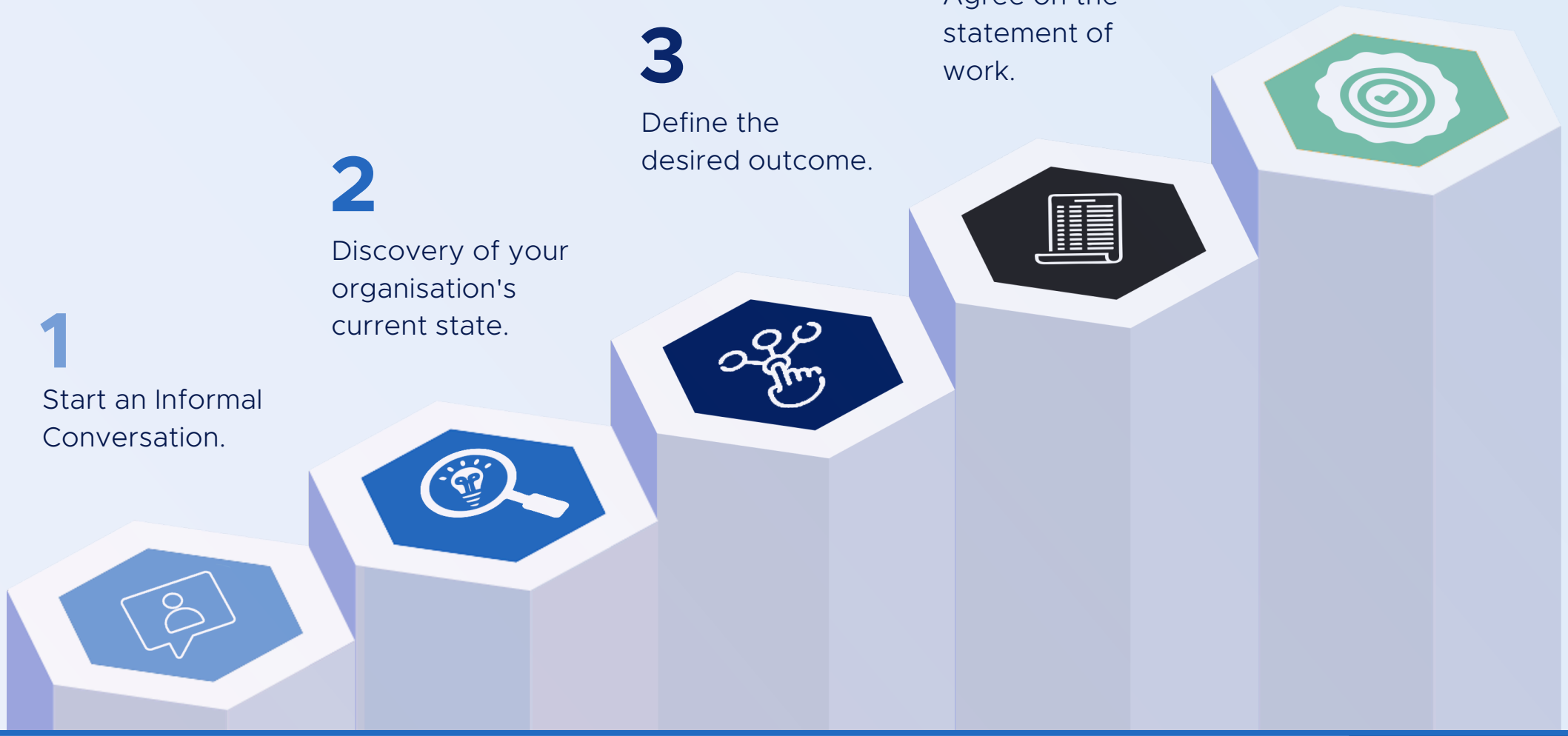
Define the desired outcome.

4

Agree on the statement of work.

5

Beginning the path to full-compliance.



Back to Service Diagram

ISO Implementations

Work With Our Experts

Pathway to Certification

Implementations create frameworks for your business to reduce risk, save costs, and protect your business.

We develop strategies to thwart threats to your business such as phishing, ransomware and social engineering.

Our 7-Step Process for ISO Implementations

KICK OFF

Planning and hosting kickoff, identify key stakeholders and building online project environment.

RISK ASSESSMENT

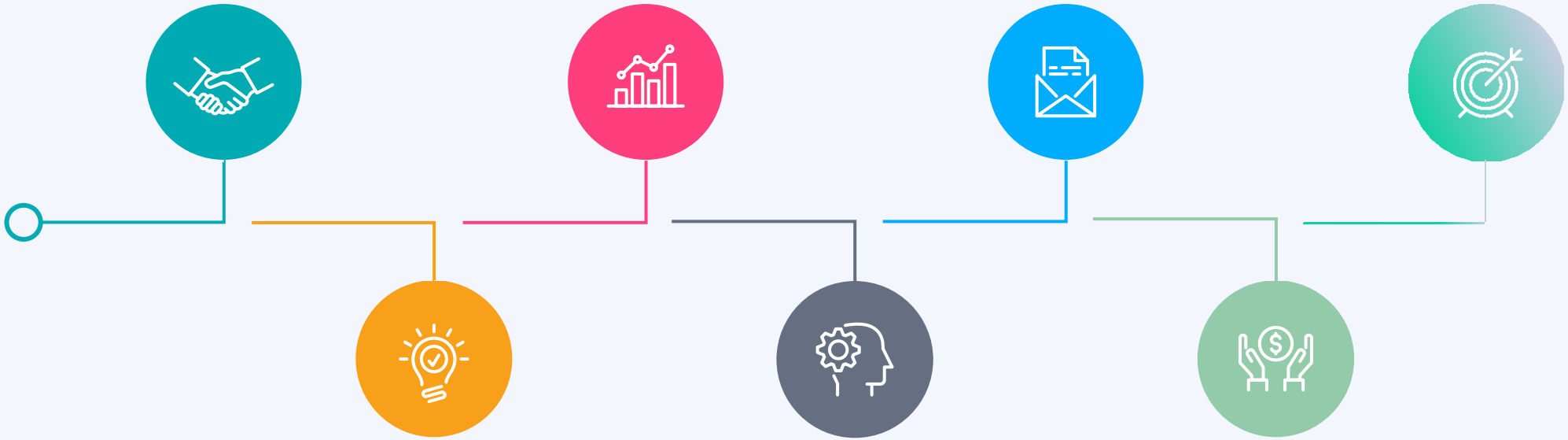
Perform ISO 27005 risk assessment, inventory assets, develop risk criteria, identification of threats, sources and overall impact.

CYBER CAMPAIGN

Conduct a cybersecurity campaign, perform vulnerability scanning, spear phishing, penetration testing and more.

INTERNAL AUDIT

Conduct an internal audit, measure implementation, prepare organization to be audited by a third-party for certification.



DISCOVERY

Set up interviews, develop compliance requirements and contractual obligations.

INTERNAL CONTROLS

Build the ISMS, integrate ISO 27002 control objectives, develop the BCD plan and more.

TRAINING / AWARENESS

Launch awareness campaigns, specialized training courses, and record performance.

ISO Implementations

ISO 27001:2022

What Is It?

System for assessing risk, protecting data and preventing data breaches.

How Is It Achieved?

~9-12 month engagement, for as little as one headcount.

Who Needs It?

All organizations looking to protect their data from breaches and leaks.

ISO 27001; Information Security Mgmt. System

One-third of the ISO 27001 program concerns technical policy and practices, such as vulnerability scanning, how cookies are managed and tracked, the security of web portals and APIs, and penetration testing, to name a few areas.

Implementing ISO 27001 means your organisation is implementing a data protection program, resulting in real world benefits:

- It reduces security threats and protects again data breaches.
- It simplifies the vetting process for customers to use your service, including the simplification of questionnaires.
- It protects against regulatory fines, because laws require service providers to implement a written information security program, and ISO 27001 demonstrates due diligence and due care to safeguard the data it collects and processes.
- It protects the company's reputation, demonstrating to stakeholders that information security is taken seriously.
- It creates a security-focused culture to ensure everyone within the organisation takes security seriously, doing their part to safeguard customer data.
- It provides an independent attestation of the company's policies and practices, conveying trust and assurance to customers that your service has implemented data protection best practices.
- It leads to supply chain assurance by ensuring suppliers implement flow-down terms from your organisation's data protection program.
- It leads to improved processes by implementing policies and procedures that are consistent, repeatable and maintainable, following an international framework of best practices.
- It results in continual improvement, because once implemented, the organisation strives to improve the system, the protection of assets and compliance with changing laws.
- It fosters worldwide recognition because the organisation has implemented an international standard respected globally.

ISO Implementations

ISO 27017:2015

What Is It?

Security controls to prevent compromised cloud services

How Is It Achieved?

~6 month engagement, for as little as one headcount.

Who Needs It?

Necessary for cloud service consumers and providers.

**(Supplement to ISO 27001)*

ISO 27017; Cloud Security Mgmt. System

Industry experts agree that an ISO/IEC 27017:2015 implementation provides additional safeguards for data transmitted to and processed within the cloud that is not adequately addressed with ISO/IEC 27001.

The cloud service provider that implements ISO/IEC 27017 will see many benefits, including:

- Reduction of risks that would otherwise lurk in the shadows of an ISO/IEC 27001 organization.
- Competitive advantage in the cloud services industry compared to others who do not implement the additional safeguards to protect data in the cloud.
- Cultivating trust that rises from greater assurances that data is protected in transit, in storage and in processing.
- Protection of reputation that otherwise arises when data breaches damage brands because trust has been damaged.
- Protection from financial loss that might otherwise impact the business that is victim to breach of confidentiality or availability, resulting in customer attrition.
- Protection from regulatory fines imposed by supervisory authorities that find insufficient protections in place for the type and kind of services marketed to customers.

ISO Implementations

ISO 27018:2019

What Is It?

Guidelines and controls for handling personal data via cloud services.

How Is It Achieved?

~6 month engagement, for as little as one headcount.

Who Needs It?

This is for cloud service providers.

**(Supplement to ISO 27001)*

**(Supplement to ISO 27017)*

ISO 27018; PII in the Cloud Mgmt. System

ISO 27018 is part of the ISO 27001 family of standards, expanding Annex A with additional controls. The standard was first introduced in 2014 and updated five years later in 2019 to align with the privacy principles of ISO/IEC 29100 for public cloud computing and to reflect lawful requirements in recent data protection law such as the GDPR and the CCPA.

ISO 27018 also spans 18 sections with the following objectives:

- Helps the public cloud service providers to comply with applicable obligations when acting as a PII processor, whether such obligations fall on the PII processor directly or through a contract.
- Enables the public cloud PII processor to be transparent in relevant matters so that cloud service customers can select well-governed cloud-based PII processing services.
- Assists the cloud service customer and public cloud PII processors in entering into contractual agreements when PII is processed in the cloud.
- Provides cloud service customers with a mechanism for exercising audit and compliance rights and responsibilities in cases where individual cloud service customer audits of data hosted in a multiparty, virtualized server (cloud) environment can be impractical technically and can increase risks to those physical and logical network security controls in place.

ISO Implementations

ISO 27701:2019

What Is It?

The latest standard to protect personal information.

How Is It Achieved?

~6 month engagement, for as little as one headcount.

Who Needs It?

Organizations who manage or store large amounts of personal information.

**(Supplement to ISO 27001)*

ISO 27701; Privacy Information Mgmt. System

While ISO/IEC 27001:2013 refers to policy and practice that can protect any kind of confidential information, a more recent standard relates to the rights, freedoms and protection of personal information: ISO/IEC 27701:20193.

- Privacy and security are two related but different domains.
- While security ensures data—any kind of data—is not compromised, privacy concerns the confidentiality of data about living people.
- Known as personally identifiable information (PII), over 100 countries around the world have enacted laws requiring organisations to protect PII about its citizens.
- Failure to implement prescribed protections can result in steep fines. Because an individual's life can be fully reflected online, it can also be lost and destroyed online without sufficient mitigating measures

ISO Implementations

ISO 22301:2019

What Is It?

Business continuity ensures your organization continues to run smoothly even in a crisis.

How Is It Achieved?

~12 month engagement, for as little as one headcount.

Who Needs It?

Critical infrastructure providers or organizations requiring high-availability.

ISO 22301; Business Continuity Mgmt. System

ISO 22301 is an international standard for Business Continuity Management (BCM). It is designed to help organisations to prevent, prepare, respond & recover from disruptive and unexpected incidents.

ISO 22301:2019 is the latest standard that was published on 31st October 2019 as a revision to the existing ISO 22301:2012 to streamline the requirements and convert them to more practical as it consists of less repetition, discipline-specific business continuity terms and more

The specific benefits of ISO 22301 standards for the organisation:

- Improving overall efficiency–Implementing the ISO 22301 standard allows organisations to improve recovery time when a disruption arises
- Identifying potential risks – ISO 22301 is aligned with BCMS; organisations proactively identify threats, assess the impact and measure to mitigate and eliminate them.
- Flexibility – having a business continuity plan ensures the operations run during disruptive incidents.
- Legal Compliance – ISO 22301 is used for legal and regulatory certification of BCM and ensures that the organisation meets the requirements and standards.
- Market advantage – Establishes brand reputation by building credibility with certification.

Back to Service Diagram

Audit Services

Our Certified Professionals

Maintain Evidence of Compliance

Ensure your implementation was successful and remedy any non-conformances. Prepare for a strenuous third-party audit.

Show the world your organization complies with international standards and regulations and stand apart.

Audit Services

Why would your organization need an internal audit?

It might be a legal requirement.

If your company operates in a specific region or industry, you're legally obligated to have your implementations audited.

You need to prepare for an upcoming 3rd-party audit.

If your company operates in a specific region or industry you're legally obligated to comply with regulatory standards.

Drive Continual Improvement

An internal audit is a great way to safely discover oversights from an implementation and prescribe solutions.

Gain insights with an executive summary and boost performance.

Measure goals and keep a record of your organization's efforts. Get an executive summary for review and recommendations.

Audit Services

We have two styles of internal audits:

Standalone Internal Audit

A one-off engagement to satisfy a scope, usually scheduled prior to an external audit.

Internal Audit as a Service

We provide monthly internal audits as a subscription instead of a one-time, standalone audit.

Current implementations we'll audit:

ISO/IEC 9001
Quality Management System

ISO/IEC 14001
Environmental Mgmt. Sys.

ISO/IEC 20000
Service Mgmt. Sys.

ISO/IEC 22301
Business Continuity Mgmt. Sys.

ISO/IEC 27001
Information Security Mgmt. Sys.

ISO/IEC 27017*
Cloud Security Controls

ISO/IEC 27018*
Cloud Privacy Controls

ISO/IEC 27032
Cybersecurity Mgmt. Sys.

ISO/IEC 27701
Privacy Information Mgmt. Sys.

ISO/IEC 28000
Supply Chain Security Mgmt. Sys.

ISO/IEC 45001
Occupational Health & Safety Mgmt. Sys.

ISO/IEC 55001
Asset Mgmt. Sys.

*ISO/IEC 27017 & ISO/IEC 27018 are audited within an ISO/IEC 27001 implementation.

Audit Services

Typical end to end flow of an audit:

We Perform Steps 1 & 2

Officially passing an audit is achieved at the external audit stage.

We help organizations with preparation and performing internal audits to maintain evidence of compliance.

Back to Service Diagram

Data Protection as a Service

An Inclusive Package

Full-Service Compliance

Data Protection as a Service (DPaaS) includes everything we offer on a subscription basis. This includes recurring audits and improvements.

Your organization is supported by a full data protection team of experts. This includes legal and technical personnel – attainable for as a low as one headcount.

Data Protection as a Service

Get everything you need in one place without breaking the bank.

Ongoing Service

Continual upkeep and improvement.

Scalable Pricing

Attainable pricing for any org. size.

Always Ready

We keep auxiliary staff for global availability.

Fulfilled by Certified Experts

Our experts stay up to date with the latest global standards and regulations.

Services (Maintenance & Audits):

ISO 27001

ISO 27017

ISO 27018

ISO 27701

Access To:

Security Incident Response Team

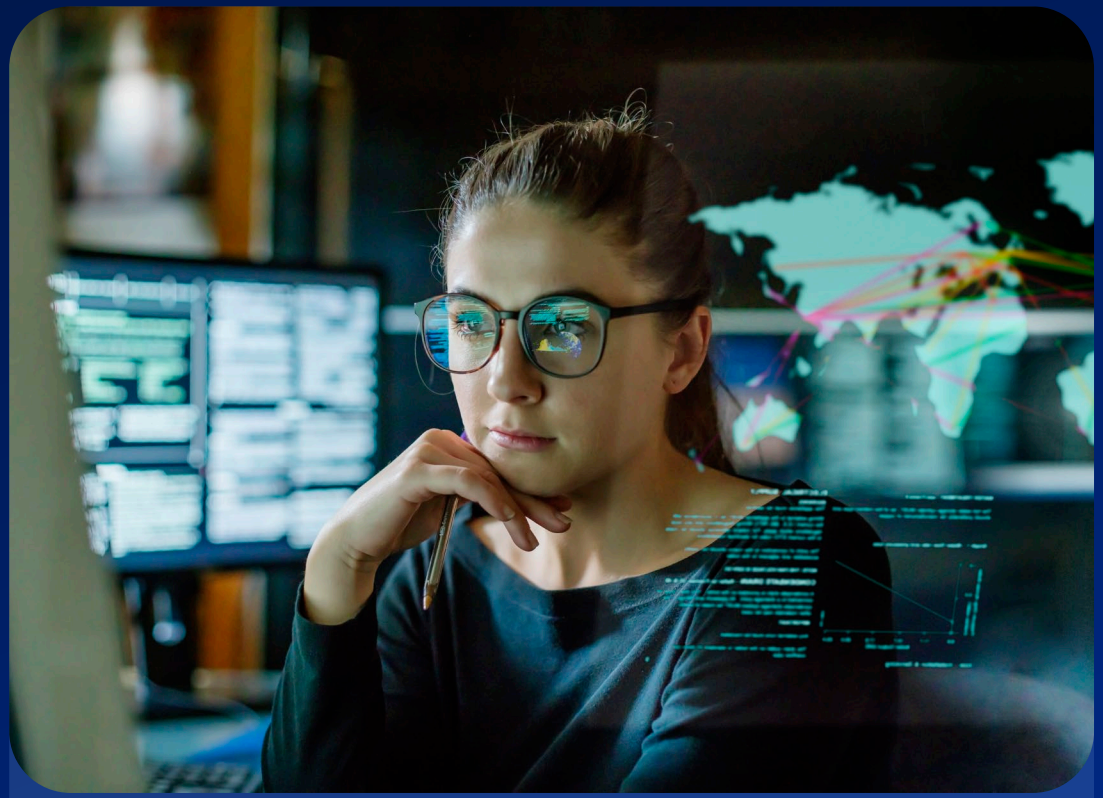
On-Call 24/7 Rapid Emergency Response

Data Protection Officer Pool

Shared legal experts who are always ready

Back to Service Diagram

Incident Management



24/7 Rapid Response Team

Security Incident Response Team

Our global team will move from detection to recovery as quickly as possible, all managed through tracked ticketing.

We perform cyber forensics and investigations to identify the source of the incident and provide a legal analysis to understand implications.

Incident Management

Report and Track Security Events

Pair our monitoring with internal reports.

24/7 Rapid Response

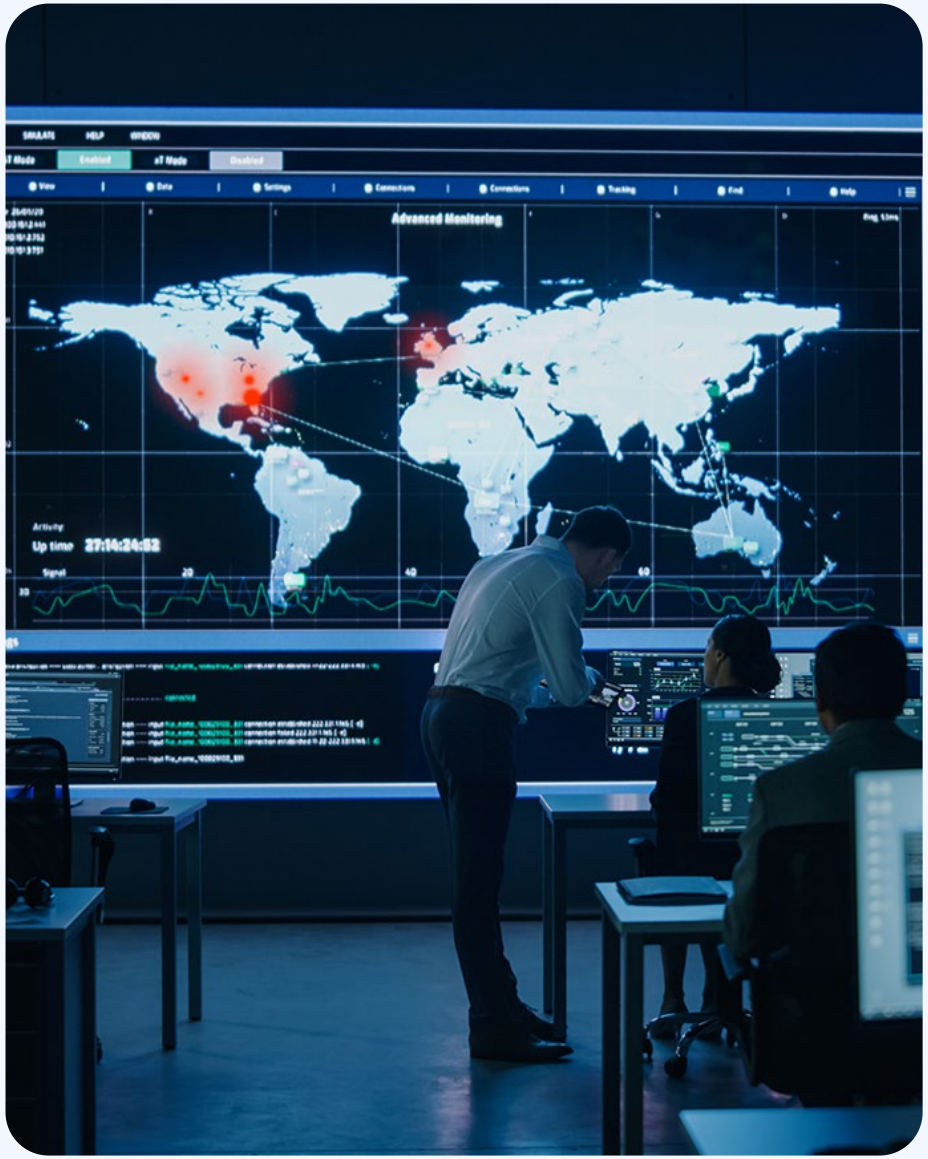
Our global team is prepared to handle a crisis at any moment.

Training and Awareness

We train your personnel recognize and report suspicious activity.

Setup Cyber Insurance

Data breaches can be expensive, mitigate the cost of security events with insurance.



Changing How Organizations Protect Their Business

Save and Simplify Your Data Protection Efforts

- Cybersecurity, Privacy, and Compliance in one place
- Benefit with a Full-Service Team
- Global Data Privacy and Compliance Legal Department
- Certified Cybersecurity Experts
- Certified Auditors and ISO Implementors
- 24/7 Cyberattack Response Team (SIRT)

constellation

Scan to Get Started

Get in touch and keep your business safe.