Insight's Data-Centric Security Guide

Introduction

At Insight, we recognise the importance of a holistic approach to security. Attackers will look for your weakest area, not your strongest. We have technical expertise in the five technology domain areas (Endpoints, Applications, Cloud, Network, Datacentre and IOT, and Data-centric) – but as a leading solution integrator, we believe you should also pay close attention to the interactions between these technology domains (Governance, Risk and Compliance, Identity and Access, Threat Detection and Response, and Human Factors). The gaps where the technology domains connect are often where additional value can be achieved, helping improve your overall security posture in a cost-effective manner.

Insight's holistic security model

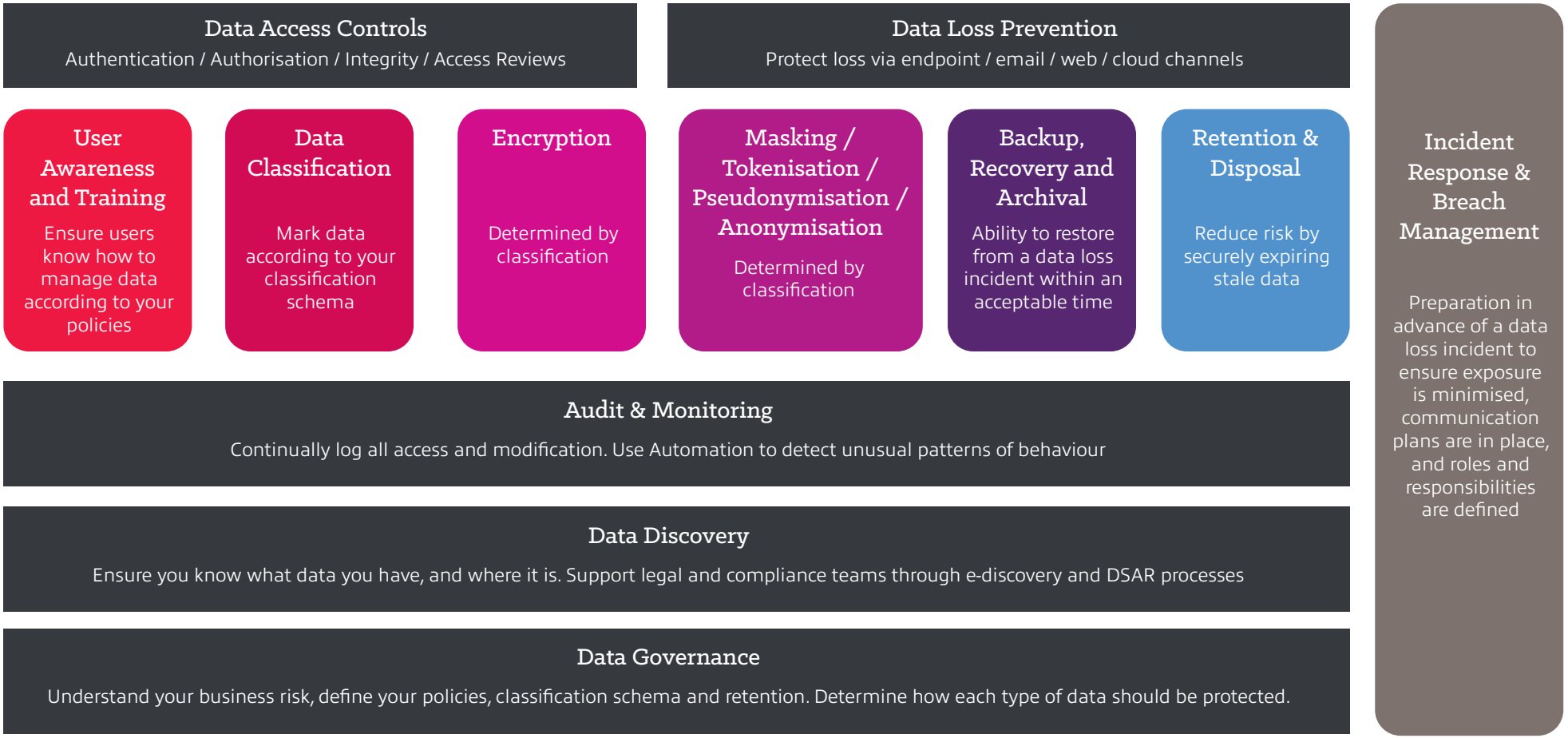
What is Data-Centric Security?

Data-centric security involves implementing security controls and measures that directly protect the data itself, ensuring its confidentiality, integrity, and availability. The goal is to secure data at rest, in transit, and in use, regardless of the storage medium, network infrastructure, or applications involved.

Traditional perimeter based security is no longer sufficient or sustainable when most of the people who access and use the data reside outside of the corporate network.

There are various components that demand attention within data-centric security and others which are optional. Each business will have their own unique security requirements. We explain each component using our data-centric security model in this guide.

Insight's Data-Centric Security Model



Key considerations in Insight's data-centric security model

While security professionals spend a lot of time on securing applications and infrastructure, ultimately, almost everything we do boils down to securing data. Whether it's employee information, client orders, production figures or intellectual property, it's the data moving around your business that is likely adding most value for your end customers and business.

A good place to start when thinking about your holistic security strategy is with data, and a data-centric approach should begin by engaging your business stakeholders, not with technology.

Data Security Governance

Too much security can be as damaging to organisations as not enough, frustrating users and slowing business processes. On the other hand, every organisation must meet a minimum level of security by law, with many industries requiring additional tiers of protection for example as prescribed in PCI-DSS or NIS2. Matching your security strategy to your business strategy is part of Data Security Governance and should be the root of all the technical decisions which follow.

Data Discovery

Businesses have generated vast amounts of data over the years and this will only increase in the future. This data may reside in a variety of locations, such as on-site servers, cloud storage, and various backup and disaster recovery systems. It could be organised in structured databases or exist in an unstructured format in uncontrolled environments such as laptops.

Gaining visibility over what data you have and where it is will be critical to everything that follows, and we call this Data Discovery. There is a tendency to hold onto data for longer than is required "just in case" and while this data may now hold very little business value, it can represent a significant business risk should it be lost, misused or stolen. Finding and securely disposing of this 'stale' data can reduce both cost and risk, and make the following steps in your data security journey simpler.

Audit and Monitoring

Now you know where all your data is, you can ensure that any access to it is both monitored and audited. A minimal level of auditing is required to be able to see who is using the data and how, which provides a useful retrospective view after an incident – but more useful, is to provide a continuous monitoring based approach to user behaviour.

Various machine learning techniques can be applied to identify unusual access to data outside of typical hours, or large volumes of data movement, which can flag a potential breach is in progress and allow you to respond more quickly when an incident occurs.

Whilst a lot of data is processed in automated methods by machines, it is the use of data by people which represents the greatest risk. Users don't have to have malicious intent to cause risk, they can be well-meaning and still cause damage.

User Awareness and Training

User awareness and training is often overlooked when it comes to data, but time spent up front on this activity can mean the difference between a successful or a failed implementation.

Consider the situation where an employee sends work-related data to a personal email address for after-hours work. This action moves the data beyond the organisation's control. To prevent such issues, it's crucial to educate staff on correct data handling. Understanding how upcoming changes may affect business operations is also essential for the success of any data security initiative

Data Classification

Not all data has the same value or risk, so it shouldn't all be treated like the crown jewels. As part of your data governance work from the outset, you should have defined a data classification schema. This will outline the broad categories of data your users will be working with, and how each type of data should be protected.

Now its time to start applying sensitivity labels to your data which indicates to users and various automated security controls how that data should be treated.

Encryption

One way that more sensitive data might be treated is through the use of encryption. This allows for a granular control of who can see and use the data in its original format, which decreases the risks if the data should fall into the wrong hands, for example if a laptop is stolen. You should consider encryption for data which is; at rest (sat on storage systems waiting to be used), in motion (flowing across a network), or in use, maybe stored in memory while it is being processed.

Masking

Masking is another control that can be applied to data, as an example, hiding the first 12 digits of a credit card number when displaying on screen to a contact centre agent.

Tokenisation

Tokenisation is a process of replacing the actual sensitive values with a unique but meaningless value in a less secure database, where the original sensitive data is stored elsewhere in a more secure area that has more restrictive access.

Pseudonymisation

Pseudonymisation is similar to tokenisation, an example could be in court records released to the public which talk about "Witness 23". With the right access to the data mapping, the original name could be retrieved, but for most purposes, privacy can be maintained.

Anonymisation

Anonymisation is a further step where any personal data is stripped and removed in a way which is non-reversable. For example, "12% of male patients suffered an adverse reaction to a drug" could be an anonymised summary of a medical trial.

Backup and Recovery

While security often focuses on the confidentiality (privacy) of data, and the integrity (tamper-resistance) of data, availability is also a key tenet of security. If critical data is unavailable, whether that be due to a hardware failure, or a ransomware attack, it can have devastating impacts on an organisation's ability to operate. Backup and recovery procedures are required, they need to be well defined and well tested to ensure that data can be reliably recovered in a timeframe that allows business operations to continue.

Retention and Disposal

A key element of the lifecycle of data is secure disposal of data which is no longer needed. This could form part of a formal data retention policy to delete financial data after the legally required period expires, or to delete customer data as part of a GDPR "right to erasure" request. Erasing data in a way which is non-trivial to recover, and ensuring all copies of the data including backups are put beyond reasonable use and an audit log is maintained.

Access Controls

An important consideration which falls outside of data security but is critical to it is that of identity. Identity allows for access controls, where data is only accessible to the people or systems who are authorised to view it. Role based access control allows for granular restrictions on groups of people and specifies how data may be accessed, e.g. read but not write.

Data Loss Prevention (DLP)

Data loss prevention acts as a backstop for data which is being used outside of defined policies. Sending confidential data outside of the corporate boundaries, or cross-contamination of client A's information being accidentally sent to client B are examples. DLP can alert a user to the potential breach condition, or in many cases can prevent the user from taking the action. It should be considered at multiple points – for example on emails, web traffic, access to cloud repositories and on endpoints to prevent data being copied to USB sticks.

How Insight can help

Insight's Data Security Posture Assessment provides a comprehensive overview of your organisation's data security posture and delivers clear, detailed advice on effective actionable plans for improvement.

Our data and security focused experts will evaluate your current data protection, governance, and privacy measures to identify risks. We will document how well your current data posture enables you to classify, protect and govern your data across your on-premise, cloud, and hybrid/multi-cloud environments.

By accurately determining your data posture and your existing data controls and processes, we enable you to confidently implement the most appropriate data compliance plans, controls and processes to maximise your return on investment.

Following on from the Data Security Posture Assessment, Insight can help you with the technology acquisition, implementation, and adoption and change management of a data security solution tailored specifically to your needs. requirements.