Unissant White Paper Series

Data Security– Unissant Cyber

Data Security–Unissant Cyber

Data, the digital building blocks of information, are a valuable corporate asset outlasting applications and processes. Data are used as input into tactical and strategic decisions. Analysis and management of data allow organizations to learn and grow. Data are received from and transmitted to customers and business partners. Data are reported to investors and regulators and used by the media. Data flow through every process your organization runs and are used by every individual your organization employs. As important as your central nervous system is to your body, data are to your organization. Data signal when you should move, how fast, and in what direction. If those signals are infected, corrupted, or stolen, you may find yourself paralyzed into inaction, moving in the wrong direction at the wrong speed, or see a competitor take your Intellectual Property (IP) and dominate a market.

Ideally, an organization should aim for protecting all their IP. Unissant recognizes that desire for some organization to protect all their data while at the same time we understand the constraints that come into picture trying to do so. One such constraint is the resources required to protect ALL data at the highest level. Thus, we assist organizations in prioritizing their data protection strategies based on proven frameworks and methodologies tested in both the government and financial industry. We start with multiple factors using probing questions and then lead our customers through our process to discover what data needs protecting and at what level is appropriate based on the data.

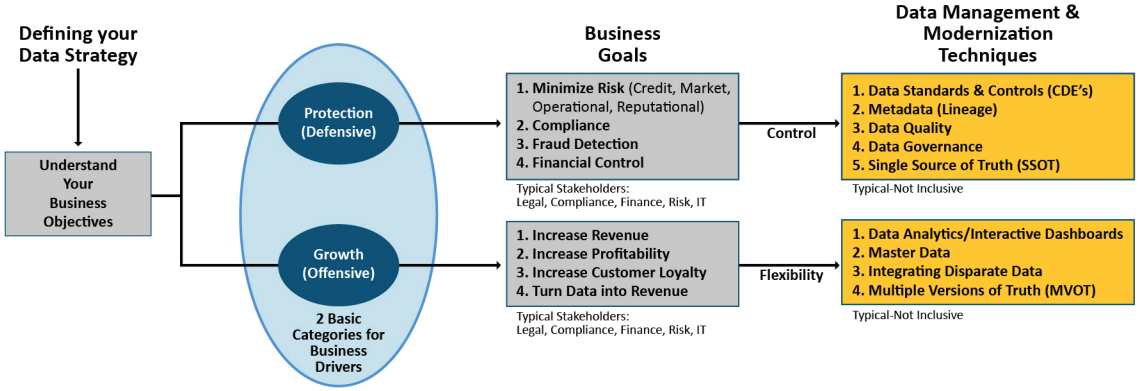
When speaking with organizations about data security, we often start with some high-level questions like below:

- How will you do it?
- Who must be involved?
- Where will it be stored?
- What data needs to be protected?

These are very high-level important questions but, often with long government decision trees, the biggest question gets delayed…*when will it be protected?* Unissant has developed frameworks and partnership with data loss prevention leaders to start protecting data on day one while developing data governance within the organization to narrow down what needs to be protected.

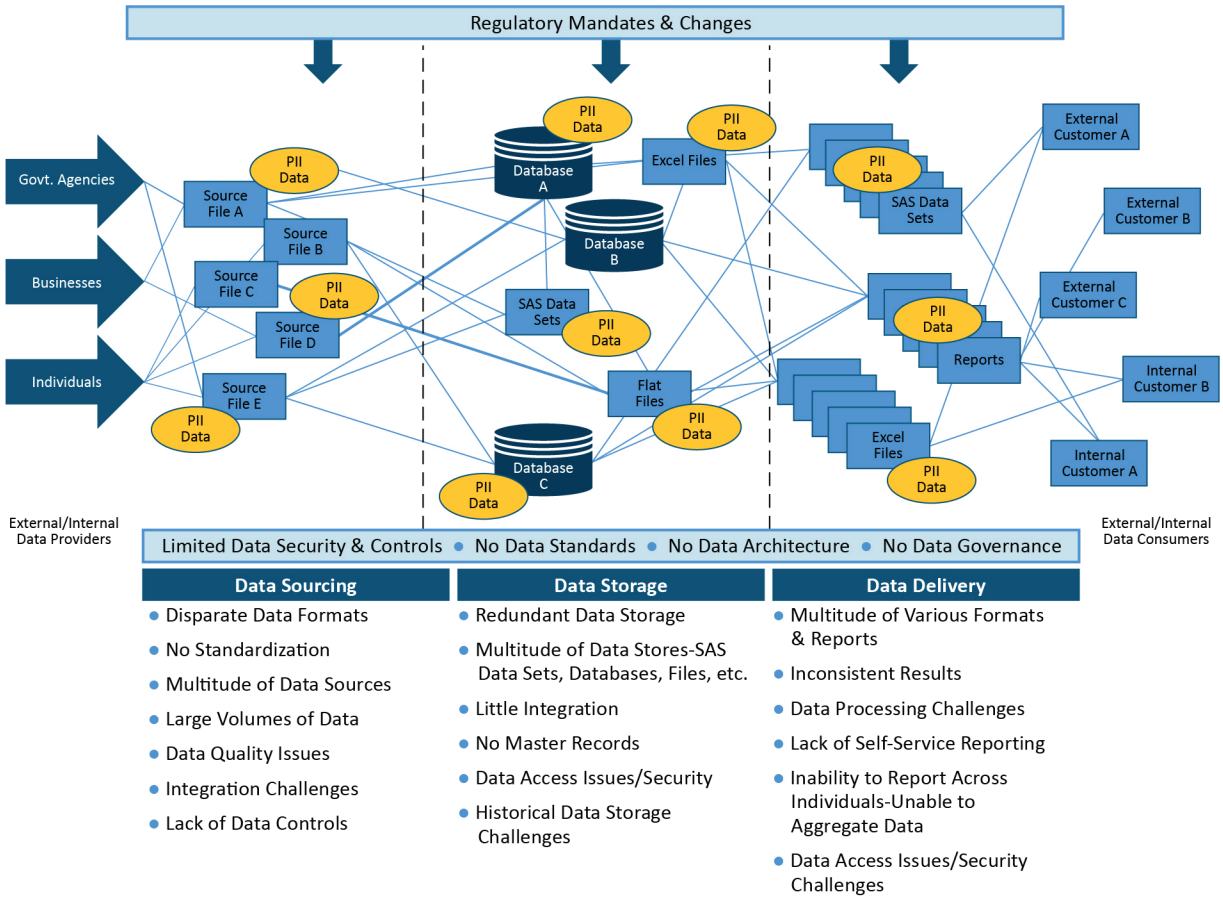
The evaluation of the organization goes deeper into the data strategy. We will want to understand the business drivers for your data strategy. Are you in an offensive or defensive position today and where do you want to be?

Data Modernization Approach



Once the data strategy is identified, the data governance steps follow.

Data Challenges-Typical



Data Governance is the process and people charged with directing, guiding, and regulating the usage of an organization's data assets in order to optimize its value and control associated risks.

Ultimately, all your organization's data should be governed, but it is not realistic to tackle all of it at once. Combining & applying the dimensions of criticality, commonality, and quality to your organization's data assets to establish a prioritized list of data categories is a key initial step on the path to data governance.

Some data are more critical than others. Their degree of importance is driven by usage – i.e. the criticality of the processes, reports, or decisions relying upon those data. Each organization will have a different view on their most critical processes and decisions and, therefore, pieces of information. To make things more complex, this view will change over time.

A good data governance function addresses each of the following areas:

- **Data Acquisition & Integration** – What data sources ***should*** be used (external and internal) and what sources ***are*** being used? For homogeneous data coming from multiple sources, what is the proper priority of sources and how are entities uniquely identified? For heterogeneous data, how should the data relate to each other and new data derive from the intersection?
- **Data Usage** – Which processes, systems, and reports use the data and why? How do the data flow along the process and system information supply chain and do the parties involved understand and agree to their direct dependencies and dependents?
- **Data Quality** – How complete, accurate, and valid are the data in relation to their stated usage purposes? What risks is the organization exposed to due to defects with the data (non-conformance to stated business rules)?
- **Data Persistence** – Where and how should data be stored; how long should data be kept readily available, archived, and purged; how many redundant copies of the same data should be kept and how many actually exist?
- **Data Definition** – What are the conceptual, logical, and physical names and descriptions of the data; how do they relate to other data attributes and objects (entities); what type of data are they and what domain of values are allowed?
- **Data Security** – Who authorizes access to the data and what mechanism(s) are used; how are the data classified from a sensitivity and privacy perspective; how are the data protected from loss, theft, and unauthorized intrusions?

Unissant understands that Implementing a data governance program and sustaining its value over the long term is a tough proposition for many organizations. This is primarily due to the need for organizational change management, which arises because data governance often forces the organization to operate much differently from status quo.

Unissant's approach to Data Protection consists of 5 phases:

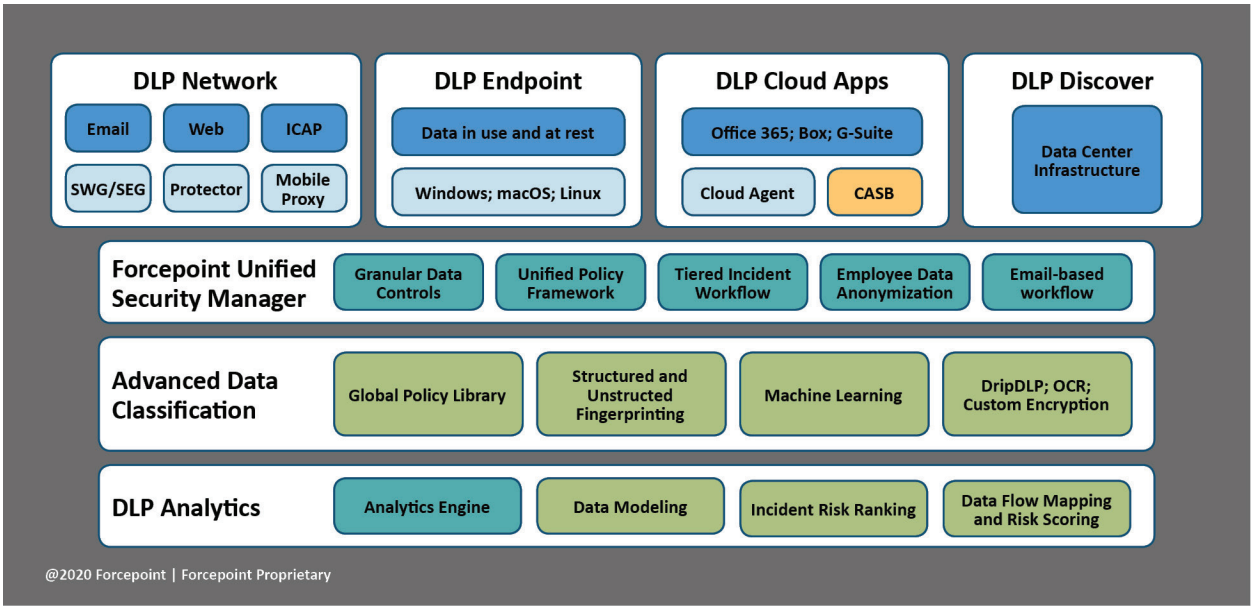
- **Phase 1: Discover**
- **Phase 2: Identify/Clean**
- **Phase 3: Classify**
- **Phase 4: Secure**
- **Phase 5: Monitor**

To give our customers a 360 protection that includes data policy, governance technological protections, Unissant has partnered with Forcepoint. Forcepoint DLP is an industry leader in data loss prevention (DLP) as it protects intellectual property and regulated data against malicious attackers, insider threats, and accidental loss wherever data resides in the cloud, on the network, or on endpoint devices. With Forcepoint DLP, an organization can easily demonstrate compliance and avoid costly fines and headlines. Specifically, Forcepoint DLP supports:

Our employment of **Forcepoint Dynamic Data Protection (DDP) Suit**e in our offerings includes capabilities spanning:

- Data discovery
- Data classification (using Bolden James OEM)
- DLP on endpoint, network and cloud (DLP Cloud Apps)
- CASB
- Automated Policy Enforcement (using Forcepoint Behavior Analytics for Risk Adaptive response)

Forcepoint Data Protection Components



**** Below we have shown where Forcepoint solutions are employed in each phase of our framework.**

Discover ID/Clean Classify Secure Monitor

Unissant's approach to Data Security starts with the discovery phase. In this phase Unissant focuses on three pillars: People, Processes and Technologies. Each one of these pillars will help us understand your organization's data and how they are produced and consumed as we progress through the framework.

We will use Data Loss Prevention (DLP) /Cloud Access Security Broker (CASB) Discovery to find data across the organization's network. This includes data in the traditional data center, data stored in cloud and cloud services like Office 365 and Box Enterprise. There may be terabytes of data discovered and, with our technology partner, we will begin to protect it on day one. The result of this phase will be a **complete inventory of all data sources across the organization and everything will be secured**. An organization could stop right here but they still won't understand how the organization's data are produced and consumed and what are the critical data elements of each data source.

In this phase, we employ Forcepoint's solutions to:

- Advanced detection and controls that follows the data
- Our unique PreciseID Fingerprinting can detect a partial fingerprint of structured (database records) or unstructured data (documents) on Mac and Windows endpoints – whether an employee is working online or offline
- Optical Character Recognition (OCR) identifies data embedded in images while at rest or in motion; identifies sensitive data and IP markers within images such as CAD designs, scanned documents, MRI's and screen shots
- Robust identification for Personally Identifiable Information (PII) offers data validation checks, real name detection, proximity analysis, and context identifiers
- Custom encryption identification exposes data hidden from discovery and applicable controls
- Cumulative analysis for drip DLP detection (i.e., data that leaks out slowly over time)
- Analyzes encrypted files and applies appropriate DLP controls to the data

Next, we look at the Functions, Drivers & Success, Setup, Data Quality. We assist the organization to identify sensitive data, regulated data and intellectual property at rest. In this phase, we look at reducing redundant data sources and really position the organization to create authoritative data sources for their consumers. Once we have the organization at this point, we work with stakeholders to understand the **Critical Data Element (CDEs)**. Identification of the CDE's will help us understand the level security a particular data element needs and the approach we will use ensure the security of that element. **The result of this phase is a comprehensive understanding of data and all relevant information regarding data sources. An understanding of producers and consumers.**

In this phase, we employ Forcepoint's solutions to:

- Precise ID Fingerprinting – Partial and Full Fingerprinting of structured and unstructured data (database tables, files, and folders).
- Machine Learning – Unstructured data, registered and learned to identify data of a similar nature
- Scripts – Over 300 predefined classifiers (Python scripts, multiple languages) in order to identify sensitive data such as PII, PHI, PCI and more
- Regular Expressions & Files Types – Perl based regular expressions and detection of close to 600 true file types
- Keyword/Phrases/Dictionaries – Over 1,000 pre-defined classifiers supporting various regulations and international compliance (support in multiple languages)

In this phase, classification is the result. To understand the data, the data strategy and what the needed classifications will, be the organization will need to understand the CDEs and what data sources have multiple CDEs. Once we have a thorough understanding of the CDEs, we prioritize them and set classifications. **The result of this phase is a clear understanding of CDE Prioritization, and all data classified.**

In this phase, we employ Forcepoint's solutions to:

- File Classification Labels – File metadata label identification, as well as built in integration with Boldon James and AIP/MIP labeling schemas

NOTE: The phases above can be used for preparation for data automation, business intelligence, artificial intelligence programs also. The value derived by doing the above is endless.

Cyber security protections become the focus in this phase. The organization now has a level of understanding of their data (producer and consumers) that will allow them to employ a myriad of business strategies while at the same time making protection decisions. We assist our customers in building a comprehensive data security strategy that consists of risk assessments, remediation of security gaps, passive and active vulnerability analysis, risk mitigation, employment of technology protections, protecting data by applying appropriate encryption and controls across environments, ensuring data integrity of Critical Data and the implementation of DLP Protections Technologies. **The result of this phase will be a comprehensive review and security plan. Implementation of controls and technologies to protect data. Reduce data protections to what really needs to be protected.**

In this phase, we employ Forcepoint's solutions to:

- Automatically encrypt data being transferred onto removable storage devices to enable secure data sharing with partners
- Leverages User & Entity Behavior Analytics for unique, risk-based outcomes
- Protects user accounts from account takeover
- Identify and automatically prevent sharing of sensitive data to external users or unauthorized internal users
- Protect data in real-time for uploads into and downloads from critical cloud applications including Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack, and many more
- Identify and automatically prevent sharing of sensitive data to external users or unauthorized internal users
- Protect data in real-time from uploads into and downloads from critical cloud applications including Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack, and many more
- Deploy a Forcepoint-hosted solution that extends DLP policy features including fingerprinting and machine learning to cloud applications. while having the option of maintaining incidents and forensics data within the data center
- Unify policy enforcement via single console to define and apply data in motion and data discovery policies across all channels—cloud, network, and endpoints

Finally, as an organization, there is a greater understanding of the data and a comprehensive data *security* strategy has been wrapped around the overall data strategy. Now, the key is to monitor the implementation of that strategy to ensure it is working as designed and can adapt to the changing landscape of the organization. Some of the monitoring that we suggest are:

- Access Control Auditing
- Privileged User Monitoring
- Real time and threshold alerting
- Integrate alerts in the SIEM
- Compliance
- Constant review of alerting and reporting requirements
- Advanced Analytics

The result of this phase is a focus on process improvement, alerting and reporting. As organization matures, a move towards advanced analytics.

In this phase, we employ Forcepoint's solutions to:

- Visibility no matter where the data resides and focus response teams to identify and protect data across cloud applications, network data stores, databases, and managed endpoints
- Enable data owners and business managers with email-based distributed incident workflow to review and respond to DLP incidents making it easy to distribute an incident for review and remediation to data owners and business stakeholders without having to provide access to the DLP management system
- Provides full operational context to more effectively adjudicate DLP alerts
- Automatically escalates more stringent policy deployment and enforcement for users based on data exfiltration risk indicators
- Maximize workforce productivity
- Visualize and triage risks for response teams with prioritized incidents that highlight the people responsible for risk, the critical data at risk, and common patterns of behavior across users
- Increase employee awareness for handling sensitive data and IP with employee coaching on Windows and macOS, in addition to enabling employees with integration of classification solutions like Boldon James and Microsoft Azure Information Protection
- Enforce advanced DLP data identification capabilities, such as fingerprinting, on remote work endpoints and in enterprise cloud applications
- Safeguard user privacy with anonymization options and access controls
- Add the context of data into broader user analytics through deep integrations with Forcepoint User Protection (Insider Threat) and Forcepoint Edge Protection (NGFW, SD-WAN, etc.) using Forcepoint Behavioral Analytics

As discussed, Unissant can do these all at once or can work with data leaders to design an approach that works for the resources that are available today based on our crawl, walk, run and fly methodology.

If you would like more information on this framework of other data and cyber security services provided by Unissant, please contact us at information@unissant.com or 703.889.8500

About Unissant

Unissant is an advanced data analytics and business transformation services provider with expertise in healthcare and health IT, finance, national security, and energy. The company delivers innovative solutions to assist government agencies and private sector businesses in tackling their biggest challenges. Founded in 2006, Unissant is a prime contractor on various government vehicles such as CIO-SP3, GSA PSS, GSA HealthIT SIN, and GSA 8(a) STARS II and is a CMMI Level 3, ISO 9001 & 27001 certified company headquartered in Herndon, Virginia with a satellite office in San Antonio, Texas. In March 2017, Unissant received the Government Project of the Year award by Small and Emerging Contractors Advisory Forum (SECAF). Unissant has experience with implementing machine learning solutions and full stack implementation on cloud. Unissant is a Select Consulting Partner Public Sector and is leveraging this relationship with AWS to strengthen our ability to support our customers in their Digital Transformation journey. We are already supporting several of our customers in the public sector with their Machine Learning implementations, cloud adoption strategy and implementation.

Copyright

Restricted Rights Legend

For additional information on Unissant full range of services, please visit our website at www.unissant.com or call us at 703.889.8500.