DATA SECURITY INTELLIGENCE FUTURE STATE

White Paper

EXECUTIVE SUMMARY

In this White Paper, Neuralytix analyzes the Data Security Intelligence (DSI) market. Our research indicates that this market will reach US$800M by 2018, growing at a CAGR of 27.8%. North America and EMEA will be responsible for over 95% of the DSI spend.

The framework behind DSI enables enterprises to understand the risk and profile of the data they retain. This framework not only helps to minimize risk, but can also maximize enterprise value and competitive advantage.

The Internet is inherently insecure. Even the most “secure” network and host solutions will eventually be breached. Moreover, insiders present special challenges, as they may be unwitting aids to breaches through social engineering or human error.

Enterprises must turn towards a data-centric approach to data security.

Ultimately, data security is not just the responsibility of IT, but requires an organization-wide understanding of the value, opportunity, and risk of the vast array of data sources available to an enterprise.

The DSI technology portfolio and a resetting of business processes will ensure success, growth, and security for the enterprise.

Ben Woo & Matt Healey
4/2/2015
Document #: 194328

Neuralytix

TABLE OF CONTENTS

INTRODUCTION

What do Apple, Dairy Queen, UPS, and Yahoo! have in common? These multi-national companies have all been on the receiving end of public and embarrassing cyber-attacks in 2014.

Figure 1 is an infographic that visually depicts the largest reported data breaches around the world, and the number of records stolen since 2011.

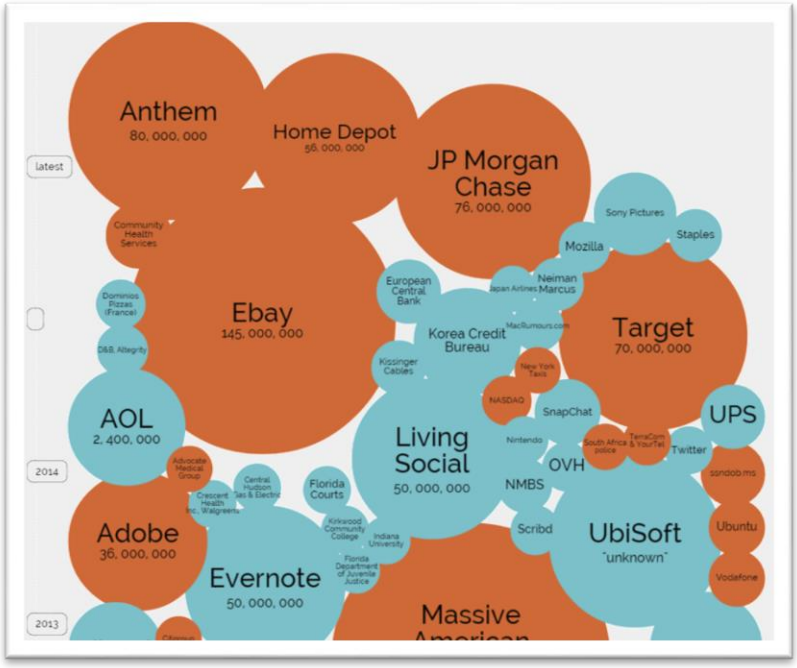


Figure 1: World's Biggest Data Breaches (Information is Beautiful 2015)

Security Technology Segment Evolution

Over the last quarter century, as shown in Figure 2, the evolution of successfully adopted security technology segments has witnessed remarkably common go-to-market and adoption patterns. Each major player in key segments such as intrusion detection (IDS), data loss prevention (DLP), and Advanced Persistent Threat (APT) to Cloud Security began with a technology that offered visualization of the problem. Each segment evolved to real-time detection, and then to protection. This shows that a major requirement for adopting new security approaches is being able to communicate the threat to a non-technical, non-security-savvy audience (i.e. C-Suite executives and Boards of Directors).

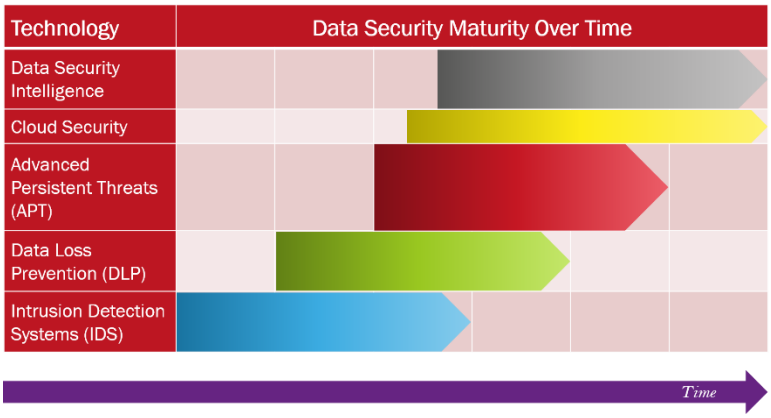


Figure 2: Data Security Maturity Over Time (Neuralytix, 2015)

As we look into the future trends of information technology, vendors investing in this market should take heed of these common success criteria.

Data Proliferation Is on the Rise

The traditional approach to security had been to protect the network and endpoints such as laptops and mobile devices. However, these approaches by themselves are neither sufficient nor effective, as data proliferates exponentially across the enterprise and beyond the perimeter of an enterprise firewall or national border. Data exposure is a function of its proliferation from the original point of creation. Measuring risk is no longer just a function of keeping malicious people out. It is also about making sure that employees do not inadvertently (or intentionally) expose sensitive or regulated data. An increasing number of regulations govern the privacy and sensitivity of data.

As mentioned above, security risks are not only coming from outside the enterprise, but from inside as well. In many cases, the breaches will not be detected until months after the attack has taken place. This, in part, is due to the proliferation of data and the lack of visibility and controls that follow the data wherever it is copied. Nevertheless, this extends beyond proliferation of data. Data sources both internal and external to an enterprise are insecure. Data that may have originated external to an organization (e.g. email, social media, etc.) may infiltrate inside an organization through techniques such as phishing and malware. These threats expose enterprises to new and fast-evolving data security risks.

The need to integrate disparate datasets from internal and external sources (and by extension, varying levels of data security) is also

increasing the risk of exposure, as most enterprises outsource common transaction-based business processes to cloud and third-party vendors.

Apart from the damaging optics to an enterprise, consumers are losing trust in otherwise *bona fide* enterprises, as those with traditional security controls are breaking their promises of keeping consumer, patient and employee data safe.

DATA-CENTRIC SECURITY - THE NEXT BIG THING

The rise of Advanced Persistent Threats, and the availability of alternatives to traditional internal IT operations, by way of "shadow" IT services, including (but not limited to) email, file sharing, and Software-as-a-Service applications that mirror or improve on internal IT services, gave way to a realization that IDS, DLP, APT and Cloud Security alone are insufficient to protect data. The emphasis on data security has become significant and is not just about keeping people out, but equally about keeping data *visible* to those who are authorized to see it.

By deploying data security intelligence in combination with data security controls, enterprises can gain active insight into where risks exist and proactively set controls to mitigate the impact in the event of a data breach.

Data-Centric Security is an approach to security that focuses on the data itself: to cover the gaps of traditional network, host and application security solutions.

Data management vendors like Informatica believe that enterprises are deploying data-centric security controls because they need additional safeguards as threats escalate and data proliferates. As noted earlier, internal and external parts of the enterprise can be a source of data security risk, and having intelligence with respect to all data is critical. In fact, Advanced Persistent Threats (APT) are likely to cause data security risks even more than data proliferation.

Enterprise security leaders understand that visualization, in addition to real-time detection (and ultimately protection) of potential data threats, is just as important when attempting to justify spending security budgets on additional security controls.

By deploying data security intelligence in combination with data security controls, enterprises can gain active insight into where risks exist and proactively set controls to mitigate the impact in the event of a data breach.

It's All About Securing the Data

In today's data-prolific world, another facet must pivot to the front lines: data security. It is no longer just about protecting domains and applications. Data security is about protecting individual data objects that traverse across networks, in and out of a public or private cloud, and from source applications to targets such as partner systems, back office SaaS applications or data warehouses and analytics platforms.

Data needs to not only be governed by corporate policies, but also by (often competing) legislative and regulatory compliance – especially when these target systems mean that data crosses national borders.

This is not an easy task. Data security demands the cooperation of all executive and senior management to address this issue.

The Approach

The approach needed to begin to address the data security imperative is a multi-step process (see Figure 3 below).

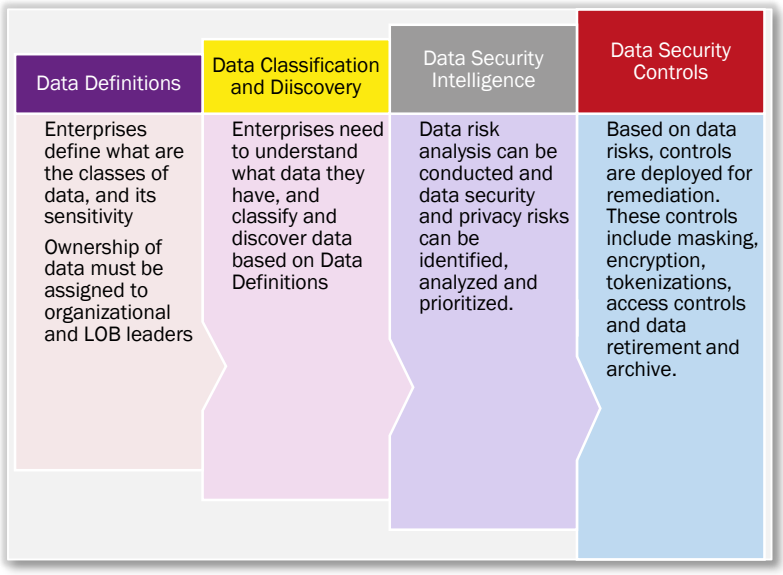


Figure 3: The Approach to Modern Data Centric Security (Neuralytix 2015)

Enterprises must first start with defining and segmenting the types of data they own. That way, data "stewards" or owners can be assigned and made responsible to create the necessary policies to govern that data. Data steward residency is often in the line of business, not in IT – this varies by industry and region.

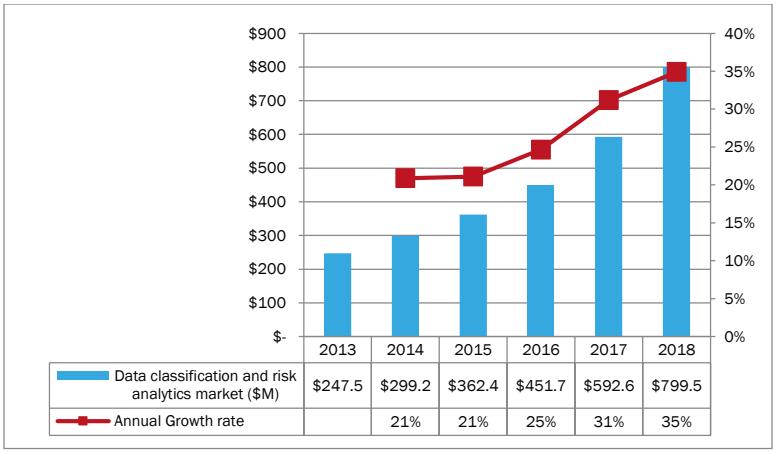
With this ownership and understanding, enterprises must engage in data discovery so that all data within the business unit (or ideally, the enterprise) can be classified based on policy.

Only when this is completed can true intelligence and insight be assessed to compute and analyze risk and exposure of data. This way, a security risk assessment can be undertaken, and ultimately, data security controls can be prioritized based on the highest risk and implemented accordingly.

The Data Security Intelligence Market

Neuralytix research shows that the overall data security intelligence (DSI) market, which was valued at roughly $247M in 2013, will reach almost US$800M by 2018, growing at a CAGR of 27.8% between 2014 and 2018 (see Figure 4). DSI is comprised of technology that provides the definition, classification, discovery, and assessment phases of a data-centric security approach. This model does not include the Data Security controls market, such as data masking or encryption.

Not surprisingly, North America (the United States in particular), and Europe will continue to be the largest consumers of data security software. By 2018, these two regions will make up 96% of the data security market (see Figure 4).



	2013	2014	2015	2016	2017	2018
Data classification and risk analytics market ($M)	$247.5	$299.2	$362.4	$451.7	$592.6	$799.5
Annual Growth rate		21%	21%	25%	31%	35%

Figure 4: The Data Security Intelligence Market (Neuralytix 2015)

The increasing growth of the market is comparable to other security segments based on adoption and maturity of vendor offerings.

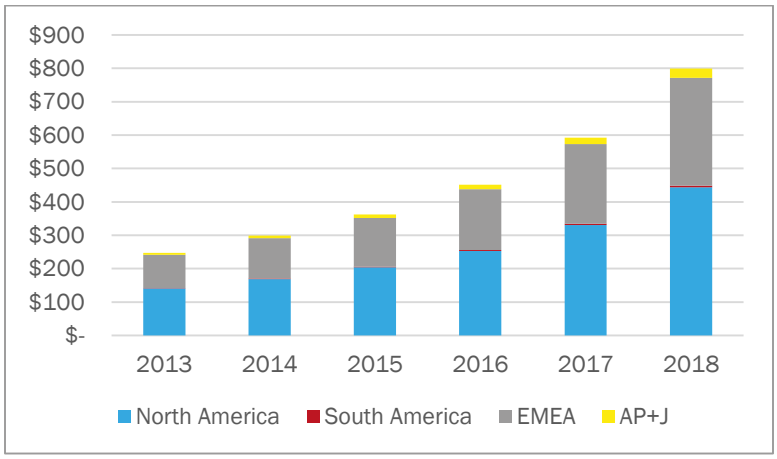


Figure 5: Data Security Intelligence Market by Region (Neuralytix 2015)

It is expected that regulations will drive adoption of data security intelligence offerings. The adoption of legislation with effective enforcing tenets (i.e. fines, imprisonment) is strongest in North America and EMEA with South America offering the greatest room for improvement.

CONCLUSION

What Can Users Do today?

Neuralytix research suggests enterprise users must immediately start or sustain the data-centric security approach journey laid out in Figure 3 above. Data-centric security goes beyond basic governance. The impact on an enterprise goes beyond the exposure of its data. The public embarrassment that goes along with an enterprise's inability to secure and keep private its customer or any other sensitive data has a lasting effect on customer confidence towards the enterprise.

As the adage goes, "*it is cheaper to retain a customer than to find a new one*!" With so much competition in every industry, and the globalization of commerce, customers have more opportunities to switch providers than ever before. Those organizations that adopt a data-centric security approach sooner than their competitors will win over the trust of their customers, stakeholders, and employees.

Opportunities for System Integrators

For system integrators, the last 10 years have primarily focused on infrastructure and physical controls based on a defined network perimeter. Between consolidation, virtualization, and other optimizations, these cost-mitigating actions have almost run their course.

The opportunity is bountiful for system integrators to move beyond the highly competitive infrastructure integration business, and move to the higher-value data security intelligence business. This is more apparent in an industry with a significant shortage of data security skillsets.

All system integrator customers have seen the disastrous public humiliation of some of the world's most trusted and largest companies due to failures to control data security.

By helping enterprises understand the impact, and providing them with solutions to gain intelligence into the effectiveness of their data security policies, there is a vast opportunity for consulting, integration and maintenance of these environments.

Data Security Intelligence

Data security intelligence is a framework for understanding the risk of sensitive or confidential data and recommending the optimal set of controls to mitigate that risk. DSI is comprised of technology that provides the definition, classification, discovery, and assessment phases of a data-centric security approach.

Typical users of DSI are security architects, CISOs, CPOs, security architects and data stewards. Consumers of intelligence reports span to lines of businesses, the C-Suite and BOD members. DSI should not replace existing security frameworks and should be used with complimentary security technologies and platforms.

DSI technologies speed the discovery and identification of risk, assist in decision-making processes such that security controls are procured and implemented based on evidence of high risk.

DSI Generates Business Value

While this Paper has focused on the definitions, classification, intelligence and controls of a data-centric enterprise, Neuralytix hastens to note that apart from security, the processes described herein go beyond risk mitigation.

The definition and classification of data has very strong economic benefits for enterprises. Once classified, data has new value that can be exploited by the enterprise to generate growth and competitive advantage.

APPENDIX

Terms and Definitions

Market Definition

The Data classification and risk analysis market is composed of the following sub-markets.

- **Data Discovery** – The data discovery market consists of software that scans the enterprise environment and identifies the data stored in that environment. This capability is often the first step in the broader discovery and classification of data.
- **Sensitive Data Classification** – The data classification market is comprised of software that identifies and classifies the sensitivity of data. The data can be structured or unstructured data.
- **Data Security Risk Analytics** – The risk analytics market is comprised of software that evaluates and displays the extent to which data is accessible, in use, exposed, and proliferated. Products may provide anomaly detection, uncover suspicious data usage patterns, and utilize behavioral analytics. The software indicates varying degrees of risk to enable users to identify and prioritize areas of high risk and take appropriate action.

Consumption models

This market includes the following end user consumption models

- **Traditional On-Premises software** – This represents the traditional approach to software deployment on premises. In this model, the end user either purchases or subscribes the software license from the provider and deploys the software in their environment. This category includes both the initial software license (perpetual or subscription) and the ongoing maintenance.
- **Public Cloud** – In this consumption model, the customer pays a fee for the use of the software. In this model, the end user does not own the license for the software. Furthermore, the public cloud is a multi-tenant environment. The environment resides in the provider's data center.
- **Private Cloud** – In this consumption model, the customer pays a fee for the use of the software. In this model, the end user does not own the license for the software. This model differs from the public cloud in that, rather than a

multi-tenant environment, a private cloud represents a single-tenant environment. The environment may reside in either the customer or the provider's data center.

Exclusions

This market excludes the following:

- **Professional Services** – The professional services are not included. These include IT consulting and systems integration. IT consulting is comprised of services that assist the user in identifying and selecting software. Systems integration services are comprised of the services associated with deploying the software in the customer's environment.
- **Support Services** – On-going support services are not included. Support is comprised of services that fix problems associated with the software. They are delivered through on-site support, phone support, and remote support. For services to be considered support and not software maintenance, the customer needs to have either purchased a higher level of support, e.g. gold support, or purchased the services from a third party. Basic support services that are included with the software maintenance agreement are not considered support services and as such are included in the software forecast.

CONTACT US

To learn more about Neuralytix and our other solutions, contact your local representative – or visit Neuralytix.com.