Secureworks®

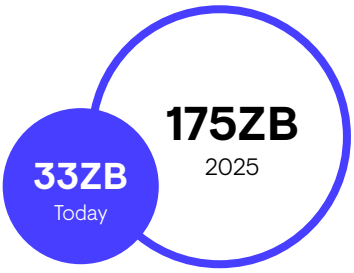
GUIDE

A Guide to Effectively Managing Big Data from Security Systems

What is Big Data?

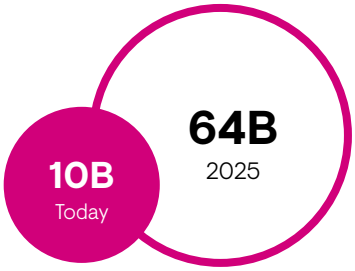
Businesses today are driven by big data. The data underpins digital banking initiatives from customer portfolio management and investments to loan management, and beyond. When an industry captures and stores healthcare and medical records, DNA, inventory, and manufacturing process telemetry, they are participating in this new digital paradigm. But big data is increasingly being housed in multiple, disparate systems across today's organization, which brings new challenges to security teams charged with protecting this most valuable asset.

This paradigm creates new opportunities for businesses to engage with customers, provide more customized and tailored services, and fuels growth into horizontal and vertical market segments. The data proliferates at an increasing rate and becomes the most critical element of business operations.IT systems are also evolving to capture, store, and analyze all of this data across multiple technologies, geographic regions, and various tools. This evolution of IT systems brings about a new emerging threat to security programs, where business critical assets are managed across cloud providers and on-premise systems. When businesses embrace big data platforms to inform decision making, security programs need to leverage big data in order to adequately protect them. As with all evolutions of security needs, the emergence of big data sets, or "lakes," comes with some inherent risks and new challenges. Today's organizations need to prioritize developing effective strategies to manage big data and protect it in tandem with agile security programs.



Global Datasphere[1]

Hyperscale Data Centers[2]



IoT Devices[3]

How Do You Protect Big Data Itself?

The first item to address when discussing big data strategies is the protection of big data itself. It's essential that an organization utilizing large data sets is capable of maintaining their privacy. Some high-level recommendations for protecting big data itself are[4]:

1. **Ensure confidentiality:** The decoupling of any personal identifiable information from the data will help to segregate the privacy concerns of the data from its applicability as part of a big data strategy.
2. **Keep a check on your physical and logical infrastructure:** Whether your data is stored in the cloud or on-premise, you must ensure sufficient protection mechanisms, including controls such as patch management and regular technical tests for vulnerabilities, are in place.
3. **Ensure adequate access control policies are in place:** Sound policies should allow access to authorized users only, protecting data from unauthorized access by both external and internal agents.

Secureworks®

4. **Encrypt your data in transit and at rest:** Encryption is a critical component of any security strategy. This includes adequate protection be given to data that is at rest and in transit, ensuring confidentiality and integrity of the data itself.
5. **Enable real-time security monitoring:** The ingress and egress points of data storage requires 24x7 threat intelligence enriched monitoring for unauthorized access to the data.

Opportunities with Cybersecurity

In the Big Data era, all data is relevant to enterprise security, and cybersecurity technology solutions can capture unstructured data from across an organization and carry out complex queries and receive results in a timely fashion. This data, which stems from modern security priorities such as web traffic, app usage and email, is hard to analyze and make sense of using existing technologies alone given unstructured data was difficult to capture in the first place. One of the advantages of Big Data and NoSQL databases is that they can store such data in a format that is scalable and simultaneously indexed for rapid query and analysis.

A robust security program that is successfully leveraging big data will benefit by gaining

- Machine learning threat detection capability
- Business context-aware risk scoring
- Recommended remediation controls
- Greater visibility into the environment

With the advent of big data, the biggest opportunities for security programs to leverage is supervised or unsupervised machine learning algorithms. Machine learning algorithms stand the greatest chance to proactively identify potential threats to the organization's data prior to a compromised asset. Machine learning pattern detectors should be able to support security professionals with the identification of potential adversaries doing reconnaissance in the environment prior to an actual exploit faster and with greater accuracy. This can only be accomplished with a big data security platform that leverages a vast set of normalized data from disparate sources to establish the baseline of day-to-day activity and flag anomalous activity to the security professionals.

Prior to the inception of the big data platforms for normalized behavior monitoring, this type of threat identification was extremely labor intensive and error-prone. Big data security platforms play a much more strategic role in identifying threats prior to exploitation, giving security professionals a tactical advantage. Big data security programs allow for more sophisticated pattern detection and advance the ability to detect suspicious activity far faster. Traditionally, security programs have not been able to unite disparate systems into a large data lake, often missing indicators of a threat actor's reconnaissance due to the inability to detect non-authorized, abnormal transactions.

Another opportunity to leverage Big Data from a security perspective is to analyze historic data and root causes of security incidents by going 'back in time'. By collecting data on a large scale and analyzing historical trends, it is possible to identify when an attack started, and the steps that the attacker took to establish a foothold in your systems. Even if they did not detect the original attack, security teams can carry out a historical correlation in the analytics platform to identify the attack. Big data security programs offer a holistic point of view to improve the overall efficacy of the program. Based on larger aggregate data sets, security practitioners can more effectively identify hot spots of threat activity and prioritize proactive measures to shore up security controls. Identifying how the threat actor is attempting to penetrate the systems over time allows security teams to most effectively prioritize investments in areas of the highest rate of threat activity. Coupling this data with a more robust understanding of the operational impact on the business for systems empowers security teams to tailor responses, investments, and priorities to most effectively mitigate the threats while conserving dollars for the business.

In cases of known threat activity or identified patterns, big data behavioral analysis empowers security professionals to be more surgical in their response capabilities and allows for increased levels of automation that can mitigate attacks before they proliferate in the environment. Imagine the ability to orchestrate responses from known threat activity by industry and threat tactic to further enhance the security efficacy of the program without having to hire additional highly sought-after professionals to do it. But such an outcome is only possible if your organization is feeding the program with rich data. If you limit your data inputs, then the expectation for contextualized outcomes that lead to actionable intelligence will not be achieved.

Wider Risks & Challenges of Big Data

With great data power comes great responsibility. With the inception of the big data security platforms, organizations need to manage and mitigate the challenges to maximize their investment. Common struggles for an organization can generally be grouped into three major challenges:

Knowledge Gap Challenges

Knowledge gaps exist in many facets of big data, particularly across a big data strategy's key dependence of business-critical assets, the security data being collected and the devices collecting the data itself. This lack of intimate awareness of business-critical assets is born out of the digital revolution, as organizations move away from the traditional on-premise models of storing critical data towards software as a service (SaaS) models where things like CRM data, HR Data, or financial data is being stored on external platforms. These external platforms are often referred to as 'shadow IT,' creating further issues when it comes to understanding the value of the security data being captured. Security data systems are an ongoing evolutionary process that requires upfront strategic planning and insight for normalizing the data. Oftentimes, security

professionals don't know what insights or queries they need from the data, leading to challenges designing the appropriate data stores, which is worsened by the lack of knowledge about business-critical assets. This is further compounded by a knowledge gap as to the trustworthiness of the devices, platforms and systems collecting the data, where security professionals are questioning the efficacy of the technology collecting various data points and thus not knowing the potential value of that data itself.

Physical and Logical Constraints of Systems and the Data

Big data strategies are dependent on technology and software to operate. As such they are subject to the same limitations of said technology and software as standalone solutions. These challenges are exponentially accelerated when they need to work together to produce an outcome. The already existing challenges around application software security, access control and authentication and the secure use of cloud computing are magnified when applied to interoperability of applications. The movement away from defense-in-concert towards Big Data strategies is hindered by the siloed nature of data caused by defense-in-concert techniques. Often organizations looking to secure their assets store data without the strategic mindset to convert the data into information. This leads to a costly investment in determining if the data produced by physical and logical technologies can be leveraged by a Big Data strategy.

Demurs from Business, Regulatory, and Compliance Requirements

The public perceptions around data are changing; consumers care about their personal data now more than ever. On top of this the changing global regulation landscape is putting increased pressure on business to take adequate care of data. More and more regulations, such as GDPR, are mandating that customer data is secured across its lifecycle up to a high standard expected by the regulator. It's now incumbent on security professionals to clearly understand where potential data compromise may exist and evolve the Big Data security strategy to ensure visibility and telemetry for each area of the organization's critical business assets and articulate this to the business leadership, auditors and regulators. This often becomes a larger risk to the operational excellence of the organization as security teams lack awareness of several critical business assets or lack the ability with limited resources to provide coverage across all the multiple spans of control within the new data-driven business.

Organizations that overcome these challenges will be well-positioned to earn not only regulatory compliance but the confidence of staff and end users. The following recommendations will help to address these challenges.

Recommendations to Manage Challenges and Reduce Risk

To effectively strategize the organization's big data-enriched security program, security teams need to focus on the end in mind and scale out:

1. Critical prioritization of business-critical assets, their location, and the types of threats acted against them. Appropriate prioritization will yield the greatest input for designing the data lake, telemetry requirements, and normalization processes needed for an effective big data strategy.
2. Conducting a thorough risk assessment of all dependent components of your big data ecosystem: Everything from your cloud service provider, to applications, business processes, data controls and access points.
3. Prioritize gaps and weaknesses in your big data security program highlighted by your risk assessment.
4. Implement controls to address the gaps, for example:
    a. Access controls to ensure Big Data queries are executed only by authorized users and entities.
    b. Application security controls which include regular security testing procedures for new and updated components of the system.
    c. Encryption of data at rest and in transit.
    d. Compliance to security standards and data regulations.
    e. Monitoring and logging – enabling monitoring and logging on Big Data nodes, databases, applications to detect malicious behaviors such as modification of logs or exfiltration of sensitive information.
5. Continue to review and improve the overall system, process and ecosystem with regular testing and continuous improvement initiatives.

Conclusion

Big data strategies in a security program are vastly beneficial at improving an organization's security posture and reducing risk to the business, but they can be challenging to implement. Not asking the right questions up front can create compounding issues as your program is adopted. Questions like; what are my critical risks? Where is all our data housed? Do we have awareness of our physical and logical infrastructure? How do we normalize the data? Are we asking the right questions of our data? Do we have the right resources to develop our capability?

In order to leverage a view of risk vs. cost of big data in a security program CIOs should start with the end in mind - prioritize known crown jewel assets first for laser focus and scale out to the less sensitive data from there. Have a firm understanding of the physical and logical infrastructure. Ensure data is pointing to a learning model rather than just data storage and focus on efficacy based on the impact of a potential breach or compromise to the business. Following this guide will help you to determine the need for a big data strategy based on risk vs. reward, effectively manage a big data strategy, or at least ask the right questions of a third party who can provide one to your organization.

Risks and Challenges to Securing the Business with Big Data	Opportunity for the CIO to Balance the Risk v. Reward of Big Data in Security Programs
1 Not knowing where to begin with a big data program with the data structures being less forgiving because you don't have the right questions in mind.	Start with the end in mind – Prioritize known crown jewels assets first for laser focus.
	Understand both physical and logical infrastructures.
2 Not having awareness of the critical risks that would guide the data structures for normalization and querying of the data.	Mature data science elements with a learning model as opposed to basic data storage.
3 Missing the awareness of the physical and logical infrastructure that gaps go undetected in the security program.	Focus on Efficacy based on paradigm of impact to business if breached or compromised operationally.

Want to learn more?
Click on the assets below to continue learning

Sources:

[1] https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

[2] https://www.datacenterdynamics.com/news/synergy-number-of-hyperscale-data-centers-reaches-390/

[3] https://www.businessinsider.com/internet-of-things-report

[4] https://www.newgenapps.com/blog/big-data-security-challenges-solutions-problems-security

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp