Hexnode for data security

Protecting your business data with Hexnode

WHITE PAPER

hexnode

TABLE OF CONTENTS

Introduction

In today's digital age, data is one of the most valuable assets for any organization. However, with the increasing use of technology and the rise of cybercrime, data security has become a critical concern. Ensuring the security of sensitive information has become more important than ever, as data breaches can have devastating consequences for businesses and their customers.

Eons ago, the first men started socializing, and soon enough, they realized the importance of transactions. What started as a barter system has now evolved into a fully functional currency system. The world has come a long way from trading meat for pulses to paying a few bucks for groceries. Equally remarkable is the transition from inventing the wheel to inventing life-like robots with unmatched thinking capacity, an age where data runs the world. In this age and day, organizations take to data the way cars take to fuel. Data, indeed, prints bills and mints coins. Entities pay millions to get their hands on data and spend billions on protecting their data.

While most resources keep depleting, data is one that keeps on increasing by the day. Anything and everything we do in the digital space is data and worth a lot of money. The concept of data security in the digital world took root because of its growing importance and people's awareness.

1

Dusting the past

Over the years, corporations have developed and refined their data security measures to protect sensitive information from the increasing threat of cyber attacks. From basic encryption to advanced threat detection, businesses have adapted their security measures to safeguard valuable data and ensure its confidentiality and integrity.

The act of protecting and safeguarding one's belongings is an instinct. One that's been ingrained into the very fiber of humanity. But the question of how and why data security became a vital concept remains. The answers to these questions lie in the time when people first started targeting data as a means of spreading unrest and holding power.

In a time and age when everything was on paper, all thieves had to do was run away with the documents, but then came the era of digital data, and the playing field just got a whole lot bigger.

THE 1970S: CREEPER STRIKES THE ARPANET

First used in 1969, ARPANET - Advanced Research Projects Agency Network was developed by the Advanced Research Projects Agency (ARPA) arm of the US defense. Initially designed to provide connectivity across all the computers at the Pentagon-funded research institutions, it is now attributed as the forerunner to the internet. Around the same time, ARPANET came into the world, Ben Thomas from BNN created 'Creeper' to create a self-replicating program that could transmit to other computers. It was designed to target the ARPANET-linked Digital Equipment Corporation (DEC) computers. Although the Creeper was not malicious, unbeknown to them, they had just shown the world how to create a computer virus.

THE 1980S: RISING CONCERN FOR DATA SECURITY

The 80s is the decade when the western world saw the rise of computer clubs and more and more computer geeks outing their potential. An era of creative excellence is taking root. The decade saw a quick shift of interest in viruses from harmless fun to malicious intent. The year 1986 witnessed the launch of the first malicious virus, the brain virus. The brain virus specifically targeted floppy disks by replacing the boot sector with the virus, inevitably slowing down the disk drive. All this while data security as a concept started gaining more and more attention.

THE 1990S: THE WORLD JUST GOT SMALLER

While the 90s did see an alarming increase in the chaos created by the launch of computer viruses left and right, it was also the decade that shaped data security into the set of procedures and protocols that we know today. A major incident that kickstarted this change was the 'Solar Sunrise' breach. The year 1998 witnessed two Californian sixteen-year-olds along with their eighteen-year-old Israeli mentor shock the world as they hacked into the US Department of Defense’s computers. The teenagers used a virus to gain access to the computers operated by the government, the military, and the private sectors.

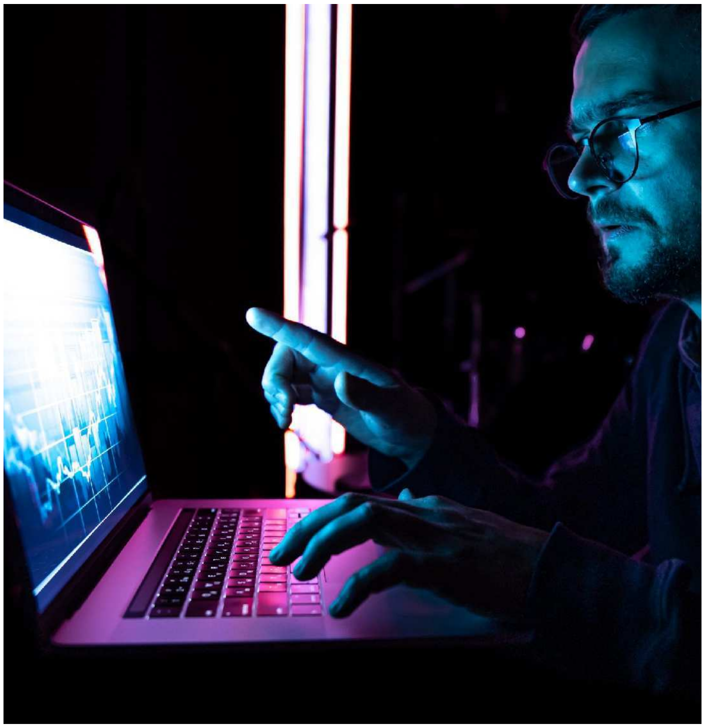
The young hackers had zeroed in on a common OS vulnerability and then devised their MO comprising of four steps:

- Probing the system to ensure the vulnerability was there
- Exploiting the vulnerability
- Placing a sniffer to gather data
- Returning later to collect the data

This incident propelled thinkers and computer enthusiasts across the globe to give more thought to data security.

THE 2000S: A NEW MILLENNIUM WITH EXPONENTIAL ADVANCEMENT IN TECHNOLOGY

The first ten years of the twenty-first century saw the evolution of harmful online activities into a lucrative criminal enterprise that was largely motivated by financial gain. Millions of Microsoft Windows machines linked to the Internet were infected by the Sobig Worm in August 2003. This was swiftly followed in 2004 by the notorious "MyDoom." Hackers broke into Target's servers in 2013 and took somewhere between 70 and 110 million customers' personal information. The projected loss from this specific data breach was around $162 million. Target did not recognize the attack on its own. Credit card processors, who saw an increase in fraudulent transactions using credit cards that had previously been used at Target, were the ones that notified the company.



Every single one of Yahoo's 3 billion email users was a victim of cybercrime in 2013. Reviewing data provided by law enforcement in 2014 alerted the authorities to the breach. Yahoo hired InfoArmor's chief investigator, Andrew Komarov, to find proof that a dark web vendor was selling a list of more than a billion Yahoo accounts for about $300,000.

2

Importance of data security

Data security is the technique of preventing digital data from being accessed by unauthorized parties, corrupted, or stolen at any point in its lifecycle. It is a notion that covers all facets of information security, including administrative and access controls, logical security of software programs, and physical security of hardware and storage devices. Organizational policies and procedures are also included.

Robust data security measures, when executed correctly, guard against insider threats and human mistakes, which continue to be among the main causes of data breaches in the modern era, while also safeguarding an organization's information holdings against cybercriminal activity. Implementing tools and technology that improve the organization's visibility into where its crucial data is located and how it is used is a key component of data security. In a perfect world, these technologies would be able to automate reporting, apply protections like encryption, data masking, and redaction of sensitive files, and apply protections like encryption, data masking, and compliance with regulatory standards.

In a perfect world, these technologies would be able to automate reporting, apply protections like encryption, data masking, and redaction of sensitive files, and apply protections like encryption, data masking, and compliance with regulatory standards.

INFORMATION GOVERNANCE THE NEW NORM:

Every facet of how organizations today operate and compete is being radically changed by digital transformation. Enterprises are producing, storing, and manipulating an ever-increasing amount of data, which increases the need for information governance. Computing environments are also more sophisticated than they used to be, frequently encompassing the public cloud, the enterprise data center, and a variety of edge devices, including robots, remote servers, and Internet of Things (IoT) sensors. The increased attack surface that results from this complexity makes it harder to secure and monitor.

Consumer understanding of the value of data privacy is growing concurrently. People everywhere are educating themselves about the various privacy laws that have been passed recently, in response to the growing public demand for data protection efforts, like the California Consumer Protection Act (CCPA) and Europe's General Data Protection Regulation (GDPR). The Sarbanes-Oxley Act (SOX), which shields shareholders in publicly traded companies from accounting errors and financial fraud, and the Health Insurance Portability and Accountability Act (HIPAA), which protects electronic health records, are among the long-standing data security regulations that these new regulations join. Every business has a significant financial motive to ensure compliance given the potential penalty of millions of dollars.

COMMERCIAL WORTH OF DATA

Data's commercial worth has never been higher than it is right now. Intellectual property (IP) loss can affect future innovations and profitability. Consumers place a greater emphasis on reliability as most of them say they won't buy from businesses they don't believe will protect their data.

The risk matrix of an organization grows as its data footprint spreads across more environments, partners, and endpoints. Information that is sensitive and valuable is in danger from cybercriminals looking to exploit security flaws. A zero-trust approach to security is based on confidently securing data, which serves as a crucial foundation for any corporate process.

Whether deployed on-premises or in a hybrid cloud, data security solutions enable more visibility and analytics to detect and eliminate cyber threats, enact real-time controls, and oversee regulatory compliance.

3

Cornerstones of data security

Did you know?
The consequences of a security breach in a business go beyond affecting just its employees. The monetary loss in itself is a big blow. According to a recent Cyberthreat Landscape report by Acronis every hour of downtime due to a ransomware attack costs upto $250,000.

Source: Acronis

Together, confidentiality, integrity, and availability are regarded as the three key ideas in data security. The formulation of security policies for businesses can be influenced by taking into account these three elements collectively within the "triad" framework. Understanding the relationships between the three is made easier by considering the three notions of the CIA triangle as a whole rather than as separate ideas. Neglecting one or more of these principles can lead to security vulnerabilities that can be exploited by cybercriminals, potentially resulting in financial loss, reputation damage, or legal consequences. By taking a holistic approach to data security and considering the CIA triad as a whole, businesses can better protect their data and systems from a range of threats.

CONFIDENTIALITY

Special training may be required for those who have access to sensitive documents to protect data confidentiality. Authorized individuals can benefit from training to become more familiar with risk factors and preventative measures. Strong passwords, password-related best practices, and knowledge of social engineering techniques are possible additional components of training to deter users from violating data handling policies with good intentions and potentially devastating outcomes.

Requiring an account number or routing number when conducting online banking is a good example of a technique used to protect confidentiality. Another popular technique for maintaining confidentiality is data encryption. The use of user IDs and passwords is conventional practice, and two-factor authentication (2FA) is gaining popularity. Security tokens, key fobs, and biometric verification are other choices. Users can also adopt security measures to reduce the number of locations where information is displayed and the number of times it is transmitted to complete a necessary transaction. Documents that contain highly sensitive information may require additional security precautions, such as storage solely on air-gapped computers, disconnected storage devices, or in physical copy form.

INTEGRITY

The safeguards to protect the integrity of data include user access restrictions and file permissions. Version control can be used to stop authorized users from making mistakes or accidentally deleting things. Organizations must also provide some method for detecting any data changes that can happen from non-human events like an electromagnetic pulse (EMP) or server crash.

Checksums, including cryptographic checksums, may be used in data to verify its integrity. Redundancies or backups must be accessible to restore the impacted data to its original state. Digital signatures can also be used to provide strong anti-repudiation protection, which makes it impossible to dispute the evidence of logins, messages transmitted, and the reading and sending of electronic documents.

AVAILABILITY

The best ways to do this are to keep all hardware under strict maintenance, fix any hardware issues as soon as they arise, and maintain a stable OS environment free of application conflicts. Additionally, it's critical to stay up to date on all required system upgrades. Equally crucial strategies include ensuring appropriate communication capacity and avoiding bottlenecks from occurring.

Quick and flexible disaster recovery is essential for worst-case circumstances. This capability depends on the presence of an extensive DR strategy. When creating precautions against data loss and connection interruptions, unpredictable events like fires and natural disasters must be taken into account. To prevent data loss in the event of these occurrences, a backup copy of the data may be preserved in a remote location, perhaps even in a fireproof, watertight safe. Additional security measures, such as firewalls and proxy servers, can protect against network invasions, malicious Denial of Service (DoS) attacks, and unavailable data.

WHAT CAN BE DONE?

Although the concept of a data breach might be a very scary one considering the hefty consequences, securing the data with the right tools and approaches is not too hard to achieve. Some tips and tricks to keep in mind...

- Staying up-to-date on the updates and patches
- Strict control over who gets access to what and for how long
- Content archiving - sidestep the chaos of saving all the data on the primary storage devices
- Filter anything and everything that comes inside
- Encrypting data

Apart from these, there are a few different concepts that go hand in hand to ensure data security in any organization.

- Enterprise Content Management (ECM) - a blanket term covering the collection of procedures, technology, and tactics that control, protect, deliver, and archive information to the appropriate individuals at the appropriate times.

- Virtual Desktop Infrastructure (VDI) - stops exfiltration of data into a USB or hard drive all the while improving workplace flexibility, cost-effectiveness, and centralized troubleshooting.

- Data Loss Prevention (DLP) - a strategy that combines technologies, tactics, and procedures to secure data protection by prohibiting unauthorized personnel's access to confidential information held by the company.

- Unified Endpoint Management solution - help businesses keep track of all the devices used by their employees, manage and update software and applications on those devices, and enforce security policies to protect company data.

4

Hexnode aiding data security

Hexnode's data security plan involves the perfect blend of comprehensive security, Data Loss Prevention (DLP), containerization-based work profiles, application and content security, Device Theft Prevention and complete threat management.

HEXNODE'S SUPER-EFFICIENT CENTRALIZED CONSOLE

Hexnode is a Unified Endpoint Management (UEM) solution that offers a powerful yet easy-to-use console for managing endpoint security. Developed by Mitsogo Inc., it is designed to provide a comprehensive security suite that is adaptable to the modern workspace. The UEM is developed with meticulous attention to detail, allowing for easy management of enterprise standard password rules and system-level encryptions such as BitLocker and FileVault. Hexnode's security features are designed to meet GDPR and SOC 2 regulations, giving users the confidence to manage their data and infrastructure safely. With its expert-prepared checklist, Hexnode ensures that all security requirements are met.

ALL-ROUND SECURITY

Hexnode assists the company in establishing data security rules that aim to reduce unintentional data loss. The IT manager can make sure that confidential information is secured on company-owned devices. Use Hexnode to limit data transmission from a managed device using tethering, Bluetooth, and USB. To reduce dangers brought on by data interception, mandate data channeling through regulated corporate Wi-Fi and VPNs. To stop data from leaking into unmanaged programs, enforce copy/paste restrictions. Managed open-in controls prohibit the opening of managed content and applications from unmanaged sources.

CONTAINERIZATION

Hexnode ensures data security not only in the corporate-owned devices but also the personal devices deployed in the corporate environment. Strike the right balance between data security and employee privacy by making use of the containerization-based work profile feature pushed out by Hexnode. In simple words create a separate workspace or container to house the work-related applications, documents, and other data. Eliminate access from unmanaged sources by implementing separate container password and open-in policies. Experience application and content security at your fingertips with Hexnode by employing an array of security features and functionalities that empowers its workforce with ready access to apps and content.

PROTECTING DATA ON LOST/STOLEN ENDPOINTS

But what happens if the device is stolen or lost? Can the data be protected even then? The device theft protection strategy that Hexnode applies is a combination of real-time location reports, immediate device lockdown, custom messaging even in lockdown mode, and selective wipe-down of corporate data. This strategy takes care of data security in case the device is either lost or stolen.

MANAGING THREATS

Threat management is a well-known facet of endpoint security. Hexnode enlists multi-level threat monitoring, detection, and protection based on a zero-trust strategy, continuously checking device integrity and adherence to management standards. Hexnode ensures maximum security through thorough periodic checking. The strategy technically involves:

- Compliance tests that are real-time to find vulnerabilities and policy changes.
- Protecting smartphones against jailbreak (for iOS) or root access (for Android), as these scenarios increase the risk of security breaches.
- Fixing non-compliance by imposing restrictions or implementing remote wiping.

Conclusion

As our world becomes increasingly digital, the importance of data security cannot be overstated. With the potential for devastating consequences such as data breaches, identity theft, and financial loss, safeguarding sensitive information has never been more critical. By staying vigilant and implementing robust security measures, we can ensure that our data remains safe and secure in an ever-changing digital landscape.

There is no denying the fact that data is here to stay. Day after day the importance of data is only increasing and so is the awareness amongst the general public. Data is the modern equivalent of a king-maker. Whoever has data holds raw power in their hands. At an age and time when data is gaining all this importance, it is only natural to strive towards protecting your data.

What better way to protect your data than equipping yourself with a robust and dynamic Unified Endpoint Management solution that keeps evolving to keep up with the current market trends all the while standing rooted in the global market conditions? If endpoints are the doorways into an organization’s data, then UEMs like Hexnode are the cyber-tight solutions to bolt these doors. Lock your doors with the best fail-proof bolts on the market.