SecureAge

Using Transparent Encryption to Defeat 12 Common Data Breaches

SecureAge Whitepaper 2020

The New Cyber Security Perimeter

Securing the network perimeter has long since been recognised as insufficient. With today's environment of local networks, networked devices and cloud applications, organisations use security techniques such as Zero Trust, the Software Defined Perimeter and Microsegmentation to cope. These approaches and related technologies are designed to block unauthorised access to data containers, i.e. files. Control over access to files is the new security perimeter.

Data Breaches Are Common Despite These Controls

However, with a reported 12.3 billion data records reported lost or stolen in 2019 it's clear that data theft remains a common problem. There will always be flaws in operating systems, network hardware and other devices that evade cyber security controls and that can be exploited to provide unauthorised access to files.

> Microsoft SMBv3 vulnerability could enable an unauthorised attacker to execute code on the target server or client machine, providing immediate, privileged access to data

The human factor is of great importance as well. Beyond the external actor, insiders and associated third parties are perhaps the most significant source of data loss – whether accidental or deliberate – because they are authorised to access information.

This raises an important problem with technologies like those mentioned above: they are unable to distinguish between authorised access **to** data and unauthorised **use of** data. This matters because these systems do not protect the data itself within files. So files – and importantly, the information held within them – may be exfiltrated even by a legitimate user because they have authorised access.

Data Breaches – Four Paths

Data is broadly lost or stolen via one of four paths.

A. Insider Data Theft

Here, an individual who, at least, appears to be a legitimate user steals data.

B. Privileged User Data Theft

Privileged users have wide access to data and are in a position to exfiltrate it.

C. Hackers Breaking In to Access Data

Stolen or purchased user credentials, malware or network vulnerabilities can all be used to hack in.

D. Human Error

We're all going to make mistakes. At some stage data will be vulnerable as a result.

Document Structure

Using the structure of the four data breach paths, we will examine a variety of data theft scenarios. These scenarios use techniques that evade existing cyber security tools that are intended to block unauthorised data access. For each scenario we describe how data can successfully be exfiltrated in that environment, and then how SecureAge's approach would mitigate the threat.

A Data-Centric Approach to Cyber Security

Information is contained – unprotected – inside files. The billions of data records, not to mention confidential information and intellectual property, stolen or lost every year are all contained in files which, once outside the organisation are completely unprotected.

SecureAge's SecureData takes a data-centric security approach by protecting information at its most fundamental level – the file – through encryption. Unlike other cyber security products which block unauthorised access to files, or which are selective about which data to protect, SecureData inherently protects all data inside all files using encryption.

Once stolen, files encrypted using SecureData are useless to the data thief because they will be unable to decrypt them. Only this approach is capable of ensuring that stolen data is inaccessible – even if exfiltrated by an insider who has authorised access to the data.

Data Theft Scenarios A

Insider Data Theft

1. User Account Compromise

A user's login and password is compromised. The criminal operates on the compromised user's laptop or has gained access to the corporate account via remote or virtual desktop. The criminal – perhaps an insider – has access to all information that is available to the compromised user account. This data could include personally identifiable information, intellectual property and other sensitive material. Clearly the user account has access to this information because it is a requirement of the job role.

> Three foreign nationals successfully infiltrated the networks of two New York-based law firms to steal inside information (about pending mergers and acquisitions deals) and trade on it. The unlawful gains exceeded $4M

Existing cyber security tools will give access to sensitive files of data based on the identity of the logged-in user but cannot determine whether their intentions are legitimate or malicious. Once the file is stolen it no longer carries any protection so the information can easily be accessed.

Solution

With SecureAge's SecureData, files remain encrypted on all storage media at all times. The unobtrusive nature of SecureData means that users are in no way disrupted, and in fact do not need to be aware that file encryption is going on in the background.

Even though the criminal may be able to view files when logged in to the user account, SecureData ensures that when copied to a new storage location – say, to a USB stick – files will still be encrypted and therefore useless once taken outside the organisation. If token-based authentication were in place, where encryption keys are stored on the token, a criminal using stolen credentials would be unable to view file contents without access to the token.

2. User Extracts Data From an Application

A legitimate user copies or exports application data into a local file. The application's own security no longer applies, so the data in the new file is not protected and can easily be stolen.

> A senior auditor at Morrisons Supermarket leaked payroll data of around 100,000 employees in an attempt to damage the company because of a grudge

Solution

SecureData's inherent file-level encryption silently encrypts files upon creation, maintaining this protection throughout the file's lifecycle. If data is copied or exported from an application into a new – or existing – file, it will be encrypted at source and will remain protected even if the authorised user takes the file home. However, outside the organisation the file cannot be decrypted.

Other file encryption products rely on users making active decisions to encrypt or not. This may be data classification that encrypts files based on a specified status, or it may be direct file or folder encryption like Microsoft EFS. Either way, leaving users to make these decisions is problematic since (a) they may be unaware of the privacy and security impacts of their choice, and (b) they may make a choice based simply on convenience rather than on security.

3. Database Log & Temporary Files Stolen

Database log or temporary files containing sensitive information are copied to USB storage. Log and temporary files are unprotected and not classified as important by rights management software, and so are not protected by them. In addition, unstructured files along with log and temporary files are not protected by database Transparent Data Encryption (TDE) products so this technology does not prevent information theft.

> Bithouse Inc., the developer of the Peekaboo Moments app, failed to secure more than 70 million log files that included information such as email addresses, geographic location data, detailed device data, and links to photos and videos

Solution

By encrypting all files in every storage location, SecureData ensures that no information is unprotected. In this way, any stolen log or temporary files remain encrypted and useless. Many applications in addition to databases generate temporary files that contain elements of information that could be sensitive – Microsoft Office applications represent just one such group.

Rights management or classification solutions disregard temporary and log files as unimportant. However, they often contain much of the data held in the primary files. SecureData's seamless approach to file encryption is transparent to users and applications alike, with no performance impact due to the way that data is "streamed" through the encryption engine en-route to or from memory. In addition, its use of the AES-NI instruction set in the CPU ensures that encryption processes are faster than I/O.

4. Ineffective Third-Party Security

A third-party partner company or consultant that processes sensitive data does not maintain adequate security over information. Being outside of your control and constant oversight, third parties represent a potential source of data loss.

> Nedbank security breach involved 1.7M customer records at a third-party service provider. Though the data was sent to the third-party vial SSL/TLS, it was stored unencrypted

Solution

Mandating that third parties use SecureData will mitigate this problem. Any data then stolen from the third-party or consultant would be encrypted and therefore useless. Beyond deploying SecureData, the third-party's work will be unaffected due to the unobtrusive nature of the file encryption technology. Your data will remain encrypted but can be accessed, modified and managed as necessary.

Security Management Server (SMS) enables you to maintain control over the third-party endpoint data use. It also ensures that your data remains under your control using your encryption keys. Access to that data can be revoked by changing the appropriate policy via SMS

Data Theft Scenarios B

Privileged User Data Theft

5. Privileged User Accesses Unauthorised Files

A privileged user employs their access rights to steal files that contain data which they are not supposed to see. If an individual has legitimate access to files – access they need to do their job – then they can steal the files. Administrators must be able to manage files – for example, to move them from server to server or to restore backups. This ability usually means they can also see the contents of those files. While audit logging and monitoring can tell you what happened after the event, it cannot prevent the data theft.

> Edward Snowden used his position as administrator to steal around 1.7M documents from the NSA in the US

Solution

SecureData provides per-user file-level encryption so that only the authorised user can decrypt each file. Administrators can still move files and manage permissions, but they are not able to decrypt and access file contents. In this scenario the privileged user can do their job, but they are not able to view the contents of the files they are managing. In addition, SecureAge SMS will record any unsuccessful attempts to decrypt files.

6. Administrator Steals Files From a Backup

A privileged user accesses backup media and steals files containing intellectual property Administrators must be able to access the contents of backup media so that they can restore files when required. Backups are often protected by encryption, but administrators need access to the backup's decryption keys – so they are able to restore backed up files.

> Millions of users' data were stolen from Uber. The hackers gained access to an Amazon web server using credentials that were mistakenly left in a GitHub repository. Files stolen included a backup that contained customer data

Solution

With SecureData's per-user file-level encryption any backup will now contain individually encrypted files. Administrators can still restore these files from backup media, but they are not able to decrypt and access file contents.

Data Theft Scenarios C

Hackers Breaking In to Access Data

7. Malware

An insider successfully deploys malware on your network, or a user falls victim to a phishing attack. The malware remains dormant for some time then exfiltrates data that it has found. Finally, it encrypts everything, demanding a ransom for release. Social engineering, spear phishing, deepfakes, etc. are increasingly sophisticated, so user education cannot guarantee that a busy professional will not click a harmful link or open a malicious document.

> Travelex suffered a ransomware attack knocking their business back to manual processing for several weeks. Commercial clients were unable to offer currency services while consumers were left out of pocket. It is reported that client information was stolen as well

Malware is designed to exploit vulnerabilities – technical and human – that enable the evasion of corporate perimeter controls and internal security. Having gained access, file exfiltration is straight forward. In addition, the hacker is in the position of being able to make thousands or millions of attacks, relying on just one being successful. The organisation, however, must defend against all attacks.

Solution

While it is at the very least undesirable to have unauthorised processes – malware – operating on your network, SecureData will ensure that any files stolen will remain encrypted. The attacker will find that once stolen, the files are useless to them. In addition, SecureAge's SecureAPlus is an application control and whitelisting facility which ensures that only authorised processes are allowed to run. Even an authorised user cannot execute malware.

A user who accidentally clicks a harmful link or file will find that the associated malware – whether executable, fileless attack, script or macro – is blocked from executing since it is not on the list of authorised processes. Using SecureAge products this scenario will fail both in data theft and also in disrupting the organisation.

8. User Account Compromise

An external actor gains access to the target network remotely using stolen user credentials. He operates on his own machine. In this case the actor has access to all files that are available to the compromised user account. The files are easy to copy out of the corporate network on to the external actor's desktop.

> Personal information of nearly 360,000 Quebec teachers was exposed in a data breach. The hackers stole a user code and password, enabling access to the data and facilitating its theft

Solution

With SecureData, despite having access to the compromised user account, the external actor will not have access to the user's encryption keys. Since SecureData ensures that all files are encrypted at all times, the actor will not be able to decrypt any files. SecureAge Security Management Server (SMS) collects audit data so any (encrypted) files copied outside will cause log information to be recorded. This can be used in any future forensic analysis of the unsuccessful data theft attempt.

9. Files Mis-Classified

A user mis-classifies a sensitive document resulting in a lower level of data protection. Enabling users to classify information can result in incorrect decisions through misunderstanding of the privacy and information security consequences. Automated classification tools can scan and then classify files based on their content. However these systems are only as good as their configuration. If not all data stores are scanned, or if data matching filters are not comprehensive then mis-classification remains a problem.

> Gekko Group – a leading European hotel booking platform – leaked over 1TB of data on customers, clients and partners thanks to an unsecured database, exposing them to account takeover, identity theft and financial fraud

It is important to recognise that today's "ordinary" data could become tomorrow's sensitive information, and that seemingly unimportant information can be misused. This makes the configuration of classification rules for the purpose of cyber security particularly difficult.

For example, Facebook's breach of 50 million accounts resulted in data that may have seemed fairly harmless, but could have been used to crack security questions, create fake accounts and scam users. Classification is useful for many purposes but relying on it to drive security measures is problematic.

Solution

SecureData's transparent file-level encryption protects all files and is designed so that it does not interfere with users or applications. Since all files are encrypted, there can be no concern that some data may be insecure due to misclassification or by being unclassified.

10. Cloud Database Is Left Insecure

A database is held in a cloud service but is mistakenly not securely configured. There are many media reports of cloud databases shown to be unprotected. Human error of this nature does happen, whether the database is part of a live system or a development environment. Either way, sensitive information is sometimes stored in this insecure manner and is therefore vulnerable to theft.

> A Desjardins Group rogue employee used his legitimate user credentials to steal around 2.9M records of customer account data. We must assume that DLP was in place, but it failed to detect this sensitive data export

Solution

With SecureData, the files that constitute a database are encrypted. If those files are stolen then this will not lead to any data loss since the files will remain encrypted and therefore useless.

While database encryption solutions such as TDE would also mitigate database file theft, these systems do not encrypt the associated unstructured files nor log, temporary and report files. With SecureData all of these files are encrypted automatically.

11. Cloud Storage Misconfigured/Misused

A cloud service is used for document storage and management. Configuration of the cloud infrastructure is incorrect, leading to a security vulnerability. A hacker or malicious insider can make use of infrastructure misconfiguration to gain access to files which can then easily be stolen.

A further problem is that the cloud service provider has their own systems administrators who are likely to have access to your files. Data protection regulations such as GDPR or CCPA mandate that only necessary access is given to individuals for the purpose of processing personally identifiable information. Cloud administrators do not have any need to view this kind of data.

> 100 million Capital One customer records stored in AWS were stolen by an Amazon engineer who used a misconfigured firewall to gain remote access to 700+ folders of data. The on-going theft was not discovered for 4 months

Solution

With SecureData's per-user, file-level encryption all data is encrypted. If we consider a data replication service like OneDrive or G-Drive then with SecureData, files are stored encrypted on the local system drive and the replicated cloud copy is also encrypted. SecureData's file encryption ensures that the only data which is unencrypted is that required to be in memory during application operation.

This means that files stolen by insider, cloud administrator or by an external party will remain encrypted and useless to the data thief. In addition, the cloud administrator is unable to view the contents of your files.

12. Files Stolen From a BitLocker-Protected Virtual Desktop Server

A server that provides virtual desktop services has BitLocker enabled to ensure that all data on the disk is encrypted. Files are stolen by an insider.

Full Disk Encryption (FDE) facilities such as BitLocker are only effective on systems that are not running. Live systems with BitLocker deliver any data in unencrypted form to all processes that request them – whether legitimate or malicious. FDE is great for protecting data on a lost laptop, but otherwise is sometimes used so that the "Is encryption deployed?" tick-box can be checked. FDE is of no use on a server that runs all the time.

> The details of 10.6 million MGM hotel guests were posted on a hacking forum. The data was gathered through unauthorised access to a cloud server which no doubt had FDE enabled

A rogue employee, compromised user account or privileged user can therefore easily steal any data which they can find on the system since the files will be handed over unencrypted.

Solution

SecureData's inherent file-level encryption maintains persistent encryption, with data only being decrypted when accessed by an authorised individual using their encryption keys. And even then, the data on disk remains encrypted at all times – even if copied elsewhere. Since the encryption/decryption process is transparent, the user (and application) is unaware of this activity. This is the key to making file-level encryption a practical security solution.

Conclusion

We have discussed a set of data theft scenarios along with reported examples. In each case, data can successfully be exploited because once stolen and outside the control structures of the organisation, the information is unprotected in the exfiltrated files.

If a file is stolen then with SecureAge SecureData the data is completely inaccessible. Making stolen data useless outside the organisation mitigates the devastation of a data breach – regulatory, brand damage, legal, business recovery, etc. The SecureAge approach ensures that intellectual property, sensitive and confidential information is not compromised. Every file is protected, in every place, and protection is maintained every time the file is touched in any way.

SecureAge Technology

Placing real security and usability on equal footing, SecureAge Technology is a data security company headquartered in Singapore. SecureData was first launched in 2003 for the Singapore government, based on a refinement of PKI security techniques. SecureAge made its patented PKI-based encryption an inherent and invisible component of data protection, soon becoming the preferred data encryption partner for additional government and public entities. These long-term and deeply integrated relationships have provided SecureAge with extensive experience of securing the data of large and complex organisations.

SecureAge data security solutions provide public and private entities complete control over data movement within their networks. Every File, Every Place, and Every Time.

Security products from SecureAge have been selected by organisations that need the highest levels of data protection. Customers include various agencies in the Singapore, Hong Kong and Japanese governments; British American Tobacco; Sony; Narita Airport Technologies; the Government Savings Bank in Thailand and GRG Banking.

SecureAge Technology: Our Approach to Data Security

Proactive Protection, Which Is:

Data Security

Data security means pervasive encryption. Data should be secured at the most basic, self-contained unit: the file. Competitive solutions only protect some of the data some of the time, focus on compliance rather than security, or add complexity that introduces risk. Perimeter defences are insufficient as users (the most vulnerable segment of any system) are already inside.

Application Integrity

Application integrity means control through whitelisting and binding of data to applications. Only authorised processes should access specific data for specific purposes. Traditional anti-malware systems represent passive protection, which is too late. They focus on previously known malware and attempts to stop malicious processes that are already active.

Usability

Usability means inherent & invisible technology. Solutions should remove the human element entirely rather than try to account for or change it. Training and monitoring don't work all of the time, and if the solution is not natural, people will create their own (non-secure) methods. Users should be able to work just as they want or need to without additional considerations.

No Trade-Offs

In SecureAge there are no trade-offs between these principles, and especially, usability is not sacrificed to strengthen data security. Recognising that individuals will find other ways of achieving something if the "proper" way is difficult is a fundamental principle of SecureAge product design.

Find Out More

Please get in touch to find out more about SecureAge's enterprise data security solutions. We're happy to discuss the ways in which SecureAge can improve your data security and arrange a free trial.

Website www.secureage.com

SecureAge

Singapore 3 Fusionopolis Way, 05-21 Symbiosis, Singapore 138633
United Kingdom 74 Mackie Avenue, Brigton, BNI 8RB, Company No. 11734665
Japan 1-16-6, Toranomon, Minato-ku, Tokyo 105-0001, Japan
North America 1801 Old Reston Ave Suite 301 Reston, VA 20190, USA