SecureAge

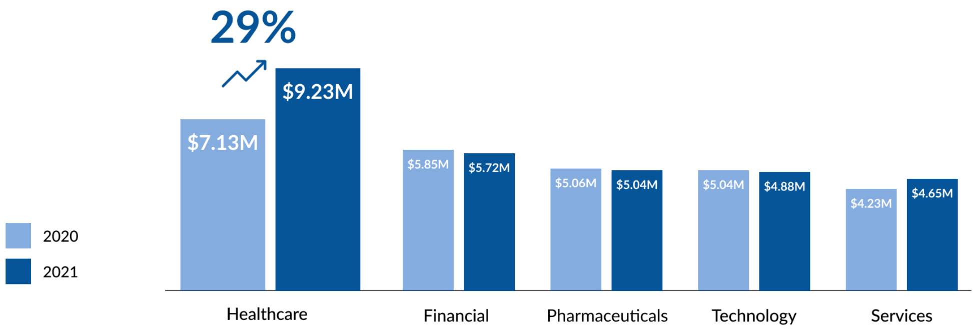
Healthcare:
A Data leak pandemic in the making?

SecureAge Whitepaper 2021

The healthcare industry leads the way in data breaches

For 11 years running, the healthcare sector has succumbed to the costliest data breaches of all sectors. Its total average data breaches in 2021 alone cost US$9.23 million and to worsen matters, the number of data breaches is increasing year on year. From 2020 to 2021, there was a 29% spike in the average total cost of U.S. healthcare data breaches.[1]

Average total cost of a data breach by industry (Measured in US$)



Source: 2021 IBM Ponemon Cost of A Data Breach Report

The Health Insurance Portability and Accountability Act (HIPAA) was passed by the US federal government in 1996 to ensure that health records are properly stored. We would think that with all the regulations in place, data breaches from healthcare would tumble but the opposite is happening. Healthcare organisations struggle to be HIPAA-compliant and are not ready for HIPAA audits or investigations as confirmed by a study by a group of health-plan sponsors.[2] It was found that one-third of the sponsors did not know when the last HIPAA risk or threat assessment was performed. An additional 10% said their analysis was more than five years old. Being HIPAA-compliant at all times is a constant challenge for healthcare entities since it requires a whole host of resources, from skilled personnel to budgets. This is a real challenge to an industry that is already resource-strapped.

But even if all the compliance boxes are checked, the real question is, is the data really secure?

Three healthcare security challenges

The stakes for data security in the healthcare sector are extremely high. In fact, it is increasingly difficult to prevent and limit damages from data breaches due to the nature of how the industry operates. Data generated and stored in healthcare systems present many lucrative opportunities for exploitation. A heavy reliance on new technology that is intertwined into healthcare systems, as well as the way data flows across different parts of the industry, opens up countless opportunities for cybercrimes.

Here are three industry nuances that make data security in healthcare challenging:

1. The nature of the data

It turns out that personal health information (PHI) is more valuable than personal identifiable information (PII) on the black market. While the average cost of a data breach (fines from government, instituting business continuity and incident response plans, employee training and hiring a CISO) from non-healthcare-related agencies is US$158 per stolen record, this increases to US$363 when it comes to healthcare information.[3] PHI is more valuable to cybercriminals

[1] 2021 IBM Ponemon Cost of a Data Breach

[2] Health Plans Struggle with HIPAA Compliance, Unprepared for Audit: https://healthitsecurity.com/news/health-plans-struggle-with-hipaa-compliance-unprepared-for-audit

[3] https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/

as innocent victims can be extorted to pay a price for the release of private and potentially embarrassing medical information, or have it publicly revealed.

Fraud is another common exploitation of PHI. By taking advantage of a victim's medical condition or a doctor's medical notes, cybercriminals can purchase prescription medication and resell it for a profit. Alternatively, they can commit fraud by using medical conditions or victim settlements to create fake insurance claims. Data laundering is another common way that cybercriminals profit by selling the PHI back to the institution from where it was stolen.

The other important thing to understand is that unlike financial account names and passwords that can quickly be disabled after being stolen, medical data lasts forever. People can change their credit-card numbers when their cards are stolen but medical data on ailments, illnesses, and medical procedures cannot be changed and will persist throughout a person's lifetime. As PHI information contains a lot of confidential information on a person's medical history, there is a higher incentive for cybercriminals to target medical databases.

2. The industry's use of legacy systems

Many healthcare organisations function in an ecosystem where new approaches face an uphill battle. In these organisations, there's nothing wrong when everything appears to be running well; the only problem is that legacy systems impose risks to network security when operating systems are no longer supported. As these organisations tend to be operating under tight budgets and with limited IT support, it is thus difficult to justify upgrading legacy systems which are outdated but seem to still be working. 83% of devices used in the US healthcare system are running on outdated and unsecured operating systems.[4] Legacy systems working in a more open environment than what they were designed for make them highly vulnerable to cyberattacks. In fact, health services are also not paying enough attention to what systems the devices they use every day are running on. Case in point, the world fell victim to the WannaCry attack in 2017 that was caused by an unpatched system.[5] Similarly a 'widely used commercial add-on software' was identified as a weak spot that crippled a German hospital in 2020.[6]

Updates are another important part of cybersecurity but legacy systems often cannot be updated to incorporate new security measures and those institutes using newer operating systems are at an advantage as they constantly change and patch these vulnerabilities. The unfortunate part about this is for an industry that is increasingly reliant on technology that's connected to the Internet, and with equipment that is getting more high-tech, any small vulnerability affects the entire system. The question then is, can healthcare organisations patch their IT systems fast enough and get funds for frequent upgrades and updates to keep up with hackers?

3. A reliance on dispersed and unstructured data

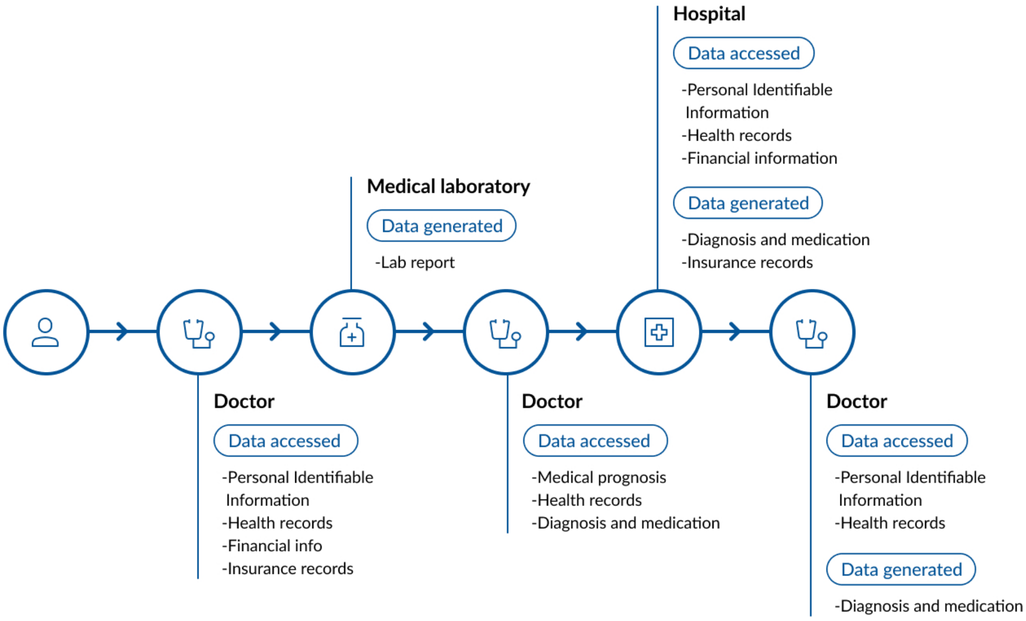
These days, providing medical services does not stop at medical diagnosis and drug prescriptions. Due to the dispersed and long-term nature of the healthcare industry, a huge amount of information needs to be accessed and generated from the very first consultation till the end of treatment - sometimes spanning years. This information includes medical records, prognoses and prescriptions all of which include personally identifiable information such as names, addresses, identification numbers, financial information and insurance details.

[4] https://sea.pcmag.com/mobile-operating-system/36589/while-us-fights-covid-19-83-percent-of-healthcare-systems-run-outdated-software

[5] WannaCry Ransomware Targeted Outdated HIT Infrastructure: https://hitinfrastructure.com/news/wannacry-ransomware-targeted-outdated-hit-infrastructure

[6] German hospital hacked, patient taken to another city dies: https://www.nbcnews.com/tech/security/german-hospital-hacked-patient-taken-another-city-dies-rcna125

Here's how much data is generated, stored, and accessed for a single patient transaction at a medical facility:



The data flow above assumes that the entire process is automated and that all systems are running smoothly, which is not often the case leading to temporary (i.e. not secure) patches and data unaccounted for in the official workstream.

With data stored in databases and moving across clinics, laboratories, hospitals and financial entities all the time, the reality is there are many data-theft opportunities for cybercriminals to exploit.

Healthcare data security will only get more challenging

With the developing Covid-19 situation, more measures will eventually be put in place to track everyone's health status. Vaccine passports and telemedicine are two of the challenges looming on the horizon along with the fact that as data breaches continue to rise, regulations and the bar for compliance will likely increase.

Vaccine passports

While many countries are still developing their vaccination programmes, the world is already looking at opening up again with the use of vaccine passports. Unfortunately, fake vaccination certificates, which are already being sold at around US$150 on the dark web, indicate how lucrative this market can be.[7] With a lot that remains to be seen from this new system that needs to be up and running in record speed, there are many data-security issues that need to be ironed out before we can fully trust vaccine passports.

A few of the burning questions around vaccine passports are:

- How will personal privacy be safeguarded now that individual vaccination status will be stored and accessed by organisations, governments, and third parties around the world?
- Who will have access to the health records that will be spread across different systems?
- How do we prevent leakage of vaccination certificates by the same people who are accessing the system?

[7] https://www.dataguidance.com/opinion/international-vaccine-passports-and-privacy-concerns

- Can we prevent false identities or for that matter, counterfeit vaccine passports from circulating?
- Will the use of a vaccine passport complicate compliance with the General Data Protection Regulation (GDPR) or HIPAA?

Let's just say, it's obvious that both personal and business risks are high.

The sudden and unplanned rise of telemedicine

The need to minimise in-person contact has fuelled the growth of telemedicine during Covid-19 lockdowns. Based on a report by the Centres for Disease Control and Prevention (CDC), the number of telehealth visits increased by 50% in the first quarter of 2020, compared with the same period the year before. Interestingly, consumer preferences for telemedicine might also be here to stay with 73% of these users expressing their intention to continue using such services after the pandemic.[8]

While it was critical that broader access to telemedicine be rolled out quickly, we tended to overlook many security and privacy issues in the process. Not only do commercial video conferencing platforms not comply with HIPAA regulations, medical professionals are also working from home and using their own devices. This means PHI is often saved in a doctor's personal device, making it easier to be stolen.

Researchers also noticed a significant jump in the number of dark web and deep web results containing mentions of the top 20 telehealth companies in 2020.[9] Afterall, healthcare records are very profitable assets on the dark web - they're being sold from US$250 to US$1,000 per record.[10] There's no denying that telemedicine has its merits, but we need to think about managing security risks so that patients can trust the system and in turn, the healthcare provider. A recent survey supports this. It shows that almost half of the respondents will no longer use telehealth solutions if their personal health data is leaked.[11]

As you can see, the benefits of telemedicine come with major patient privacy and data security concerns.

More regulations and a higher bar for compliance

With HIPAA regulations in place come associated security standards. Healthcare organisations - health plans, healthcare providers, healthcare clearinghouses - are all required to report any data breach of PHI and Electronic Protected Health Information (EPHI).

The worrying trend however is that since this requirement, reported healthcare data breaches are increasing at an alarming rate. The HIPAA Journal reports that more than twice the number of data breaches are now being reported compared to six years ago. This also represents three times the number of data breaches that occurred in 2010.[12] In 2020 alone, more than 29 million healthcare records were breached. There were also 642 reported breaches of 500 or more records, which translates to 1.76 reported breaches of such records each day!

Since its enactment in 1996, HIPAA has only been enhanced thrice, in 2003, 2009 and 2013. With the increased reliance on technology and telemedicine, further regulation enhancements is bound to happen sooner or later to protect privacy.

As it is, many healthcare organisations are racing to show they are HIPAA compliant. Unfortunately, this tends to only be checkbox compliant, as healthcare organisations continue to perform risk analysis and implement security in silos. The problem with this checkbox compliance is that it doesn't decipher vulnerability assessments and find out where the real problems are.

[8] https://www.healthcareitnews.com/news/sound-security-practices-key-fulfilling-telehealths-promise-study-shows

[9] https://www.healthcareitnews.com/news/telehealth-biggest-threat-healthcare-cybersecurity-says-report

[10] https://www.forbes.com/sites/louiscolumbus/2019/10/20/5-strategies-healthcare-providers-are-using-to-secure-networks/?sh=4f92688b4b40

[11] https://healthtechmagazine.net/article/2021/02/how-keep-telehealth-secure

[12] HIPAA Journal https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/

The question asked earlier - 'is my data really secure even if all the boxes are checked?' still remains unanswered. Spoiler alert, it's only security that persists when the data is stolen that is a true mark of security.

Current approaches aren't working

As social animals, we tend to fall back on methods that have existed for a while and are familiar to those around us. Many organisations have cybersecurity awareness training and cyber insurance as line items inside their IT standard operating manuals and some regularly adopt the latest solutions from big name vendors. While understandable, we need to ask ourselves if these approaches are successful in protecting data?

Let's increase cybersecurity awareness

Without doubt, the human factor has always been the weakest link in cybersecurity. For too long, organisations have mandated cybersecurity training for their staff, teaching everyone that security isn't just the responsibility of the IT department. However, employee awareness and training can only go so far. A study in the Journal of the American Medical Association finds a staggering number of hospital employees falling for phishing attempts. In this simulation, out of three million phishing messages sent, a whopping 422,062 or 14% of them were clicked by employees.[13]

Based on another study presented at a security conference in 2020, retraining needs to happen at a frequency of every six months.[14] It truly takes a lot of effort to engrain a security DNA within the organisation's culture and in the end, employee education isn't effective in preventing data breaches, they still happen every day. There is only so much that training can do and the truth is don't we want our healthcare professionals diverting time away from saving lives trying to become cybersecurity experts.

Let's feel safe from potential damages with cyber insurance

In the hope of mitigating the damages from cyberattacks, businesses have increasingly been buying cyber insurance. There was a 60% increase in cyber-insurance clients from 2016 to 2020.[15] However, this band-aid solution is giving false hope as insurance companies have been increasing insurance premiums while reducing coverage for some industry sectors, healthcare included. In fact, many insurers have stopped coverage for cyberattacks and adjusted their policies to cover cyber risks instead. As these terms are loosely defined, it is often unclear what exactly is covered by a cyber insurance policy and as a result, it is likely that organisations do not have the coverage they think they do. It's also unbeknown to many, that before any insurance claim is paid, proof of having followed the best practices in data security needs to be shown. Even if the insurer pays the fines and covers all the regulatory fines from a cyberattack, time and corporate reputation are lost.

Let's trust the latest solutions recommended by big name vendors and experts

As with anything technology-related, there will always be new trends and tools recommended by analysts and large corporations. Rather than the usual practice of cleaning up after an attack, companies now want to stay ahead of attacks with approaches ranging from broad frameworks like Zero Trust to narrow solutions for specific threats. Artificial intelligence (AI) and machine learning are always fun to throw in the mix for a little extra comfort and emerging cloud solutions

[13] Journal of the American Medical Association, Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions, 2019: https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2727270

[14] https://securityboulevard.com/2020/10/security-awareness-training-how-often-should-your-employees-get-retrained/

[15] Healthcare Organisations Facing Higher Insurance Costs for Less Coverage: https://www.hipaajournal.com/healthcare-organizations-facing-higher-cyber-insurance-costs-for-less-coverage/

allow us to feel like we're starting over and doing it right. The proof is in the pudding though and none of these things prevented the data breaches we see in the news. Frameworks like Zero Trust don't go far enough, we can never identify and proactively prepare for every threat, both good and bad actors have access to AI, and cloud solutions open up more problems than they solve with vendors abdicating responsibility (and often using your data for their own purposes).

How do we solve the problem of cyberattacks then, you might wonder?

Let's go back to basics and ask ourselves, what do we really want to protect here? Rather than allocating time, manpower and money to implement employee programmes, buying insurance policies and simply riding the latest technology wave, we should really focus on what we actually want to protect. That is the data itself. It's really that simple.

It's time for a new approach! ZERO data breaches in 18 years

Rather than categorising data into different levels of sensitivity, treating them differently and additional 'gates' to protect data, our approach involves treating ALL data as sensitive. This makes the administration of data a lot simpler and straightforward. Often, identifying where sensitive data lies in the organisation is problematic: some 67% of respondents in a 2020 Ponemon report shared that discovering where sensitive data resided in an organisation was challenging.

Encryption has been around since ancient civilisation. Tonnes of research and literature have supported its efficacy and ability to proactively limit the consequences of data leakage. In the event of an attack, encryption renders files useless by masking them in an unusable string of indecipherable characters. While encryption is an affordable and effective means for protecting data, its implementation in IT security plans has surprisingly not been as widespread as it should be due to misperceptions about what protection is currently in place and the costs (both financial and system performance) involved with introducing something better. A 2021 HIPAA compliance checklist reveals that most EPHI breaches result from loss or theft of devices containing unencrypted data and the transmission of unsecured records across networks.[16]

File-level protection: securing your data where it matters

At the end of the day, security is only effective when it is applied as close to the source as possible. Would you leave your jewels unattended on your dressing table but keep your front doors locked, or if you could, would you rather apply locks to each piece of jewellery itself? Borrowing from this analogy, file-level protection works to protect data at the file level. It goes as close to the data as possible, making data protection an inherent property by both design and default.

The SecureAge Security Suite uses SecureData technology to protect ALL data, in every place, all the time. This proactive way to protect data means that in the event of an infiltration via the perimeter, data will not be intelligible to any hacker. Anything that cannot be understood by the recipient does not hold any value for them. Protection is also persistent throughout, whether the computer is on or off, whether the file is open or closed. Unlike alternative data security solutions, protection doesn't just work some of the time.

> **SecureData technology secures research data in a biotechnology lab in the US**
>
> A bioanalytical contract research organisation in the US conducts research and clinical trials in the healthcare sector. In order to comply with an internal audit, they were looking for a data protection solution to protect trial data and patient data from being potentially leaked by internal employees. With SecureAge's Private Key Infrastructure-based encryption (PKI) technology, we were able to ensure that all data collected remained protected in all states (in-transit, in-use, and at-rest) everywhere and that only employees with the appropriate level of access or authority could access specific data. Problem solved.

[16] HIPAA Compliance Checklist: https://www.hipaajournal.com/hipaa-compliance-checklist/

The SecureAge Security Suite offers 100% data protection

Through time-tested technology and design, the SecureAge Security Suite achieves data protection through the following ways:

Persistent data protection

Rather than trying to clean up and aid recovery after cyberattacks happen, each file is fully protected, which renders information useless to any unauthorised personnel.

Proactive protection throughout the data's lifespan

Ensuring data protection in all three states means your files are protected in-transit, in-use and at-rest. Unlike alternative security solutions, every file is protected, every place and every time.

Complies with regulations

Encryption is an easy way to comply with HIPAA. While encryption isn't a requirement for HIPAA compliance, organisations are required to conduct a risk assessment to document measures they take to protect data.

Cybersecurity training not needed

SecureData technology harnesses the power of Public Key Infrastructure (PKI). PKI-based encryption works silently in the background, and supports many commonly used applications across file-level encryption, digital signatures and email.

The SecureAge Security Suite also allows for natural and secure file protection. It encrypts every user file without any user action or decision making and doesn't disrupt user processes. Without requiring any additional infrastructure, it can be deployed on new or legacy systems or alongside existing applications. It is a simple way to ensure your data is protected without running the risk of human error, and allowing your people to work as normal without sacrificing convenience or security.

To find out more about our SecureData encryption technology, visit here.

To find out more about our SecureAge Security Suite solution, visit here.

To talk to us, see a demo, or discuss partnership opportunities, reach out to us directly here.

Frequently Asked Questions

Who is SecureAge?

SecureAge Technology is a data security company headquartered in Singapore with a record of protecting government and enterprise data from the most advanced and persistent cyber threats since 2003. Our government clients include the Monetary Authority of Singapore, all Singapore ministries and statutory Boards, the Singapore military, and the government of Japan. Commercial clients include NTT, Narita Airport, Sony, British American Tobacco, Temasek Holdings, the Government Savings Bank of Thailand, and GRG Banking.

Why has no one offered this before?

Early encryption technologies have been disruptive for users and applications, leading to approaches where users were forced to select only those categories of data that were felt to need strong protection. Encryption has also been seen as difficult. In light of this, 'full disk encryption' has been deployed widely because it implements data encryption without impacting users, applications or servers. This has allowed organisations to check the 'data encryption' box. The problem is, full disk encryption only protects a machine that is switched off, and encryption only applies to disk drives where encryption is enabled, as a result, data copied to another drive is no longer secure.

However, with the next generation approach taken by SecureAge information remains encrypted while the system is running and even while data is being modified. We know it is the data that is important, so with our solution, protection and authentication are an inherent part of the data. By operating at the file system level, SecureAge transparently supports all applications, databases, and services so that no users or apps have to change the way they work.

What impact does SecureAge have on performance?

SecureAge employs specialist encryption functions on the CPU so that normal data processing does not have to wait for cryptographic operations. In addition, only the portion of data that needs to be in system memory gets decrypted. This leaves the file on disk encrypted at all times. Such 'streaming' of data through the SecureAge encryption engine combined with hardware cryptographic functions means the user perceives no impact on performance.

Which file types, formats, and databases does SecureAge support?

Because SecureAge works at the file system level, all file types, data stores, and all databases are supported without any impact on applications. No software changes are required. Data security and authentication are built into each file, so that each file can be read and modified without the need to decrypt the entire file before use.

Can I search file contents which have been encrypted by SecureAge?

Yes, the contents of all files, such as Microsoft Word, Excel, and PowerPoint or Adobe PDF, are still accessible to searches by users who are authorised to access the data.

How does the SecureAge Security Suite help with healthcare regulatory compliance such as Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH)?

While encryption is not an explicit requirement, organisations are required to conduct risk assessment and implement a reasonable amount of appropriate measures to safeguard protected health information (PHI). The SecureAge Security Suite encrypts ePHI such that in the event of a data breach, the data is rendered unusable, unreadable or indecipherable to unauthorised individuals.

Encryption is one of the best ways to protect organisations from penalties associated with a breach when a device is lost or stolen. The 2009 HITECH Act does not require organisations to report if a device is lost or stolen since it is not considered a data breach.

Do I need to deploy SecureAge in one ‘Big Bang’?

No. SecureAge can be implemented in phases, at a pace that is convenient for you. Individuals, groups, departments, or divisions can install the product to enhance their data security without impacting the way they work or interact with others in the organisation.

What should I do next?

With information being accessed from uncontrolled environments, the growth in both the frequency and sophistication of cyberattacks, and the threat of insider data theft, the status quo must be questioned.

100% data encryption is a principle that you accept. And full disk encryption fulfils this. It must, however, be better implemented, so that when a file on a running system is copied from one silo to another location, it remains encrypted. Furthermore, authentication should be built into the encrypted file so that only authorised individuals – not the ‘bad guys’ – can decrypt the data. It is time for you to be able to take charge of your data proactively. Get in touch with us to find out how this is possible.

SecureAge Technology

Placing real security and usability on equal footing, SecureAge Technology is a data security company headquartered in Singapore. Our approach to PKI-based security technology saw the launch of SecureData in 2003 for the Singapore government. By making encryption an inherent and invisible component of data protection, we soon became the preferred data encryption partner for additional government and public entities. These long-term and deeply integrated relationships have provided SecureAge with extensive experience in securing data for large and complex organisations.

SecureAge's data-security solutions provide public and private entities with complete control and protection of the data within their networks. Every file is protected, at every place, and every time.

Security products from SecureAge have been selected by organisations that need the highest levels of data protection. Our forward-thinking customers include various governmental agencies in Singapore, Hong Kong and Japan; as well as 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 is:

Data security

Data security means pervasive encryption. We believe, 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 offers control through 'allow listing' 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 and invisible technology. Solutions should remove the human element entirely rather than try to account for it 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, usually non-secure methods. Users should be able to work just as they want or need without additional considerations.

No trade-offs

There are no trade-offs between these principles for SecureAge. Usability, especially, is not sacrificed to strengthen data security. Recognising that individuals will find other ways to achieve something if the 'proper' way is difficult is fundamental to how SecureAge designs its products.

Find out more

To read more of our white papers click here. Or, get in touch with us to find out more about SecureAge's enterprise data security solutions. We're happy to discuss how we can improve your data security and arrange a free trial: contact us.

Website www.secureage.com

SecureAge

Singapore 3 Fusionopolis Way, 05-21 Symbiosis, Singapore 138633
United Kingdom 74 Mackie Avenue, Brighton, 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