SecureAge

Data in the wild
– the SecureAge approach to ATM security

SecureAge Case study 2021

Introduction

IT professionals in the banking and finance sector tend to spend a significant amount of their time on the game 'whack-a-mole'. But they're not playing this in the arcades. Instead, they're experiencing this game while solving the random day-to-day issues of complex infrastructures and systems in the banking and finance industry.

One of the most common (but often forgotten) example is physical ATM security. 'Nobody uses those things anymore' you might say, but you'd be wrong - over 10 billion transactions are performed at ATMs in the US every year.[1] The scary part is, every one of these transactions is a possible doorway to a Data breach (which the Ponemon Institute estimated cost $3.86 million each in 2020). So, although digital currencies and fintech seem to dominate the news, the banking and finance sector also needs to remember to pay attention to non-news cycle security risks - like physical ATM security.

A leading Thai bank realised the importance of ATM security

Despite increased cost-cutting measures, a leading bank in Thailand was still reporting profit declines due to persistent losses from their ATM network. The bank had 5,000 ATM machines operating across the country so naturally, the most common cost was upkeep as vendor support is increasingly hard to find. But, their reliance on these physical systems was also creating significant security vulnerabilities – both internally and externally.

Insider security threats

Like most banks, their ATM network had inadequate file-encryption solutions to ensure that any and every file could withstand insider threats from technicians. While this is a common problem among businesses who rely on dispersed physical systems, the bank had been misinformed that file-level encryption solutions cannot be easily mapped to existing infrastructure.

As a result, this bank suffered regular internal attacks from maintenance staff who were being bribed to provide access to Data. This was all too easy to do as ATM upkeep entails manual processing and multiple touchpoints. Staff and third parties could easily conceal unauthorised access and plug in external media hard drives with minimal risk of being caught. The worst part about it was, the crime would only be spotted long after the incident had taken place.

Because this bank wasn't thinking about flexible and comprehensive File Level Encryption as a solution, there was nothing to stop cyber criminals from gaining access to customer Data and banking information. In the absence of any security software that secures Data at the file level, cyber criminals could later use it for fraudulent activities or sell it to third parties – all without the bank's, or the customer's, knowledge.

External security threats

Adding to the complexities of 'whack-a-mole' maintenance, the bank was also falling victim to persistent and sophisticated external threats from spoofed card infections via malware. This occurred because their legacy hardware did not have adequate application control to prevent malicious attacks.

The bank had overlooked this security risk because on the surface, ATMs seem like simple machines to interface and conduct transactions. However, the bank soon realised that physical ATMs also act as a portal to their wider network and that a spoofed card could easily cause an ATM to lose connection with the central server, allowing it, or other machines on the same network to be taken over - without triggering any alerts or logs. In the absence of an application control, ATMs could be emptied of their content without the bank being able to detect the threat and block the action.

1 http://www.nationalcash.com/statistics/

Not only were the bank's existing security solutions ineffective at protecting their Data, they also left the central network exposed. The bank was in the process of migrating to newer systems, which entailed changing security infrastructures to support remote working goals. Their CEO at the time referred to their situation as 'adding on new pipes and rooms to a house' and they soon discovered legacy technology, like homes, have hidden flaws and the old doesn't always work with the new. As the new technology they invested in was increasingly required to work in tandem with the old, the bank soon realised more security gaps were surfacing and the seams and foundations needed better protection.

Our client values the simple and proven SecureAge approach

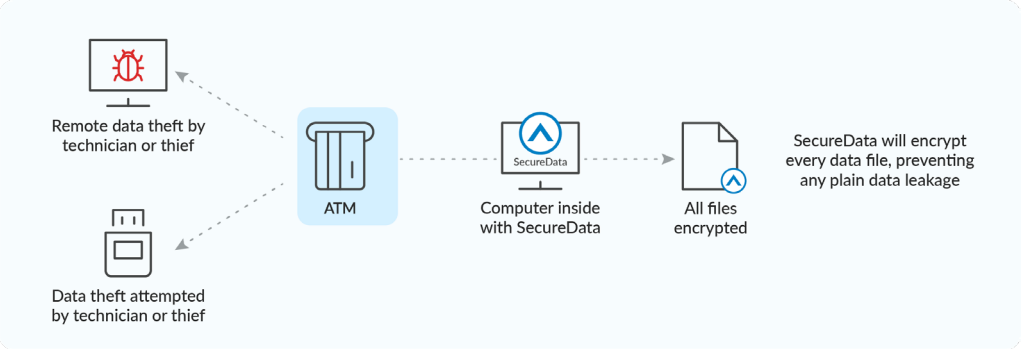
The Thai bank's ATM network was presenting a perfect storm of challenges. The simple reason for this is that physical systems were built for a different era. Not only have customer behaviours changed, but the threat landscape has also evolved.

Intrigued by our focus on protecting the Data itself, and aware of the fact that they could not withstand a breach of any size, the bank reached out to us to find a new way to secure their nation-wide ATM network. They realised that by implementing a security solution that focussed on their most valuable asset, the Data, it wouldn't matter what hardware or system they were using – old or new, the Data would remain protected wherever it went.

We offered the bank two security solutions to counteract the threats they were facing, both of which could be added to existing infrastructure and wouldn't force them to change workflows.

Option 1: 100% Data protection

The SecureAge Security Suite enabled this bank to minimise the impact of insider threats by ensuring that all Data was encrypted, and that any files stolen would be useless to the thief.



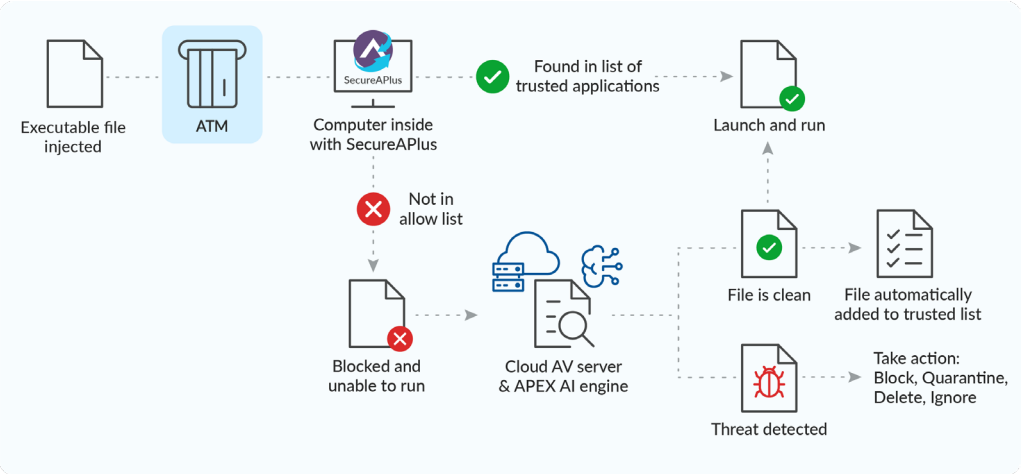
Our unique PKI-based approach to File Level Encryption provides 100% protection for ALL Data throughout its lifespan and in all three states: in-transit, in-use, and at-rest. In addition to providing reliable defence, the SecureAge Security Suite provides offense by blocking ALL unauthorised processes from running, including spoofed card attacks. The Data lens to security recognises that there is no such thing as 'sensitive Data' in today's world and that perimeter defences and Data discovery and classification are ineffective. The SecureAge Security Suite is a complete and versatile Data security addition to any environment.

Option 2: 100% Malware detection

The alternative approach we offered was our intuitive application control, SecureAPlus, which uses an AI-powered engine with a personalised 'allow list' from a central management server.

SecureAPlus is an equally effective and flexible option for physically dispersed and complex systems like ATM networks. While anti-virals are 'deny-lists' of known threats and the best AI on the market today can detect around 99% of known and unknown threats, SecureAPlus makes 100% malware protection possible in any environment.

With SecureAPlus, any threats that fall outside the 99% detection rate of our AI-powered engine are denied by default and then flagged to administrators with recommended actions. When faced with the unknown, competitive approaches apply blanket rules such as delete or quarantine – rules that can have significant unintended consequences. SecureAPlus blocks first and then asks for guidance when it knows it needs it.



Where are your security gaps?

While physically dispersed systems may be incompatible with some security features surrounding access, (such as multi-factor authentication, single-sign-on, and role-based access), it is a misconception that digitisation must include scrapping and starting over. Both the SecureAge Security Suite and SecureAPlus can fill your security gaps without interfering with other applications and without requiring new infrastructure. Our security solutions were designed to protect Data in the wild and plug security gaps wherever they exist – reach out today to learn how we can help.

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. SecureAge's 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 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 that full disk encryption only protects a machine that is switched off, and encryption only applies to disk drives where encryption is enabled. Data copied to another drive is no longer secure.

SecureAge's next generation product implements Data encryption properly so that information remains encrypted while the system is running and even while Data is being modified. It is the Data that is important, so with SecureAge, information protection and authentication is an inherent part of the Data. By operating at the file system level, SecureAge transparently supports all applications, Databases, and services so that no user or app has to change the way they work at all.

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, leaving the file on disk encrypted at all times. This 'streaming' of the Data through the SecureAge encryption engine combined with hardware cryptographic functions means that 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 impact on applications. No software changes are required. Data security and authentication is built into each file so that it can be read and modified without having 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 are obligations under GDPR and other Data privacy regulations affected?

Where organisations suffer a personal Data breach, the acquisition of an encrypted Dataset by an attacker still requires notification to the ICO[1] under Article 33 of the GDPR. However, notification to individuals is not required where the organisation has implemented Data encryption that renders the stolen personal Data unintelligible to any person who is not authorised to access it.

What core banking systems will SecureAge run on?

SecureAge's file system level approach to encryption is applicable across a wide range of core banking systems, including Finastra, Finacle, Flexcube, Temenos and other current and legacy systems.

Can I implement higher levels of security in some areas?

All information encrypted by SecureAge is protected by modern, standard cryptographic algorithms which provide the highest Data security. However, the level of security for authentication can be chosen to meet differing security requirements. For example, staff with access to 'highly sensitive' information may be required to use smartcards with multi-factor authentication to protect their decryption keys, while other individuals may use 'soft' tokens and password authentication for key storage.

Do I need to deploy SecureAge in one 'Big Bang'?

No. SecureAge can be implemented in a phased fashion 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 quantity and sophistication of cyberattacks, and the threat of insider Data theft, the status quo must now be questioned.

100% Data encryption is already a principle that you accept – full disk encryption fulfils this. But this principle must be implemented better, 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 to take charge of your Data with a proactive approach to information security. Get in touch with us to find out more.

1 Article 34(3)(a) states that notification to individuals is not required where an organisation has: "implemented appropriate technical and organisational protection measures, and those measures were applied to the personal Data affected by the personal Data breach, in particular those that render the personal Data unintelligible to any person who is not authorised to access it, such as encryption"

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 '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 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

To see more of our whitepapers click here. 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: 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