BARCLAY TECHNOLOGIES

Solution Brief

Certus Lateo™ raises the bar in security technology

swiss made software

Table of Content

What is Certus Lateo™

Certus Lateo™ is **one** comprehensive solution for data security at the end point and in the entire network and thus protects confidential information and intellectual property from unauthorized third parties.

Quite differently from traditional solutions in the data loss prevention sector, the approach taken by Certus Lateo™ is kept as simple as possible and therefore as cost-efficient as possible.
Look at the topic of data security from a previously unknown perspective and let us convince you of the completely new approach taken by Certus Lateo™.

Working Principle

Certus Lateo™ turns your network infrastructure into a secure network compound, accessible only to devices which have been granted access in the solution's central management. A software component, respectively a driver, is installed on previously-defined members of the network compound. This driver together with the assignment then serves as an automatic identification. If this identification is not present, the machine will be prevented from communicating with the network compound.

This way of implementation wraps a basic protection around your network infrastructure which covers the network traffic as well as mass storage devices like USB Sticks, CD/DVD-ROM and other mobile devices. Your data will be protected once they leave the secure environment.

Scope of Operation

Encryption and blocking functions for:

- Network connections (LAN/MAN/WAN)
- WLAN
- Peer to Peer
- USB Sticks (type independent)
- Memory cards
- Mobile device storage
- External hard drives
- CD/DVD/Blu-ray drives (blocking of write capability)

Advantages of a Layer 3 Encryption

Individual measures for perimeter security are simply no longer sufficient these days because the complexity of the threat scenarios is constantly increasing. Today we need to look at topics such as unwanted data leakage, insider attacks and external attacks.

Encryption is the only way to ensure that data that gets into the hands of third parties is worthless. It is therefore necessary to secure all communication routes that could carry data. This is not only true for CDs, DVDs, USB sticks and other mass storage devices but also for communication routes within the network, i.e. in the LAN/WAN area.

The completely new approach taken by Certus Lateo™ provides you with data security at the end point and within the network as well as with additional benefits like:

- Targeted Attack
- Wireless Local Area Network
- Rogue Access Points
- Smart Phones etc.
- Application Security
- Malware
- Employee Risk
- Unsecure Cable Harness
- Unsecure Network Connections

Targeted Attacks

Studies show an increase in targeted attacks on companies. More than 60% of data breaches where identities have been revealed could be traced to targeted attacks.

Hacking – the new leisure activity of more than a quarter of our youth!
A seemingly very exciting hobby with a still-increasing degree of popularity. Although we know that hacking violates moral principles an international study by Tufin Technologies in the UK has shown that curiosity is stronger.

These days almost everyone can use a 'crimeware kit' to build himself a malicious code with the intention of stealing data and personal information. For example 'Zeus21' is available for around $700 to buy or is even offered as a free download on certain forums, thus opening the door to hacking as a leisure activity even for non-professional computer freaks.

"Script kiddies" hack for fun but professional hackers are making a lot of money these days. According to information from the market research institute Vanson Bourne, who interviewed over 600 responsible IT specialists from seven sectors and 14 countries, more than 54% of those questioned had been victim of a major attack, resulting in an average cost of 6.3 million dollars per day in which the systems were down. This study also revealed that the risk of an attack is increasing and two-fifths of the interviewees were expecting a larger security incident in 2010. Only 20% suppose that they had sufficient protection from cyber attacks for the coming five years.

Once network traffic is encrypted it is still possible for a hacker to gain access to this network but he cannot take part in its communications. As he does not speak the same language than the other systems, because his communication is not encrypted, it is no longer possible to take part in the communication or access the systems. The network is sealed and is simply closed off to attacks from third parties.

Wireless Local Area Network

Do you want confidential information to leave your network "over the air"? It is normally very easy for hackers to gain unauthorized access to systems in the network because many WLAN networks are either not encrypted or only use WEP protection. But WEP, as we have read many times recently, can be cracked within minutes and will then allow access to the systems.

A network that is secured using Certus Lateo™ will also make wireless networks secure. Participation in

network traffic is then only possible using the installed driver and the data that is transferred via the wireless system is also secured with the highly secure encryption technology.

Rogue Access Points

If the company network has not already been secured with adequate solutions it is relatively easy to connect unauthorized hardware (e.g. an access point), even without safety tests or the permission of the IT Manager. This can also be achieved by an employee, who simply purchases an access point at electronics shop because his company does not supply him with one. Likewise an external person could also gain access this way. The IT manager's security policies has thus, intentional or unintentional, been bypassed and information leaves the company via new, previously unknown paths…

Also true in this case: If the network traffic is encrypted no device has access to the network if it does not speak the "encryption" language.

Smartphones etc.

Today it is almost impossible to separate business from private lives and many employees no longer wish to separate their business and private telecommunication conversations. They want a mobile device that can be used for mobile work and also to continue their communication to their private contacts.

The market research institute Vanson Bourne confirms that more and more employees wish to work on their own smartphones. A study by IDC also shows that 95% of the technical experienced employees are using at least one private device for work.

But what happens with company data on private devices? It is so easy to quickly upload a few gigabytes onto the device or to create a new connection with the Internet via a PC and data can already leave the network via new previously unknown routes. The complex security regulations put in place by the IT security department have been avoided but this does not really affect the employee. And the company data is at even higher risk; just imagine how many mobile phones are lost or stolen.

Encryption helps here too: On the one hand the data can be encrypted in the mass storage devices of mobile phones and is thus unusable for unknown persons. On the other hand it is also possible to make sure that a network connection can only be established if the other device also knows the same encryption language.

Application Security

The sector of application security often gets too little attention. New applications need to be integrated in very short period of time and the necessary security concept is lost in the rush.

All applications have weak points - this is nothing new because it is impossible to program several thousand lines of code without errors. This makes them vulnerable to internal and external attacks and thus makes them the cause of various security problems within companies. The most dangerous aspect is that critical business data, which represents a company's capital, is stored in precisely these applications.

Many manufacturers offer application security as part of their solutions but this means that you are quickly using a large number of different, individual application encryptions and nobody can overlook of this jungle of methods. It is for precisely this reason that large companies are now employing application security specialists who use complex concepts to secure access rights to the applications and the transfer of critical data. However small and medium-sized companies often don't have the budget for these specialists.

The encryption of network traffic offers additional security here. Even though it doesn't regulate access rights it does secure data transfers and it is very simple to prevent leakage of requested, sensitive data using portable storage media.

Malware

Trojans camouflage i.e. as Google add-ons. The Trojan Stuxnet spies on industrial system software of Siemens clients, Banking Trojans steal access data and fake bank transfers - and these are just a couple of minor examples that show how sophisticated the community is working on stealing specific data.

An Antivirus software is certainly the best solution for these threats. However the manufacturers often can't keep up to supply the corresponding pattern at short notice. In the case of Trojans, Spyware & Co. encryption of data stream can also help. It does not prevent a Trojan from accessing the network and sending out data. But if the entire data stream is encrypted and there are some accidentally opened ports, this information will also be send out in crypted form and making them useless for the recipient.

Employee Risk

Several surveys - including those by Deloitte in the current study "2010 TMT Global Security Study" - confirm that a company's own employees continue to be one of its greatest, if not the greatest security risk. Whether through carelessness or maliciously, data quickly finds its way into the hands of unauthorized persons and can cause tremendous damage.

The ever-increasing competition between companies is another driving factor for economic delinquency. Everyone is looking for new ways to access the relevant data of a competitor and one of the easiest methods is to find disloyal employees. Employees are ordinary people and can get into various situations in the course of their careers: Financial difficulties, illness, family problems etc. Or someone has built a house and then lost their job shortly after - fears for one's existence set in quickly in these situations and help to lower inhibition thresholds. Disposition to commit an illegal act increases and as it is really easy to copy data onto a memory stick these days the act is very quickly committed.

Encryption is an important topic here as well: Memory sticks and other external storage media may never leave the company unencrypted!

Encryption Technology

Certus Lateo™ simplifies data encryption. This innovative technology contradicts all popular theories of known encryption and enters a new dimension: The principle of the One-Time-Pad combined with a key system in which the key is no longer transmitted in common way.

- **Dynamic key depth per data packet up to 15.048 Bit**
  Each data packet has an individual key with the same length as the raw data.

- **Variable, dynamic algorithm**
  For each data packet Certus Lateo™ generates a unique key. This key is generated based on a random selection out of several algorithms individually for each packet.

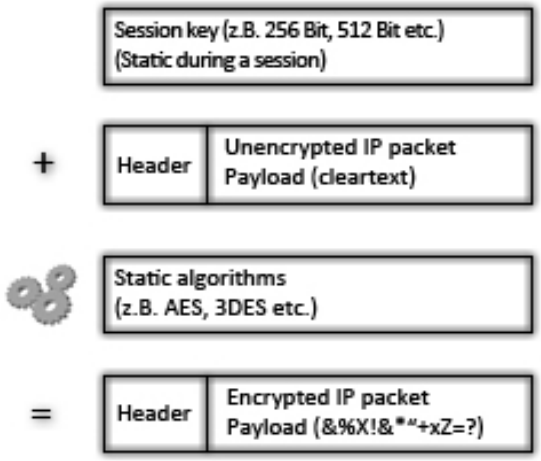
- **No key exchange in common way**
  Keys are not exchanged in a common way, instead the sender and the recipient are aware of the actual key, which allows en/decryption of the data. This handled by an embedded autonomous key management system, which is part of our solution. It does not add any volume to the original data.

- **Real time encryption per block resp. packet**
  Not whole files or disks are encrypted, but blocks resp. packets are encrypted when they leave the system.

- **Mathematical not reconstructable encryption**
  The usage of a key with the same length than the original data results in an absolute secure encryption (based on the One-Time-Pad principle), mainly because multiple readable results are existing.

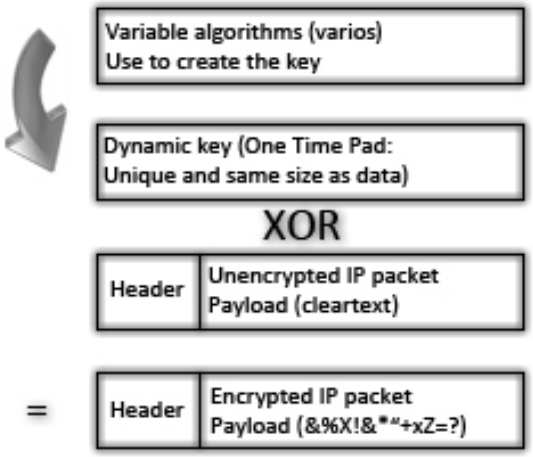
In traditional encryption procedures the key is applied on the plain text message by means of complex algorithms in order to create an encrypted message. This key must then be securely transmitted so the receiver will be able to decrypt the message. Once this key falls into the wrong hands, there is no way of preventing the unauthorized decryption of further messages.

Common solution
Example based on network traffic



With Certus Lateo™ the key is randomly generated at both ends and can be used by both parties (sender and receiver) for encryption or decryption. No key is exchanged in traditional way, thereby eliminating the need for any sort of key management. In addition, Certus Lateo™ is based on the One-Time-Pad, an encryption principle going back to Gilbert Vernam. The generated key always has the same size as the data packet or the data block itself. Certus Lateo™ combines the security of the One-Time-Pad, long proven to be unbreakable, with the additional security of never having to distribute a key. You can't get more security than that.

Certus Lateo™
Example based on network traffic



Advantages

- **No noticeable performance loss despite encryption**
  The unique encryption technology does not generate any noticeable performance loss. This is due to the use of the resources of the network card and by the encryption based on packets and not whole files.

- **No time consuming encryption/decryption of whole files**
  The files on the systems are in clear text and become only encrypted when they leave the secure environment. En-/decryption takes place packet resp. block wise, which saves time and prevents the creation of temp files on the systems that could be used as a target in certain attack scenarios.

- **No additional key management needed**
  Additional infrastructure and high planning and administration costs for complex key management is not required. This also removes additional potential risk that would need further security implementations.

- **No additional password management**
  Because Certus Lateo™ does not need any users interaction, it does not require any login information that needs additional administrative effort.

- **No additional hardware**
  Certus Lateo™ can be installed on any workstation as the central admin console can only be started and managed using a specific dongle. This means there are no additional procurement or maintenance costs apart from the licenses.

- **No configuration backup required**
  The configuration is stored on every installed Certus Lateo™ driver (properly encrypted of course), and can only be changed via the central admin console using the specific dongle. As long as one machine is available the configuration will be in place and no specific backup is required.

- **No maintenance window necessary for adaptations**
  As the encryption is packet-based it can be switched on or off during operation; one packet arrives encrypted and next unencrypted without affecting the overall traffic.

- **No user training required**
  Because Certus Lateo™ runs entirely in the background and does not demand any interaction there is no need to provide employees with specific training. Thus nothing changes in work processes. The only limitation is that encrypted data, for example on a USB stick, can only be read on an authorized machine or that data can no longer be written onto a mass storage device.

Positioning

Various data protection solutions are already available and data loss prevention or data leakage prevention (DLP) is offered by numerous manufacturers. However in order to implement these solutions you need to know the paths by which data can be lost. You need to be ready to undertake a process in several stages, i.e. a comprehensive analysis and a project-based approach. Just procuring a DLP solution - no matter what other manufacturer you choose - is nowhere near enough to ensure comprehensive protection of sensitive data. This effort is just too much for many companies and the purchase and maintenance costs are much too high. That's the reason why there are still so many companies that have not implemented any data security solution and remain very reserved towards the topic.

Certus Lateo™ has a completely different approach and is neither based on data classification nor another method of identifying sensitive data. It also does not require comprehensive data analyses without which the subsequent monitoring is not possible. Certus Lateo™ also covers a large sector with a single solution where other manufacturers provide different products. The encryption itself is based on a totally new technology and is definitely unique and without comparison.

The most important differences are listed in the following table and readers will quickly realize that no comparison is possible.

	Barclay Technologies Certus Lateo™	Content/Context Aware Data Loss Prevention Solution (Check Point, McAfee, RSA, Sophos, Symantec, Trend Micro, Websense etc.)
Field of Application		
Data protected	All data protected	Data Protection based on the classification /keywords (false positive issues). Often limited to specific file types or protocols
Encrypted Network Traffic (Layer 3)	Yes	Provided by a few of the available solutions
Implementation		
Pre Implementation Effort (Policy Framework)	Definition of profiles and membership of machines	- Concept of user rights management - Detection of available data - Defining data classes - Classification of data - Definition of security rules for each combination user/data class
User Authentication	Not required	Required
Additional Hardware required	Not required	Required
Backup/Restore	Not required	Required or as an option available
Encryption Technology		
Algorithm	Various algorithms, dynamically selected – used to define the session key	Most of them are using AES or RSA
Key Management	Not required	Required
Key Length	Up to 15.048 Bit	Up to 1.024 Bit
Key Lifetime	Based on the principle of One-Time-Pad: Each packet has a new, unique key	Per session
Performance Impacts	No noticeable performance impacts	No impacts according to their own specifications
Potential Security Issues due to Key Transfer	None	Yes
User Actions		
User Training	Not required	Essential part for a successful implementation and operation
Impacts on existing workflows/business processes	None	Yes
Administration		
Operational Tasks	Assignment of new/replaced machines to group policy	Constant user rights management and/or file classification, keyword adjustments etc.
Reports to check	None	Yes
Involved Departments	- CEO or HR (depends on who defines security rules per group) - IT Manager or Security Officer	- CEO or HR (depends on who defines security rules per group) - IT Manager or Security Officer - Data Owner - Data Protection Specialist

Prices

Certus Lateo™ is offered as a service for 1, 2 or 3 year periods. The service is an annual fee with no initial cost. 4 weeks prior to the expiration, a message is send and the service may be seamlessly renewed.

The licensing is based on the number of the installed drivers, no matter whether they are installed on a client or a server. The expiration date for additional licenses can be synchronized.

Distribution Channel

To guarantee highest quality in implementation and customer support we work with trained and certified partners. To honor the effort of our partners, Barclay Technologies does not sell the products directly to customers but instead through certified partners.