SOPHOS
Security made simple.

Next-Gen Encryption: The Sophos Approach

Data loss continues to be a real concern for all organizations - no one anywhere in the world is immune, regardless of geography, size, or industry.

At the same time the work environment has changed greatly over recent years. Businesses today need to secure against data loss - and stay the right side of data protection legislation - while also ensuring their people can be as effective as possible in today's competitive environment.

Sophos' Next-Gen Encryption strategy is designed specifically to meet these needs. This paper explains the need for Next-Gen Encryption and how it works, and also demonstrates how Sophos makes it simple for organizations of all sizes to secure their data while enabling their users.

State of Play Today

Today's work environment is much different to that of five or ten years ago. The difference in the device landscape and threats is significant. Let's look at two big changes that have impacted data protection.

The Device Isn't Mobile, You Are

A typical end user has, on average, three devices. While there used to be desktops and the occasional laptop, the landscape has expanded to include tablets and mobile devices. Think of your end users. It's very likely that they will have a laptop and a mobile phone; others will also have a tablet or two.

Mobile devices often contain just as much, if not more, sensitive information than a laptop. They can also be lost much more easily. This means that the potential attack surface is increasing as users have more devices that contain company data.

The typical workforce is mobile and they are expected to remain productive on the road. Productivity ultimately means being able to access corporate data on the device of their choice, from anywhere at anytime.

It's Midnight, Do You Know Where Your Data Is?

Do you know where your company data is? It's located on servers, desktops, laptops, mobile devices, tablets, and removable media devices as well as with cloud storage providers. Sensitive company data is outside the traditional corporate boundaries, primarily because the notion of a corporate boundary has vanished.

How do you define a corporate boundary for your data if it is on a wide variety of mobile devices and storage solutions? These devices are either unmanaged or spend little time inside a company network. Or, in the case of a cloud storage provider, you may not even know where your data is physically stored and who really has access. All of this means that there is a need to protect data where users store it.

Defining the Strategy for Next-Gen Encryption

In putting together our Next-Gen Encryption strategy, we looked at several areas where customers could be impacted by a data loss or breach, which could lead to regulatory violations. Our strategy considers the following areas:

1. Impact from lost or stolen devices
2. How people use data
3. Unintended disclosure due to human error
4. Hacking or malware attacks
5. Simplicity

While we could include targeted attacks (as opposed to opportunistic attacks using malware or phishing, for example) in this list, the statistical chance of a small or mid-sized business being the victim of a targeted attack is quite low. Unless you are a big company, like Sony or Target, or have some very specialized and sensitive information, the bad guys simply won't put in the effort required for a targeted attack.

Impact from Lost or Stolen Devices

The average user has three devices, all of which can easily be lost or stolen. Maybe they leave their phone on the train as they commute to work, or accidentally leave their laptop at airport security as they run for a flight. Devices are small and accidents happen. Full disk encryption is useful for the protection of data at rest and is a good first line of defense. But it is not sufficient to protect your company data based on today's end user behavior by itself.

How Do People Use Data?

Watch your end users for an hour and see how they use data. They create it, in the form of documents, presentations, etc. They copy files to network shares, USB sticks, or to a cloud storage provider. The end user works with files, and files move between devices and the various storage options. In these types of situations, data protection is a must.

Simple Human Error

We are all human. We all make mistakes. Everyone has created an email, attached the wrong file and sent the email out (or sent the intended file to the wrong recipient). There are many examples of simple human error that can lead a data loss or breach. Web browsers and mail clients are great examples of productivity tools that end users use to share data, but which can accidentally expose company data to the cloud or the wrong individual.

Hacking or Malware attacks

Privacy Rights Clearinghouse's analysis of 2014 data breaches categorizes types of breaches, and found that hacking or malware accounted for 51% of data breaches. Malware is increasing in size and complexity all the time. This also includes the opportunistic stealing of data. Malware can't be trusted and definitely shouldn't have access to encrypted data.

Simplicity

Encryption works best when no one notices that it's there. It silently provides protection without impacting the end user. For example, consider HTTPS. The S stands for secure, and means all communications between your browser and the website are encrypted. But most users never notice the difference in the URL they're visiting.

Encryption must be simple to use for both the administrator and the end user in order to achieve a high level of acceptance.

Introducing Sophos Next-Gen Encryption

The Sophos Next-Gen Encryption strategy begins with two assertions:

1. All data that an end user creates is important and must be protected (encrypted). This is known as "always-on" encryption, or encrypting by default.

2. Encryption should be persistent wherever a file is located, copied, or moved.

Encryption is widely considered one of the best ways to protect data. Whether the user is creating a document explaining their new patent idea, or a spreadsheet to justify a new business concept, all of this is important data, and it should be encrypted automatically and transparently. A user shouldn't be bothered with having to decide whether or not to encrypt a file based on their perceived sense of how important it is. In fact, users may not even realize that data is encrypted. This allows the user to remain productive and have their data secure while following existing workflows.

Once the file is encrypted, it must remain that way. Whatever happens to the file, whether it is moved, copied, renamed, and regardless of whether the file remains within the boundaries of the device, the encryption must be persistent. If a user accidentally loses a file, it will be lost in its encrypted form, rendering it useless/unreadable to anyone without permission to view it.

What About DLP?

When people think about data protection, they often think of Data Loss/Leakage Prevention (DLP). DLP and encryption have historically gone hand in hand. While DLP is a great technology, there are many examples of companies failing to implement a DLP strategy after spending a significant amount of time or money on the effort. The issue is the complexity of the task. Rules for data, which you may not have created yet, must be put in place. A common issue is that administrators make the rules too strict and then deal with the workload brought on by false positives. Often, administrators make the rules looser, and then data leaves the organization despite DLP systems. Sophos is turning DLP on its head by removing the necessity to classify data. This simplification greatly helps both the end user and the administrator.

This isn't to say that DLP isn't important. DLP still has a role within Next-Gen Encryption. However, it should be the exception, and not the rule. When the user wants to decrypt data, it is a conscious decision to remove protection from a file. This is the time for DLP rules to be optionally run. If no red flags are raised, the user is allowed to decrypt the file because it contains nothing that is deemed to be sensitive. However, if any flags are raised, the request to decrypt the file is denied. This approach is a failsafe to ensure that files remain encrypted. Additionally, any request to decrypt a file is audited and logged.

Using this approach greatly simplifies DLP and, as the evaluation of DLP rules becomes the exception (used only when data is decrypted), significantly reduces processing requirements.

Synchronized Encryption

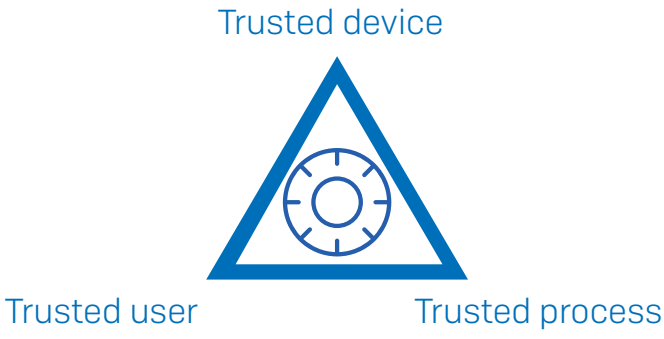
Assuming that all of the user's data is encrypted, the next most important item to protect are the encryption keys that encrypted all of that data.

The core idea of encryption keys is that only trusted devices, apps, and users should have access to encrypted data.

To achieve this, Sophos merges the know-how and functionality of Sophos Endpoint and Sophos SafeGuard Encryption (SafeGuard) products to turn encryption into a threat protection technology. The Endpoint product will do what it has always excelled at, determining the security health status of the machine in question and deciding if running processes can be trusted. And the data protection product will do what it has always been good at, encrypting data and protecting access to the keys.

In order to make a determination on when to release keys and allow access to encrypted content, we triangulate and synchronize user identity, device, and application/process.

In order to be considered trusted and access encrypted data, the user must be using a trusted device, be a trusted user, and using a trusted process or application to access the data.



All three of these conditions need to be validated in order to access the encryption key and to view the data.

In almost all cases, a legitimate, corporate end user is able to access data transparently using a trusted device (i.e., a company issued device) and trusted applications. Should they not meet one or more of these conditions, they will be denied the access key and while they can see the encrypted file, they can't view its contents. In this way, data-stealing malware might be able to exfiltrate a protected file, but that file is rendered useless without the access key.

Trusted Device

There are many ways to determine if a device is trusted. For example, it can be because the appropriate Sophos products are installed. Or it could be because the Sophos Endpoint agent has evaluated the system and given it a Healthy State (or a green Heartbeat™) status. Also, a trusted device can be a mobile device that is managed by the company's EMM solution and thus is in compliance with the company's security policy. Alternatively, an administrator may explicitly state that a system should not be trusted, such as a contractor-use case.

If a Windows or Mac laptop is in an active infection state, as the endpoint is in the process of removing malware, the system most likely should not be trusted. For a mobile device, such as an iPhone or Android Phone, if the device does not meet the corporate compliance policy (for example, if a device is jailbroken or does not have a lock screen password) it shouldn't be trusted either.

Trusted User

Just as there are multiple ways to determine if a device should be trusted, there are also many ways to determine if a user should be trusted. It can be based on their identity, or simply because they could successfully log into their system. There are use cases, such as a user leaving an organization, where users may successfully log into their device but they should not have access to encrypted data.

Trusted Process

Sophos Endpoint will take the lead role in determining as to whether a process is trusted or not. The exact details about how this is achieved, both with and without the Sophos Endpoint, is out of scope for this document.

Generically, the internal logic does not trust PUA (potentially unwanted application) malware, viruses, web browsers or mail clients. However, there are other types of applications, such as torrent programs, that organizations may instinctively not trust to access encrypted data. Web browsers and mail clients are not trusted by default, because these are ways that end users can accidentally share or lose data. This helps protect against simple human error.

Why do we talk about processes and not applications? Primarily, this revolves around ensuring that the end user can remain productive. By only blocking the process which is actually misbehaving, it allows all trustworthy processes to execute unhindered.

Let's look at three examples of a process, other than malware/viruses, and whether it can be trusted.

1. **Notepad**

   Notepad is a self-contained and simplistic application. It can be trusted because it is simple and contains no malicious activity. As Notepad is determined to be trusted, it can access an encryption key. This allows documents created with Notepad to be encrypted by default, and to display encrypted plain text documents.

2. **Internet Explorer**

   Internet Explorer has a history of being exploited, and is a common method for the delivery of malware onto a device. As such, it is not trusted by default. Because Internet Explorer is not trusted, it cannot access an encryption key, and therefore can only access files in their encrypted form. It can't open or view the contents, but can upload an encrypted file to a cloud-based file sharing service.

3. **Microsoft Word**

   Microsoft Word is in a gray area of being able to be both trusted and untrusted. Word can behave perfectly fine and be trusted, therefore when a user uses Word to create a document, it can be encrypted by default. The user can simple double click on encrypted files to read and edit these files. The process is complete transparent. This is because Word is currently trusted to access encryption keys in order to perform encryption/decryption processes in the background. However, Word can also be infected with something similar to a macro virus, at which point Word is no longer trusted to access the encryption key and cannot read encrypted data.

These are just three simple examples of determining process trust that highlight the necessity for Synchronized Encryption to continuously monitor integrity.

Continuously Monitoring Integrity Before Granting Trust

Overall, you want your data protection technology to continuously monitor the security health, integrity, and trust of the system application/process. The goal is to keep end users productive while also keeping data secure. As stated above, if a process is not trusted, then it can only access the file in its encrypted form but not the encryption key to decode the content. The majority of the time end users won't notice that this is happening. However, if the process is malicious, such as malware, obviously it should not be running at all. And, if your system is in a state of active infection, the system should not be trusted. Process trust is the first reaction to integrity, but overall system security health plays a part in the reaction to integrity as well.

Let's go back to the concept of keeping users productive. You want to stop untrusted processes from accessing plain text data and stop them from running. But for example, if you have two Word documents open – the first containing important documentation you're working on, and the second a file sent by a friend or colleague – should the second document turn out to be malicious, we'd only want to block that second Word process. We would want to allow the user to continue to remain productive on the first Word document.

Should the user's system become highly infected with one or more pieces of malware that is in the process of being cleaned up, as a last resort, Synchronized Encryption can temporarily revoke the local copies of the encryption keys. Key revocation would ensure that nothing on the system can decrypt any files or data. This does make the end user less productive, because they can't access encrypted data, but this is actually the point. Do you want a user (and the applications/processes they use) to access encrypted data on an infected system? No, you do not. Once the malware infection(s) have been cleared off and the system is given a clean bill of health, the encryption keys are returned to the system and the user can continue working productively.

Is a Non-Trusted Process a Bad Thing?

If a process is not trusted, does that mean that it is bad? No, not necessarily. There are plenty of use cases where you might want a process to access the files but only in an encrypted manner. For example, users can use an email client such as Outlook to send an attachment. The Outlook Client is not trusted, but it can access the files in their encrypted form to perform the attachment and delivery function. But once it reaches its recipient, Outlook then calls on a trusted application such as Word or Excel to open the application. In the end user's eye, the process is completely transparent, while at the same time, the attachments are encrypted and thus protected during the transmission.

This also illustrates why the Sophos Synchronized Encryption concept is different to application white-listing. You might trust the white-listed application to run, but that doesn't mean it should have access to encrypted data. With Synchronized Encryption, you're making a determination as to whether a trusted running application is trusted enough to see the plain text version of encrypted data.

Synchronized Encryption Without Sophos Endpoint

To get the full benefit of Sophos Synchronized Encryption, customers need both Sophos Endpoint and Sophos SafeGuard products. But, what happens to this concept if the Sophos Endpoint product is not present? All of the same logic still holds true; however, the validation of system health and process trust goes from being dynamic to static. The SafeGuard product cannot detect malware, so a different evaluation on system health has to be made. Process trust is then based off something closer to a list of strongly named processes, which the administrator defines as trusted. By default, anything not on that list is not trusted.

Collaboration Options with Next-Gen Encryption

End users need to collaborate, both inside and outside of an organization, in order to perform their day-to-day tasks and be productive. Next-Gen Encryption ensures that all of the data that they have created is protected, and only something that is trusted can access it. So, how does collaboration work now? Again, the focus is to allow users to remain productive and retain their workflows. Let's look into the two categories in a bit more detail.

Collaborating Internally

Collaborating internally is actually the easiest and most seamless experience. All users inside the company have access to the encryption keys. All data that is created is encrypted. It's shared encrypted and everyone can access it.

1. **John creates a Word document and saves it.** He wants to get feedback from Judy. When John saves the document, it is saved and encrypted automatically (encryption by default). John doesn't need to do anything special to encrypt his Word document.
2. **John opens up Outlook and creates a new email,** addressing it to Judy. Using his normal workflow, John attaches the file to the email. He types up his message and presses send. Outlook is a mail client and, generically, isn't trusted. As it is not trusted, it breaks one of the three pillars (not a trusted process). When Outlook reads the Word document to attach it, that file will be attached in an encrypted state.
3. **The email is then sent to Judy,** who receives it and opens the email from John. The file attachment in the email in John's Sent folder is encrypted. The file attachment in the email in Judy's Inbox is encrypted. The file attachment is encrypted while being sent from John to Judy.
4. **Judy double clicks on the Word Document** in the email and it opens seamless in Word, where Judy can now review and make comments. Outlook is not trusted, so when it saves the document to a temporary location it will be in its currently encrypted state. Outlook then launches Word asking it to open the temporary file it has just created. Word is trusted, and has access to the key. Since Judy is trusted, Judy's device is trusted, and MS Word is trusted, it can decrypt the document read and properly present the document in plain text to Judy.

   In addition,if Judy reads this email on a mobile device secured with Sophos Mobile Control, she can save the encrypted attachment to the Secure WorkSpace (and encrypted container), and because this encrypted container shares the same key, she will be able to view the content while keep it secure.

Neither John, nor Judy had to change their standard behavior, and all of their interactions are encrypted. They have a seamless experience and can collaborate together without issues.

Collaborating Externally

Collaborating externally does change when all of your data is encrypted. There are two ways that users can collaborate externally. They are:

1. Password protected (Wrapped in a HTML5 File)
2. Decrypted

Collaborating Externally With a Decrypted File

There are valid use cases for sharing data in a decrypted form. For example, public information, such as a brochure. It's public information that should be accessible to anyone, so it's perfectly fine to have it decrypted. The decryption of data is the one time that Next-Gen Encryption will "get in the face" of the end user. They, the user, need to confirm that they are making the conscious decision to decrypt this file.

A user will make a conscious decision to decrypt the file before it is sent. As discussed above, the file can then, optionally, pass through DLP for examination of the contents and if no flags are raised the file is decrypted. Also, encryption, or in this case decryption, is persistent so it will remain that way. All of this is logged and audited so that an administrator can monitor for malicious employee behavior. Once the file is decrypted, normal user workflow can resume.

Collaborating Externally Using a Password Protected File

What happens if you have a contract that you want to share securely with an external recipient, but you need to allow them to decrypt it and use it without knowing if they have any encryption software installed at all?

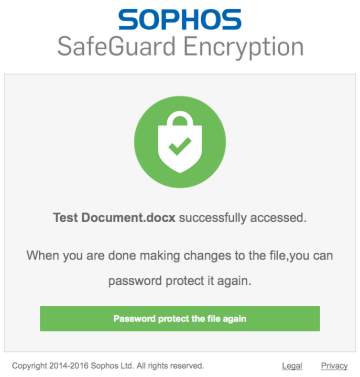
The user can simply create a password protected file and set a password. Essentially, the software re-encrypts the file contract document (let's call it contract.doc) with the password the user assigned, and wraps it into a HTML5 wrapper. This creates a file called contract.html. This password will need to be shared with the recipient. The result is a single HTML file that can be interpreted by any HTML5 capable browser, or any operating system. This single HTML file has three distinct parts:

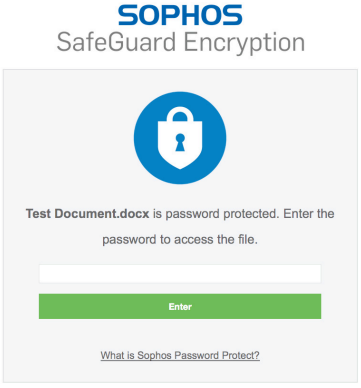
1. The presentation layer (what the recipient will see in their web browser when they open the file)
2. Code to decrypt the attached payload
3. The encrypted file (contract.doc in this example)

The user would then email contact.html to the recipient instead of the contract.doc file. When the recipient double clicks on the HTML file in their email client, it will open their browser and ask them to enter the password. Assuming that they can enter the password correctly, the browser will execute the code to decrypt the file and then it will be saved locally on the recipient's machine in an unencrypted state.

This allows the confidential file to be sent in an encrypted state, then seamlessly decrypted whey the recipient opens the file.

If the recipient needs to send back an updated file, the HTML wrapper can also be used as a container. The recipient can simply update the file and drop the updated file back into the HTML screen. This creating a two-way secure collaboration with an external user who does not have Sophos SafeGuard Encryption.





Making Life Easy for Your Users

To make life easier for your end users, Sophos provides items, such as an Outlook plugin, that can detect that mail is being sent outside the organization with a file attachment. It can then inform the user that he/she is about to send an encrypted file and ask which of the options the user wishes to choose for external collaboration and to take the appropriate steps. Alternatively, an administrator might specify a default action, via policy, that would be automatically performed.

Cross-Platform Data Access

In order to allow end users to remain productive, this Next-Gen Encryption functionality needs to run on all of the devices commonly used by end users. This functionality works on Windows, OS X, iOS and Android.

We talked about users having an average of three devices. If the Windows machine gets highly infected with malware, is locked down, and not trusted, the user can still work and remain productive on either their Mac or iPad, regardless of they are in the office or on the road. If one device is compromised, it's unfortunate, but the user can simply use another device instead.

Next-Gen Threat and Data Protection

With Sophos customers can achieve even better security when they combine Next-Gen Encryption with our broader synchronized security offering. If a customer has Sophos Endpoint, a Sophos UTM/Firewall, and Sophos SafeGuard all three solutions will work together to not only provide a great solution that will detect and remove threats more effectively, but also to ensure that threats cannot access encrypted data. This is next-generation protection for your business.

Conclusion

Next-Gen Encryption changes the paradigm of data protection. Always-on encryption instead of the traditional file/folder encryption takes the burden of deciding what is important and what needs to be encrypted out of end user's hands. As a result, this makes it simpler for the end user, transparently and automatically encrypting/decrypting files without altering their workflow. Synchronized Encryption protects data against threats by revoking keys from infected systems and denying access to untrusted or malicious applications. All of this ensures that the user remains productive while their data – and your organization's – remains secure.

More than 100 million users in 150 countries rely on Sophos as the best protection against complex threats and data loss. Sophos is committed to providing complete security solutions that are simple to deploy, manage, and use that deliver the industry's lowest total cost of ownership. Sophos offers award winning encryption, endpoint security, web, email, mobile, server and network security backed by SophosLabs—a global network of threat intelligence centers. Read more at www.sophos.com/products.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK

2016-10-18 WP-NA (NP)