Adaptive Defense

INFORMATION SENT AND AZURE CERTIFICATIONS

panda

pandasecurity.com

01 What information is sent / saved in the cloud?

02 Is any type of information shared with third parties?

03 Is the information sent encrypted?

04 What security is provided by the platform where the data is stored?

05 What security certifications are provided by the platform where the data resides?

06 Where is the Windows Azure platform located?

01

What information is sent / saved in the cloud?

This section shows the information that is sent to the cloud by Panda Adaptive Defense agents that are installed on each Endpoint to offer full protection guarantee in devices, stations and Windows servers.

The new protection model from Panda Adaptive Defense requires information collected from what applications are doing. The continuous monitoring of the actions performed by the applications and further analysis of this data with machine learning techniques in our environment Big Data, is what allows us to offer guaranteed protection to our clients.

Data collected by the Panda Adaptive Defense follows the following rules:

- Only relative information to Widows executable files is collected, (files .exe, dll, ...) that are executed/loaded in the machine.
- File attributes of those files are sent using standard references instead of user-specific information. That way for example, the file paths are standardized as LOCALAPPDATA\name.exe instead of c: \Users\USERS_NAME\ AppData\Local\ name.exe.
- The collected URLS are only for executable files download. User's navigation URL's are not collected.
- The data collected does not contain personally identifiable information.
- **In no case** Panda Adaptive Defense sends personal information to the cloud.

The following **information is collected from the machines:**

- Equipment name.
- Operating system.
- Service Pack.
- Group in which the protected PC is included.
- Default IP address of the machine.
- MAC address.
- Assigned IP addresses to the different web adapters.
- MAC addresses for the different web adapters.
- RAM memory in MB.

About the actions that applications take in the system

As essential information to support the new protection model of the Panda Adaptive Defense, **information** is sent **about the actions that applications take** in the system.

Attribute	Data	Description	Example
File	Hash	File hash referred by the event	N/A
URL	Url	Address from where a PE has been downloaded	http://www.malware.com/executable.exe
Path	Path	Standardized path where the event's referenced file is located	APPDATA\
Register	Key / Value	Windows register key and related content	HKEY_LOCAL_MACHINE\SOFTWARE\Panda Security\Panda Research\Minerva\Version = 3.2.21
Operation	Operation ID	Operation ID of the event performed (creation/modification/upload/... of executable, executable download, communication, etc.)	Event type 0 indicates the execution of a PE
Communication	Protocol/Port/Address	Collects a process communication event (not its content) along with its protocol and address	Malware.exe sends data UDP on port 4865
Software	Installed Software	Collects the software listing installed in the Endpoint in accordance with Windows API	Office 2007, Firefox 25, IBM Client Access 1.0

Additionally, it may be necessary to send executable files to our **Collective intelligence platform**. To reduce bandwidth use, in case they are not already present, only executable files are sent to the Collective Intelligence platform.

By sending only executable files, we ensure that in no event they will contain user/client confidential information.

02

Is any tipe of information shared with third parties?

All of the working information is exclusively stored in our Windows Azure cloud platform.

The information is not shared with third parties except when our clients:

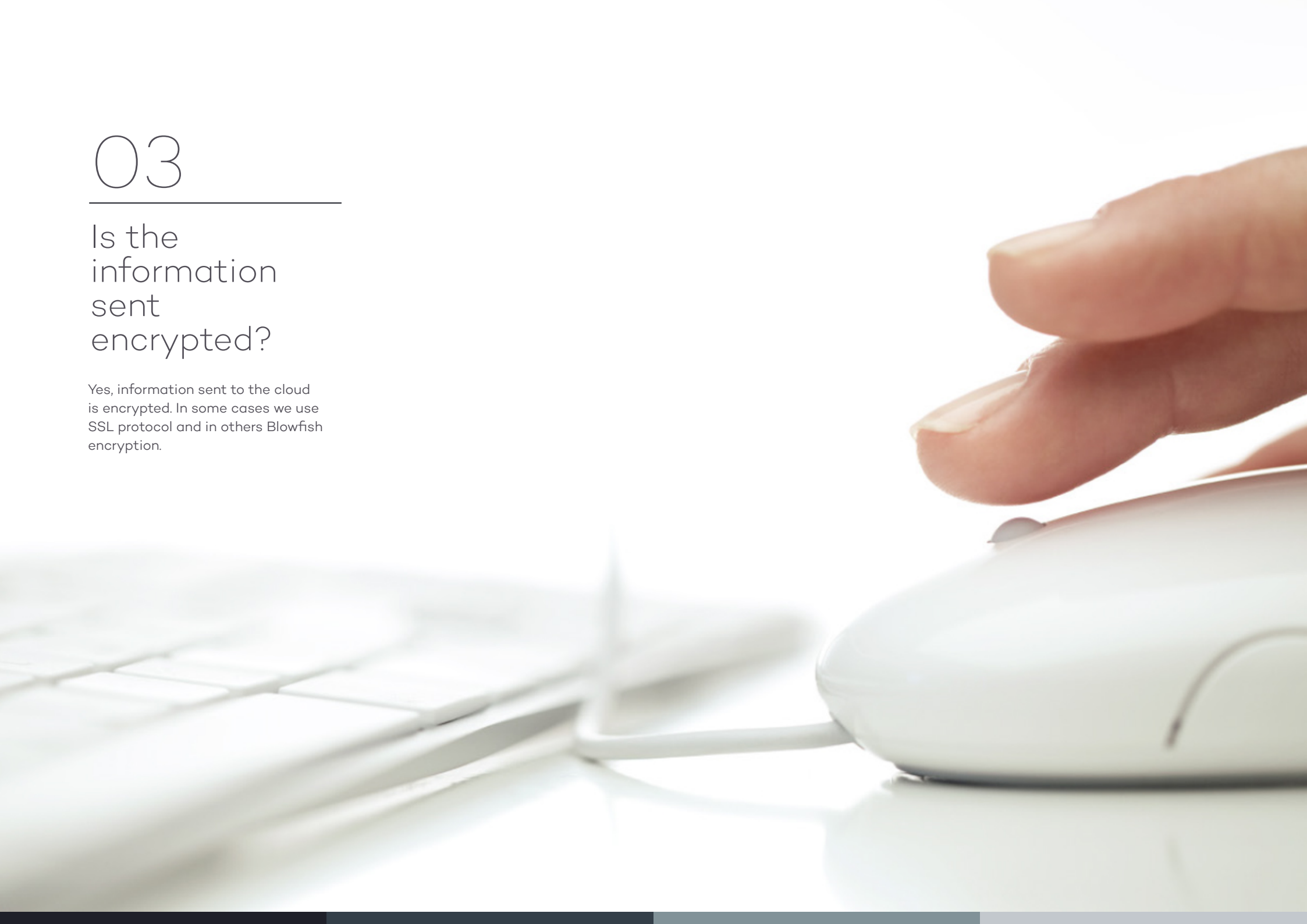
- Desire to receive information in their **SIEM** system about alerts and security data that is collected by Panda Adaptive Defense. Security information collected by Panda Adaptive Defense will be sent to client's SIEM by a secured protocol agreed by the client.

- Use the **Logtrust** platform, the SIEM that Panda Adpative Defense integrates by default. Logtrust is a cloud Big Data platform that stores in real time the data about the collected evidence in all stations protected by Panda Adpative Defense. The information is sent to Logtrust using HTTPS and stored in Logtrust CPD's.

03

Is the information sent encrypted?

Yes, information sent to the cloud is encrypted. In some cases we use SSL protocol and in others Blowfish encryption.



04

What security is provided by the platform where the data is stored?

Windows Azure, the platform where Panda Adpative Defense resides, provides maximum protection and confidentiality of the stored data. The security and control policies established in Azure are described in the Whitepater “Windows Azure Security Overview.”

Windows Azure Security Overview

WHAT SECURITY IS PROVIDED BY THE PLATFORM IN WHICH LOGTRUST RESIDES?

Logtrust uses Amazon Web Services and benefits from the physical security measures of the Amazon data centers.

For more information, refer to the following documentation:

AWS Compliance

Access to the Logtrust systems is always filtered by Firewall and protected with certificate-based authentication. In addition, all the systems, services and applications that compose the cloud infrastructure report their logs for audit and security purposes.

05

What security certifications are provided by the platform where the data resides?

As indicated in the PDF in the previous section, Windows Azure operates in the Microsoft Global Foundation Services (GFS) infrastructure.

The following document provides information about the security management provided by Global Foundation Services (GFS), the Microsoft Cloud infrastructure in which Windows Azure operates:

Microsoft's cloud services

Windows Azure certifications are indicated in the PDF:

- **ISO/IEC 27001:2005**
- Statement on Auditing Standards No. 70 **(SAS 70)** Type I and II
- Sarbanes-Oxley **(SOX)**
- Payment Card Industry Data Security Standard **(PCI DSS)**
- Federal Information Security Management Act **(FISMA)**

Additionally, we have detailed information about the 27001 certification in:

Windows Azure Achieves ISO 27001

Last, indicate that in:

Details

there is a Whitepaper that describes how Windows Azure complies with the security requirements defined by Cloud Security Alliance, Cloud Control Matrix. Attached is the paragraph from the Whitepaper:

"Our security framework based on ISO 27001 enables customers to evaluate how Microsoft meets or exceeds the security standards and implementation guidelines. ISO 27001 defines how to implement, monitor, maintain, and continually improve the Information Security Management System (ISMS). In addition, the GFS infrastructure undergoes an annual American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) No. 70 audits, which will be replaced with an AICPA Statement on Standards for Attestation Engagements (SSAE) No. 16 audit and an International Standards for Assurance Engagements (ISAE) No. 3402 audit. Planning for an SSAE 16 audit of Windows Azure is underway"

SECURITY CERTIFICATIONS OF THE PLATFORM WHERE LOGTRUST DATA RESIDES

For those clients that are going to use the Logtrust service, should know that they count with the physical security measures of Amazon's CPD.

Windows Azure Security Overview

As you can see in detail in the previous link, Amazon counts with all the main certifications for the market highlighting:

- **ISO/IEC 27001**
- SOC 1/SSAE 16/ISAE 3402 **(previously, SAS70)**
- Payment Card Industry Data Security Standard **(PCI DSS)**
- Federal Information Security Management Act **(FISMA)**

06

Where is the Windows Azure platform located?

Windows Azure has nodes in different locations around the world. At the present time, Panda Security data center is located in Ireland.

Below is the picture of the datacenter in Ireland.

WHERE IS AMAZON'S LOGTRUST PLATFORM LOCATED?

Logtrust operates on high availability through its Amazon platforms located in its datacenter in Ireland.


panda