SNOWWALL

A VISUAL FIREWALL FOR THE SURVEILLANCE SOCIETY

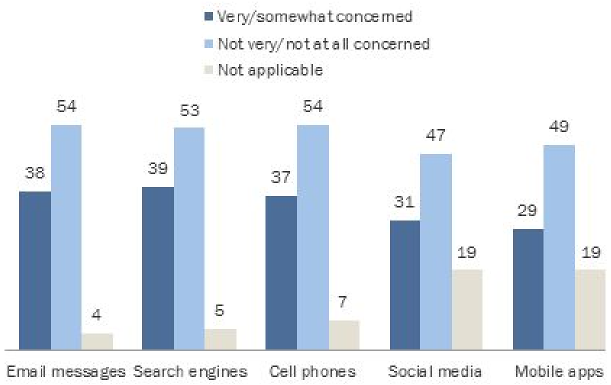
MOTIVATION

> *“We will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary.”*

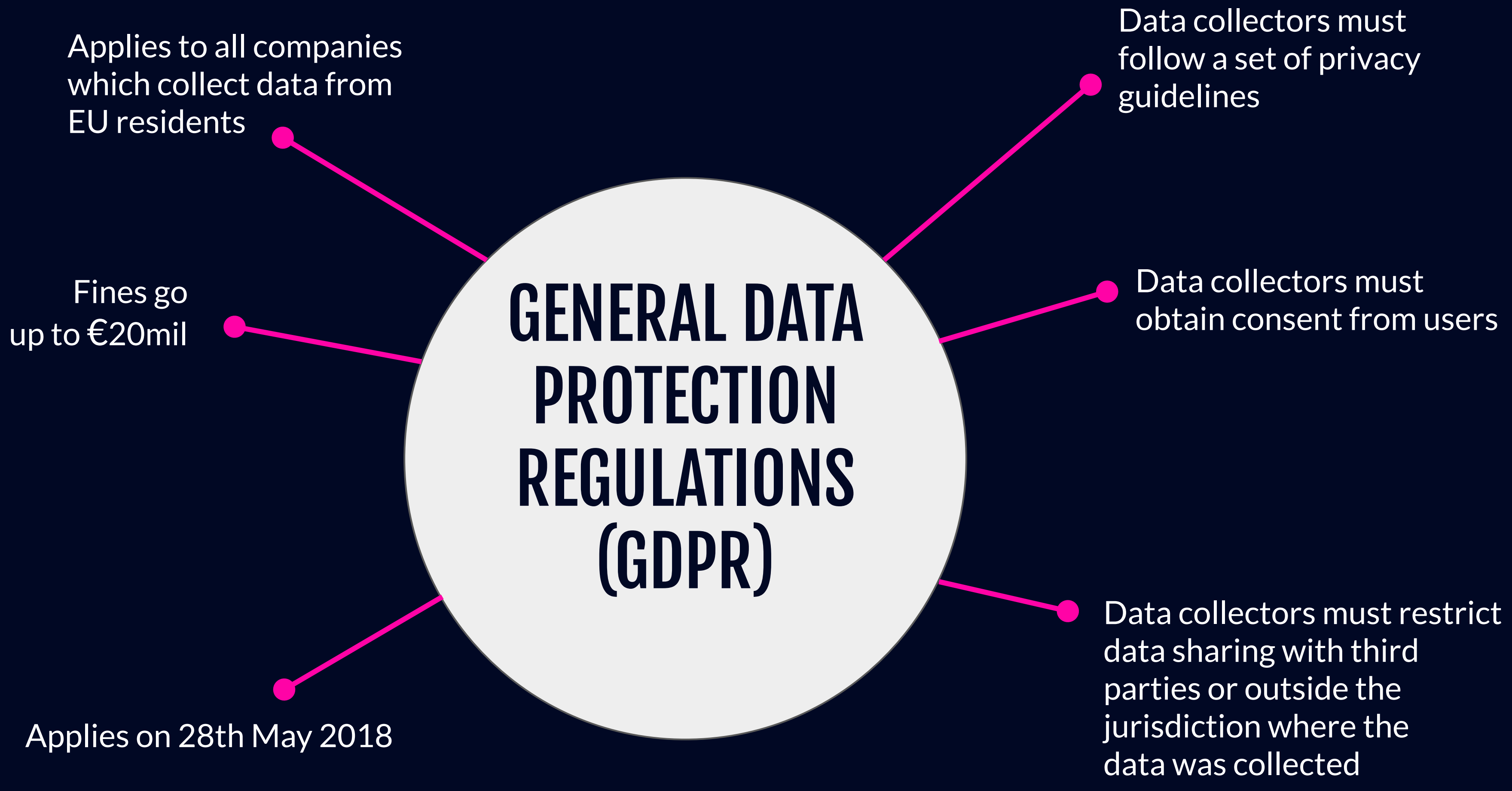
Microsoft Privacy Statement

THE CONTEXT

- Data collection is necessary for providing seamless technological experiences
- Users don’t always have control over what data they are sharing
- Companies are at risk to leak or share collected data, to implement inadequate anonymisation or get hacked
- Governmental surveillance acts through the technology we use
- People are not aware of the big picture
- People don’t care



Survey shows less than half of Americans are “very or somewhat concerned” about the government surveillance of their electronic communications and personal data.
© Pew Research Center, 2015



GENERAL DATA PROTECTION REGULATIONS (GDPR)

Applies to all companies which collect data from EU residents

Fines go up to €20mil

Applies on 28th May 2018

Data collectors must follow a set of privacy guidelines

Data collectors must obtain consent from users

Data collectors must restrict data sharing with third parties or outside the jurisdiction where the data was collected

THE PROBLEM

- 80% people in the world use Windows
- Windows 10: Software as a Service
- Microsoft gives itself the right to collect telemetry data and share it with third parties
- Users complain about personalised ads and throttled bandwidth
- Monitoring or controlling what data is collected is very hard and tedious work
- Microsoft started collecting telemetry from Windows 7 and 8.1 too!
- You can configure some of the data you are sharing, but there is no means to inspect where your data is being sent

THE IDEA

- Windows Firewall: secure, resilient, low-level, could have stopped many attacks if properly configured
- To stop WannaCry it was enough to block TCP port 445
- But creating firewall rules is hard and requires 7 steps!

- **Can we provide a better, simpler way for users to control and filter their network connections?**
- **But how can users know what to look for?**

THE OBJECTIVES

- a monitor for network traffic, bandwidth and process activity in **real-time**
- accurate and comprehensive real-time visualisations of the monitored activity, including information about the **destination** of network traffic
- a mechanism which can filter network traffic according to different dimensions, such as by destination **country**, **organization**, or originating **application**
- easy access to creating and scheduling firewall rules required for these policies

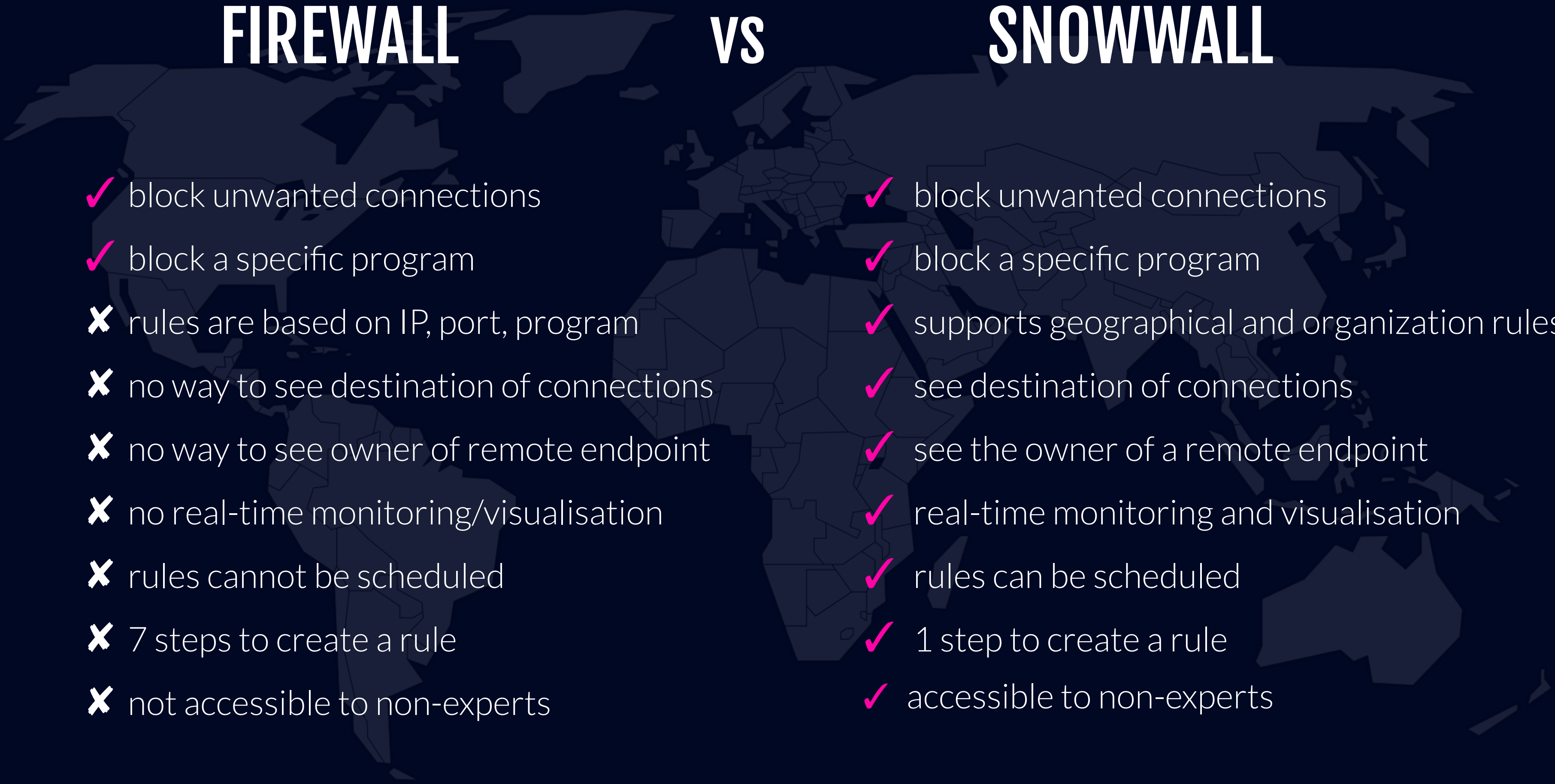
THE SOLUTION?

SNOWWALL

A VISUAL FIREWALL FOR THE SURVEILLANCE SOCIETY

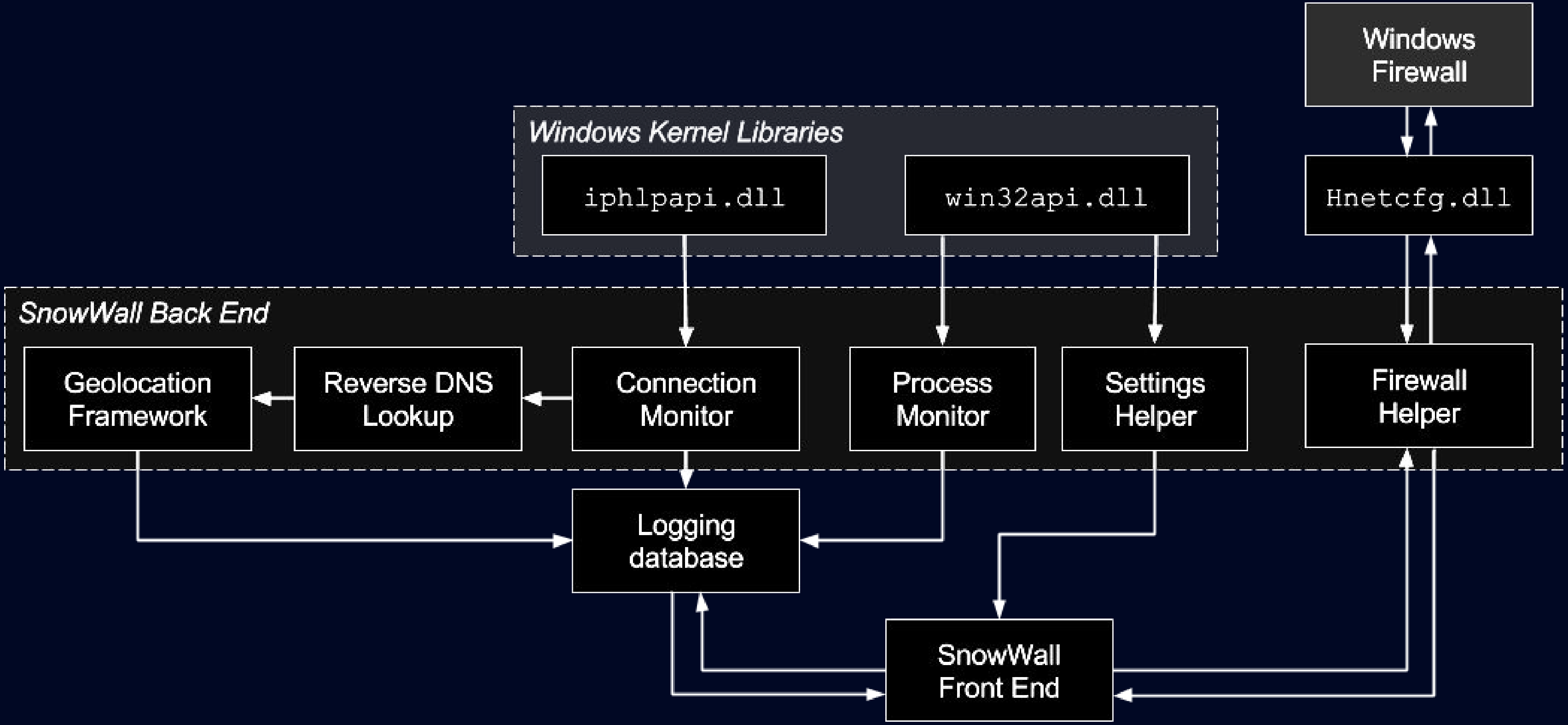
WHAT IS SNOWWALL?

1. **Monitoring**: A monitor for network traffic, bandwidth and process activity in real-time
2. **Visualisations**: A provider of accurate and comprehensive visualisations of the monitored activity, based on **geography** and **organization**
3. **Filtering**: A mechanism which can filter network traffic according to different dimensions, such as by destination country, organization, or originating application; easy access to creating and scheduling firewall rules required for these policies
4. **Control**: A means of creating high-level policies for entire networks



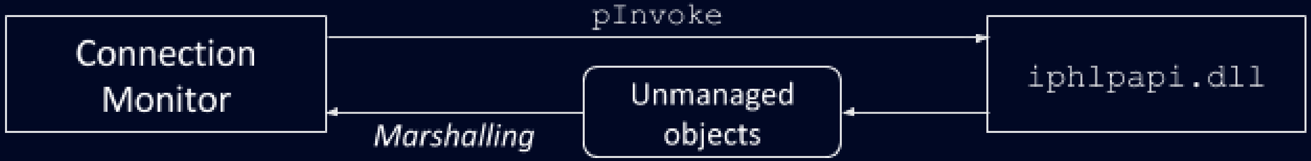
FIREWALL	VS	SNOWWALL
✓ block unwanted connections		✓ block unwanted connections
✓ block a specific program		✓ block a specific program
✗ rules are based on IP, port, program		✓ supports geographical and organization rules
✗ no way to see destination of connections		✓ see destination of connections
✗ no way to see owner of remote endpoint		✓ see the owner of a remote endpoint
✗ no real-time monitoring/visualisation		✓ real-time monitoring and visualisation
✗ rules cannot be scheduled		✓ rules can be scheduled
✗ 7 steps to create a rule		✓ 1 step to create a rule
✗ not accessible to non-experts		✓ accessible to non-experts

ARCHITECTURE



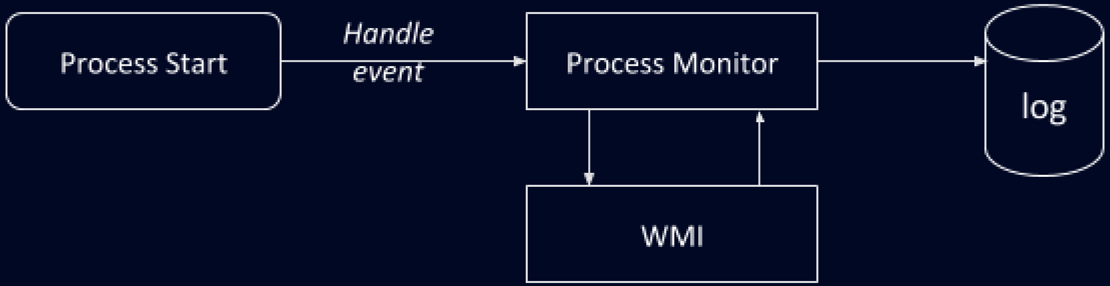
MONITORING CONNECTIONS

- interface with **IPHelperAPI.dll** via **pInvoke** to retrieve list of active connections
- unmanaged data in byte buffers is marshalled into managed objects containing information of a connection's **creation time**, **state**, **owning process**, remote **IP address**, local and remote **ports**, and bandwidth statistics
- poll for connections every second to catch changes of state



MONITORING PROCESSES

- ➔ Windows provides Management Instrumentation (WMI) which gives developers access to the functions of the operating system
- ➔ **Win32API.dll** contains unmanaged functions to interfere with the Windows Kernel
- ➔ add a handle to each process start or stop event
- ➔ use the Win32API.dll to figure out if process is 32 or 64-bit
- ➔ use the Windows Management Instrumentation to query information about the process



FIREWALL CONTROL

- ➔ Windows provides an interface to control the firewall in **Hnetcfg.dll**
- ➔ Implemented a firewall monitor which calls the Firewall API
- ➔ High-level firewall rules such as blocking a specific country are automatically generated and added to the Windows Firewall

CASE STUDIES

3
OPERATING SYSTEMS

6
SOFTWARE PRODUCTS

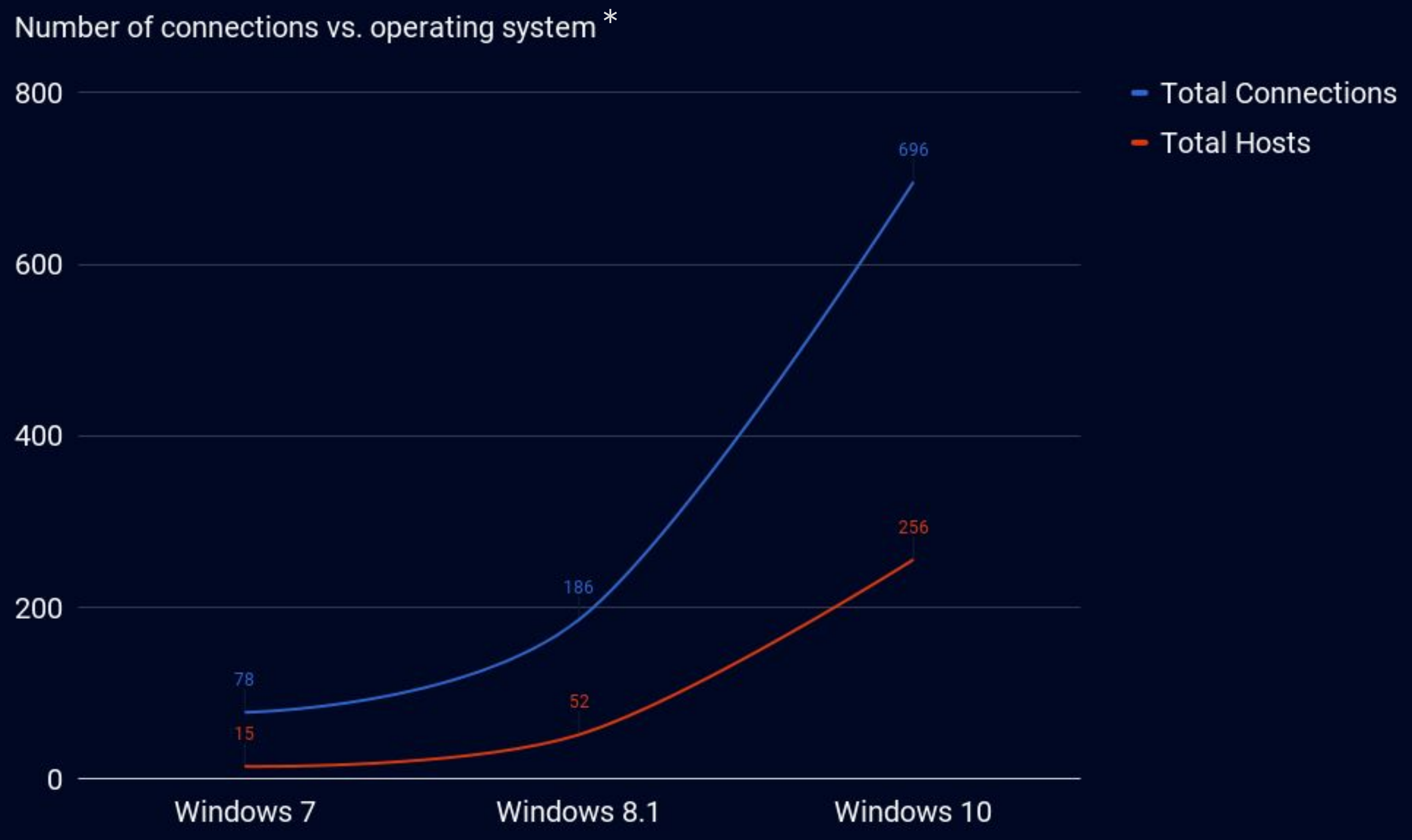
2K
MONITORED CONNECTIONS

EXPERIMENTAL SETUP

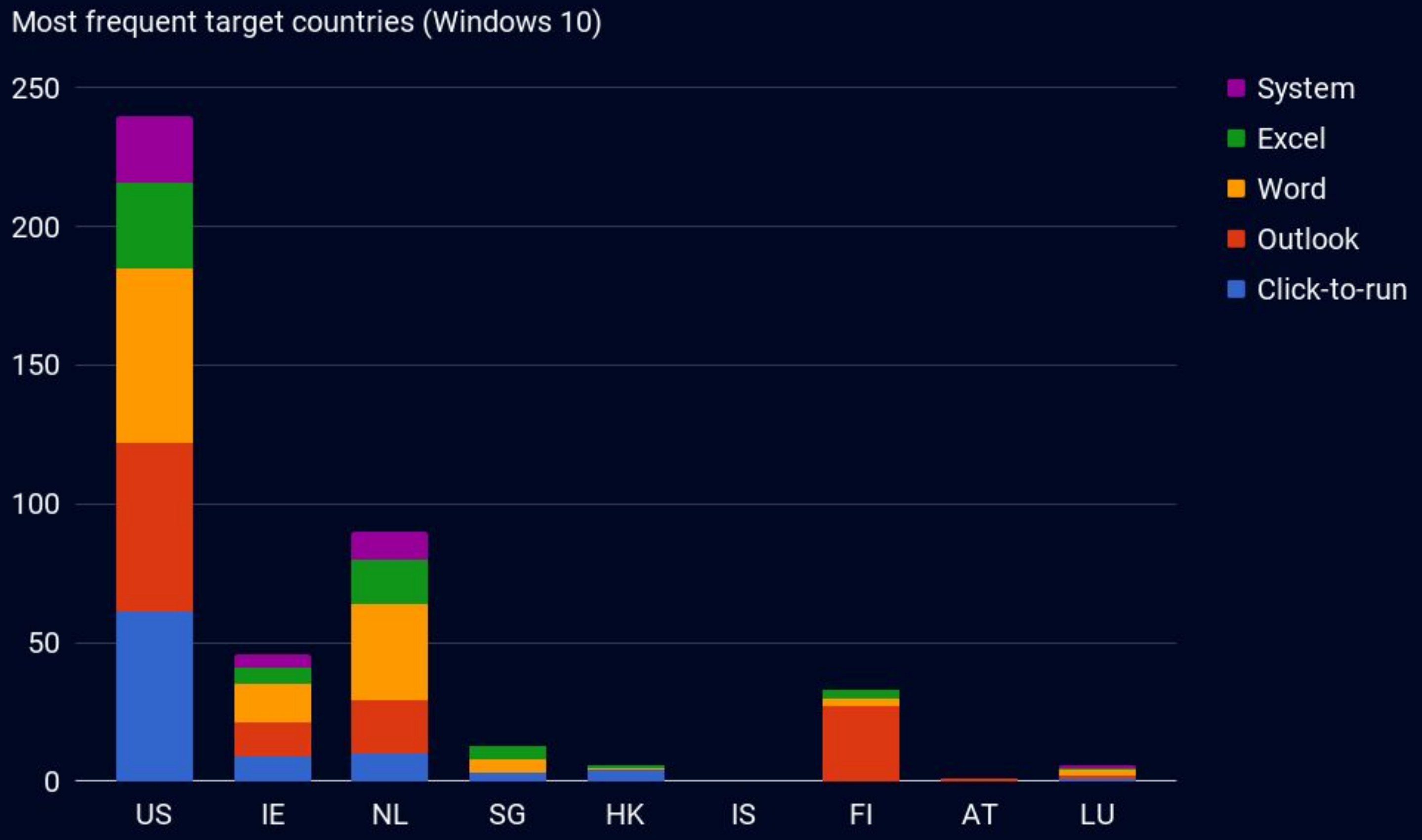
- Windows 7 Professional and Windows 8.1 Professional, out-of-the-box installs on VMs
- Microsoft Surface with Windows 10 Education
- Each tested software product is used for 5 minutes, while SnowWall monitors the connection and process activity
- One test involves simply navigating the file system and using search

RESULTS

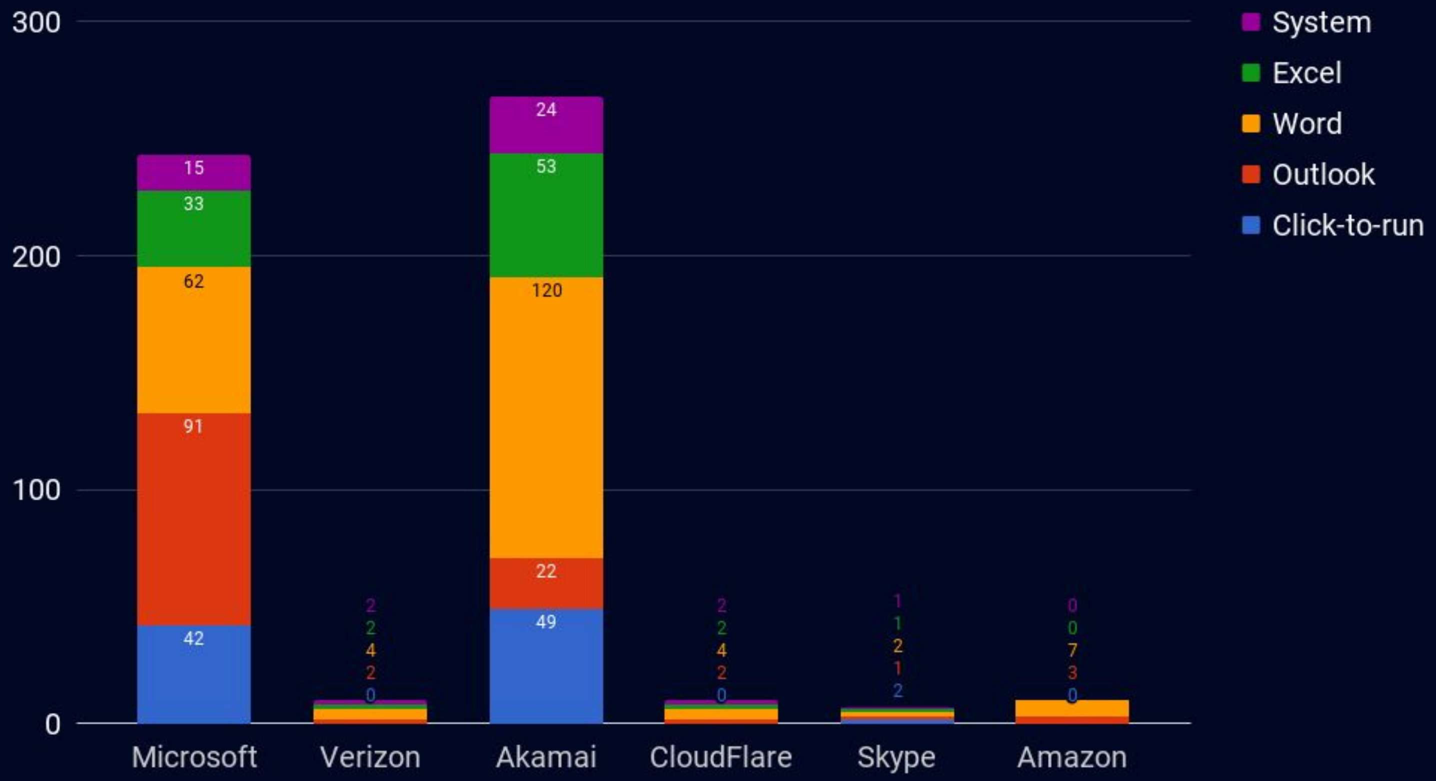
- We can observe exponential trends in the number of connections with newer versions
- Unlike previously thought, Windows 7 machines also send telemetry data
- Most data is sent to Microsoft in the US, the Netherlands and Ireland
- We have evaluated a browser in order to get an insight of how large is the problem of operating system tracking compared to browser tracking – the browser on its own opens hundreds of connections in 5 minutes of usage
- Unlike connections open by the browser, which appear to close on exit, many connections open by offline programs such as Word persist even after closing the program



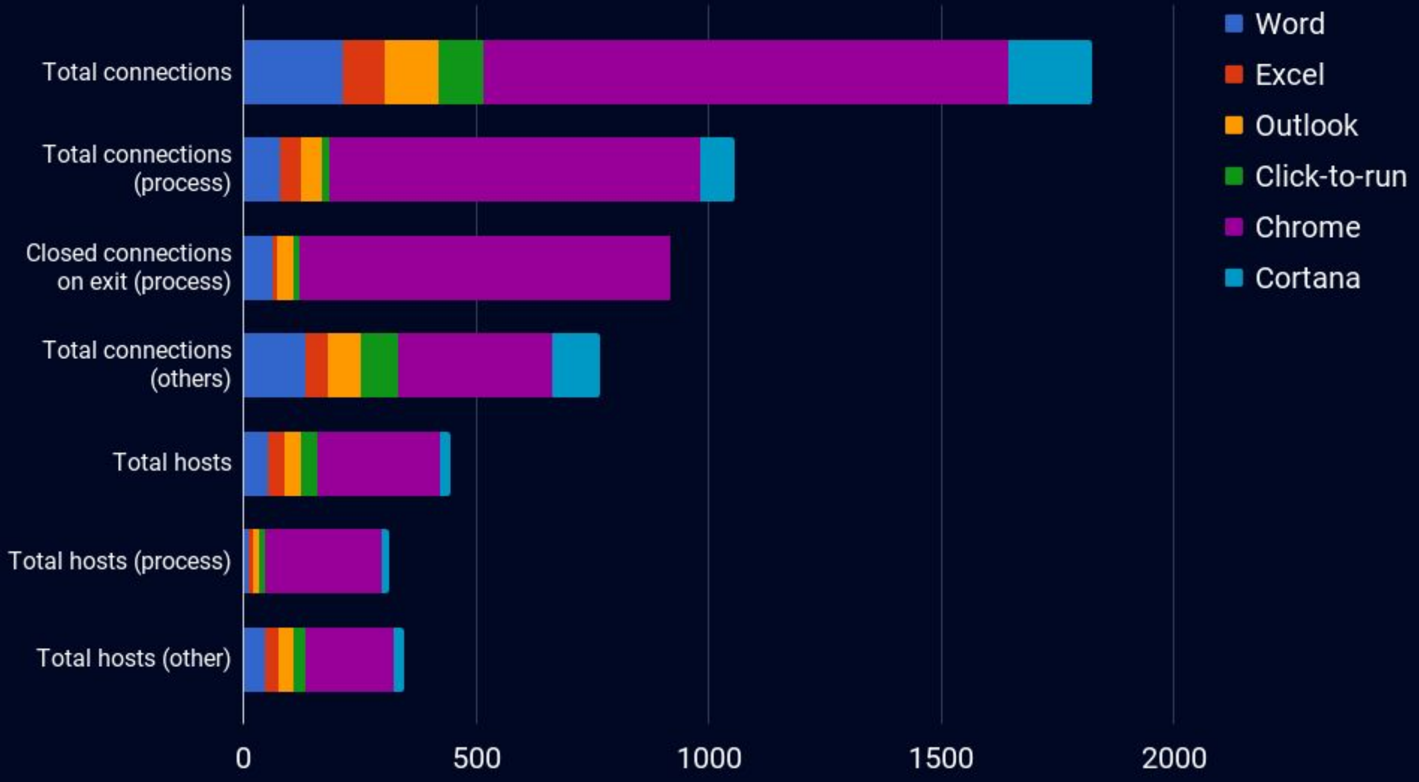
*the plot does not consider the connections opened by Chrome


Most frequent target countries (Windows 10)
250
200
150
100
50
0
US
IE
NL
SG
HK
IS
FI
AT
LU
System
Excel
Word
Outlook
Click-to-run

Most frequent target organizations (Windows 10)



Total Connections (Windows 10)


Total connections
Total connections (process)
Closed connections on exit (process)
Total connections (others)
Total hosts
Total hosts (process)
Total hosts (other)
Word
Excel
Outlook
Click-to-run
Chrome
Cortana