The New Windows Monitoring - One Year Later
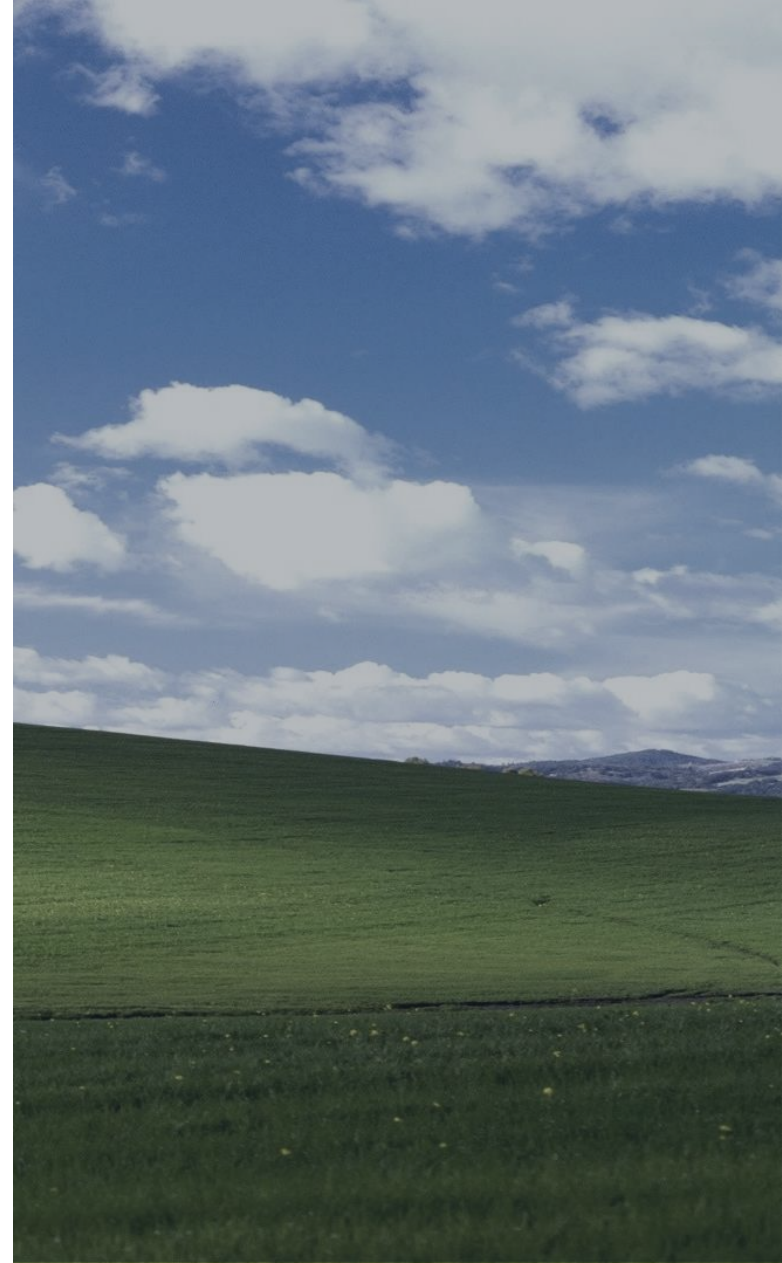
Marcel Arentz
Product Manager
tribe29

Sergey Kipnis
Developer
tribe29

tribe29

Agenda

1. LESSONS LEARNT SINCE RELEASE

2. NEW FEATURES FOR WINDOWS AGENT 1.7

3. WINDOWS ROADMAP AFTER 1.7

tribe29

Smooth first months in operation

TICKETS — Less than 80 support tickets since launch

WERKS — Less than 10 bug fixes required

TYPICAL ISSUES

- Migrating from 1.5 to 1.6
- Architecture changes in 1.6
- Agent Updater vs. AV scanner

tribe**29**

Uncertainties with migration from windows agents 1.5 to 1.6

⚡ Typical questions

- Why is the new agent not replacing the old?

- When should I remove the old agent?

- Why are not all files of the old agent deleted?

Installation procedure of the agent has mostly not changed…

…however the removal of the old agent is different

tribe**29**

Best practice for windows agent update

| **1** Install new agent | Remove old agent | Update firewall | Check files & folders |
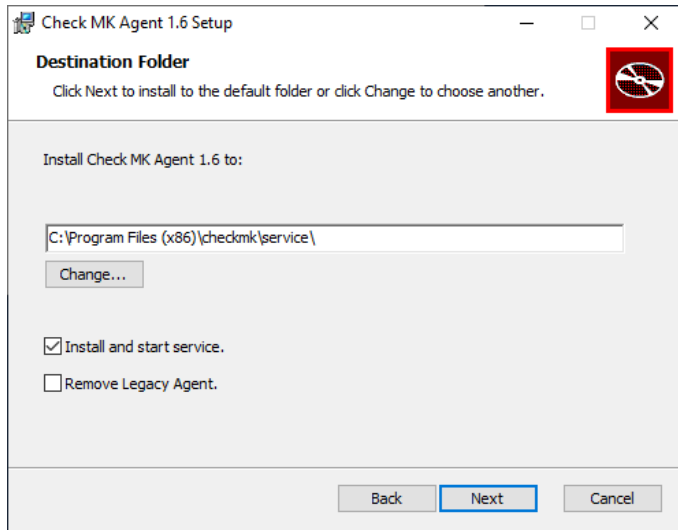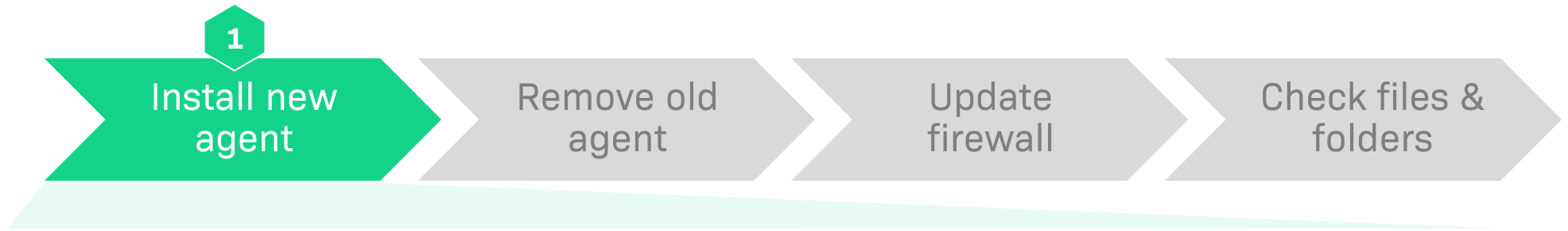
- Install new agent either…
    - …execute MSI file
    - …bake and sign agents after update of Checkmk server
- Legacy agent will not be removed by default – however disabled
- Preserve old agent in case something goes wrong

tribe**29**

Best practice for windows agent update

```
      ┌─────────┐
      │    2    │
Install new  Remove old  Update      Check files &
  agent       agent      firewall      folders
```

Install Check MK Agent 1.6 to:

C:\Program Files (x86)\checkmk\service\

Change...

☑ Install and start service.

☐ Remove Legacy Agent.

▼ WINDOWS MODULES
Install Python runtime environment 0

▼ LEGACY AGENT MANAGEMENT
      ☒ Uninstall the Legacy Agent after installation of the Windows Agent 1.6
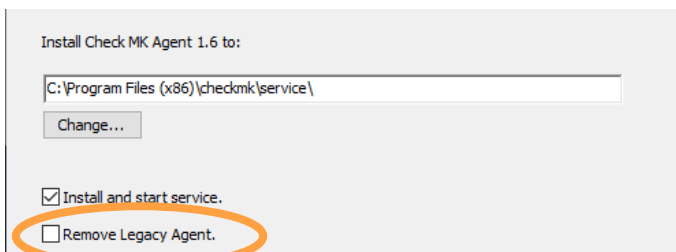
- Remove the old agent once you tested and/or productive system for some hosts work well

- Either…

  - …execute the uninstaller

  - …use automatic removal by enabling checkbox in the installer (e.g. for the rollout to remaining hosts)

  - …use automatic removal by creating a rule in 'Legacy Agent Management'

tribe29

Best practice for windows agent update

Install new agent	Remove old agent	**3** Update firewall	Check files & folders
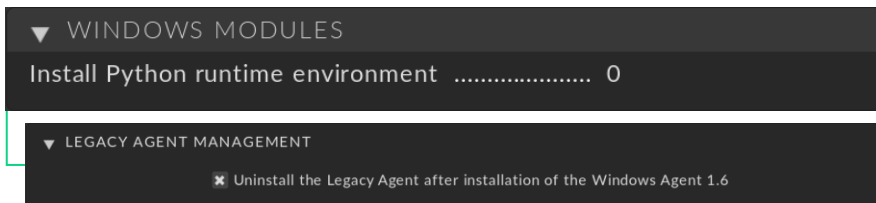
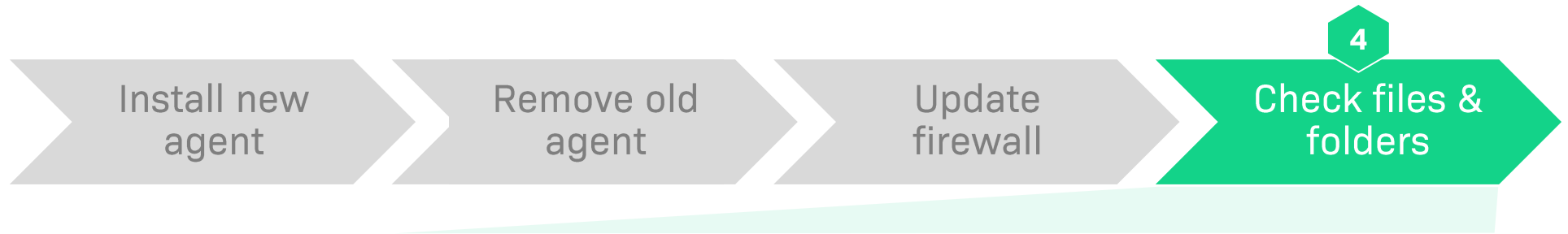- Adjust manually set firewall rules if needed:

New firewall

```
C:\Windows\System32> netsh advfirewall firewall add rule name="Check_MK" ^
More?   description="Monitoring" dir=in localport=6556 protocol=tcp action=allow ^
More?   program="%ProgramFiles(x86)%\checkmk\service\check_mk_agent.exe" ^
More?   profile=private,domain enable=yes
OK.
```

Adjust firewall

```
C:\Windows\System32> netsh advfirewall firewall set rule name="Check_MK" ^
More?   new program="%ProgramFiles(x86)%\checkmk\service\check_mk_agent.exe"

Updated 1 rule(s).
Ok.
```

tribe**29**

Best practice for windows agent update

Install new agent	Remove old agent	Update firewall	**4** Check files & folders

- Manually added files in the old agent folder will remain (together with the folder) after the removal of the old agent

- Common behavior (of all operating systems) so that you need to remove unwanted files manually

More details to architecture difference on following slides

All information can also be found in our handbook:

Chapter 4.3

tribe**29**

Architecture changes from 1.5 to 1.6

⬡ Typical questions

- What is the difference between old and new agent?

- Where do I add my custom configuration options?

- How do I specify which plugins to execute?

- Where do I store the configuration for my plugins?

- What is the new folder 'C:\ProgramData\checkmk\agent'?

tribe**29**

Differences between 1.5 and 1.6

Topics	Version 1.5	Version 1.6
1 Agent & folders	Old agent not following Windows best practices	Files and folders differentiated

Version 1.5

Old agent not following Windows best practices

- Program and user files in same folder

- No transparency on which files have been shipped with the software and which have been added later

- All files: 'C:\Program Files (x86)\check_mk'

Version 1.6

Files and folders differentiated

- Application files shipped with installer: 'C:\Program Files (x86)\Checkmk\service\'

- Custom configurations, log files of the agent itself, plugins to execute: 'C:\ProgramData\checkmk\agent\'

tribe**29**

Differences between 1.5 and 1.6

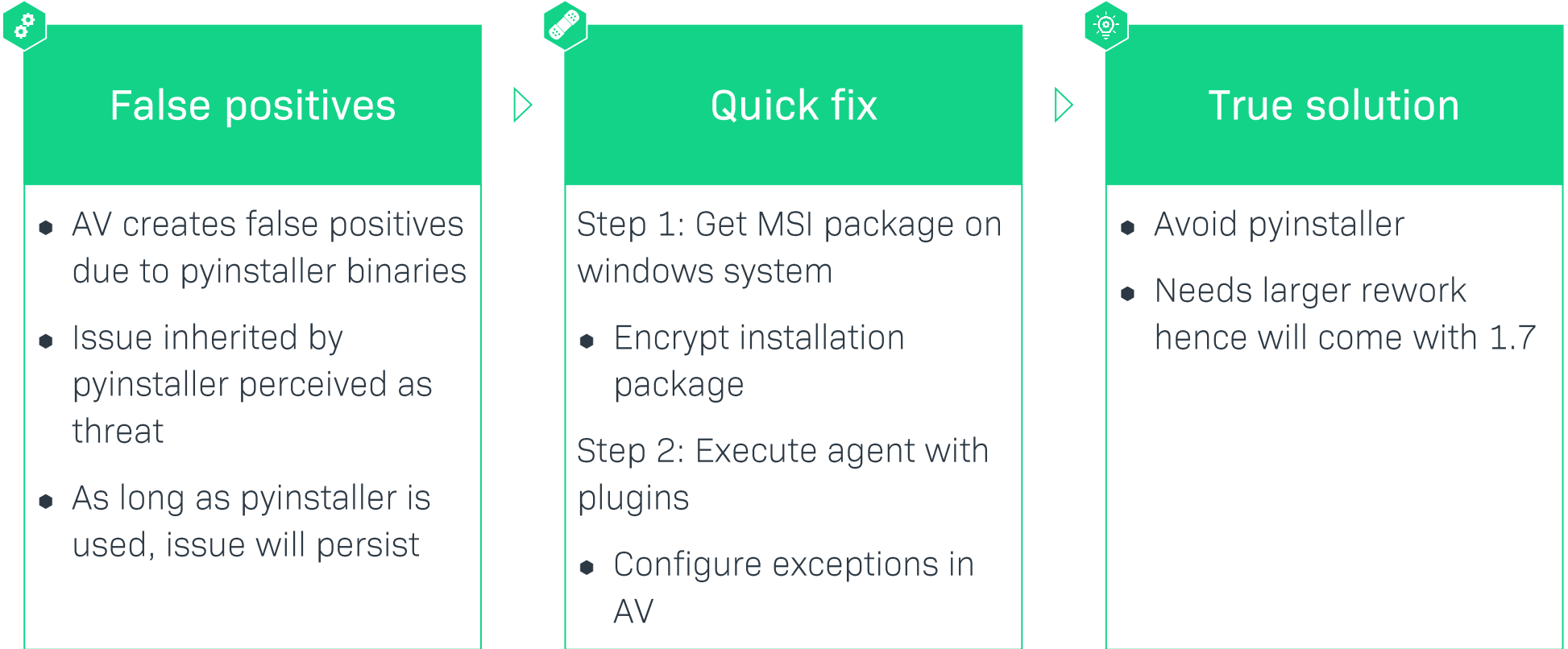| Topics	Version 1.5	Version 1.6

2 Config file format	• Format ini
	   • check_mk.ini
	   • check_mk.local.ini
	 • Relatively flat structure
	 • Ease to use for simple configurations
		• Format yaml
		   • check_mk.yml
		   • check_mk.bakery.yml
		   • check_mk.user.yml
		 • Also classical key-value pair to configure your agent
		 • Easier to use if you want to handle structured data (e.g. complex configurations)

tribe**29**

Differences between 1.5 and 1.6

Topics	Version 1.5	Version 1.6
3 Plugins	• Manually download each plugin from Checkmk server into plugins folder • Configuration of plugin execution with several independent keys • No distinction between bakery and default configuration; user configuration not well known	• Plugins executed by default saved in 'C:\ProgramData\checkmk\agent\plugins\' • No need to download plugins from Checkmk server anymore • Simply copy plugin from application folder to 'ProgramData' folder

Planned: Enhance result page of installer, include read me.txt

All information can also be found in our handbook:

Chapter 3, 6 & 7

tribe**29**

Agent Updater vs. Anti Virus scanner

False positives

- AV creates false positives due to pyinstaller binaries
- Issue inherited by pyinstaller perceived as threat
- As long as pyinstaller is used, issue will persist

Quick fix

Step 1: Get MSI package on windows system

- Encrypt installation package

Step 2: Execute agent with plugins

- Configure exceptions in AV

True solution

- Avoid pyinstaller
- Needs larger rework hence will come with 1.7
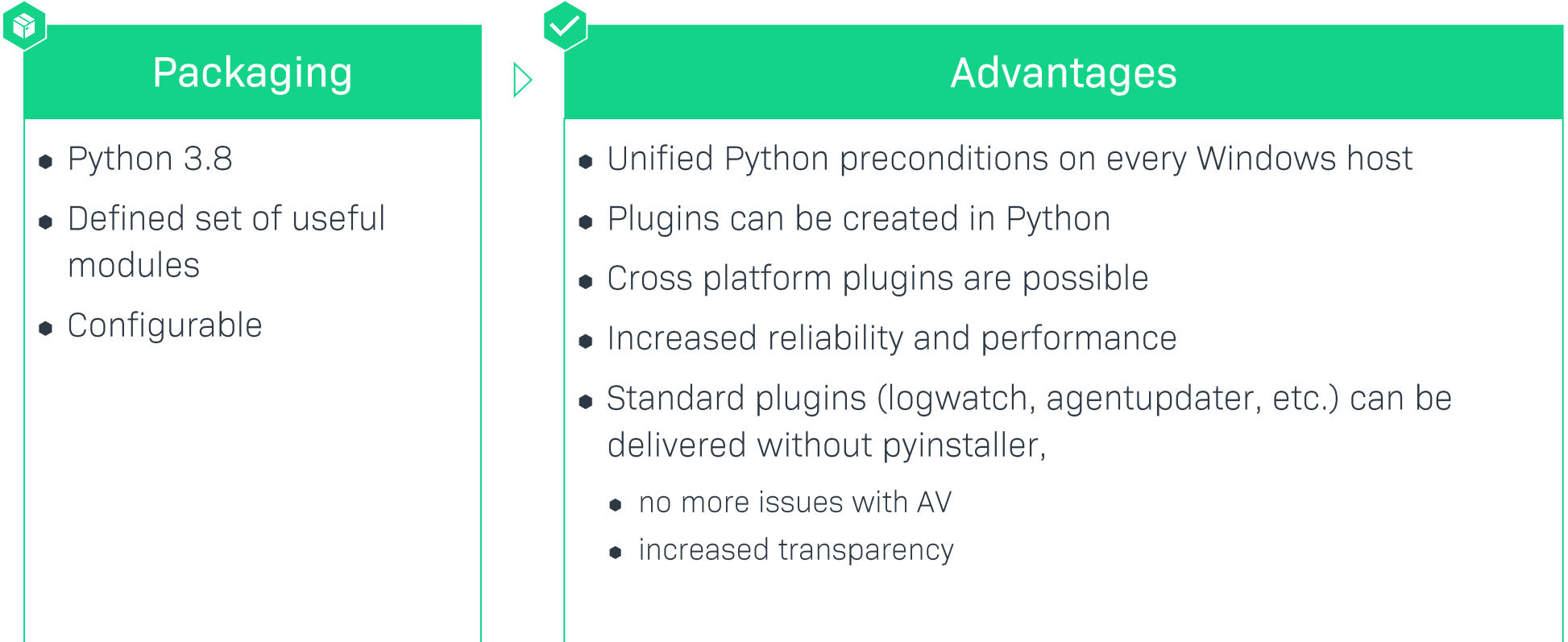
tribe29

Agenda

1. LESSONS LEARNT SINCE RELEASE

2. **NEW FEATURES FOR WINDOWS AGENT 1.7**

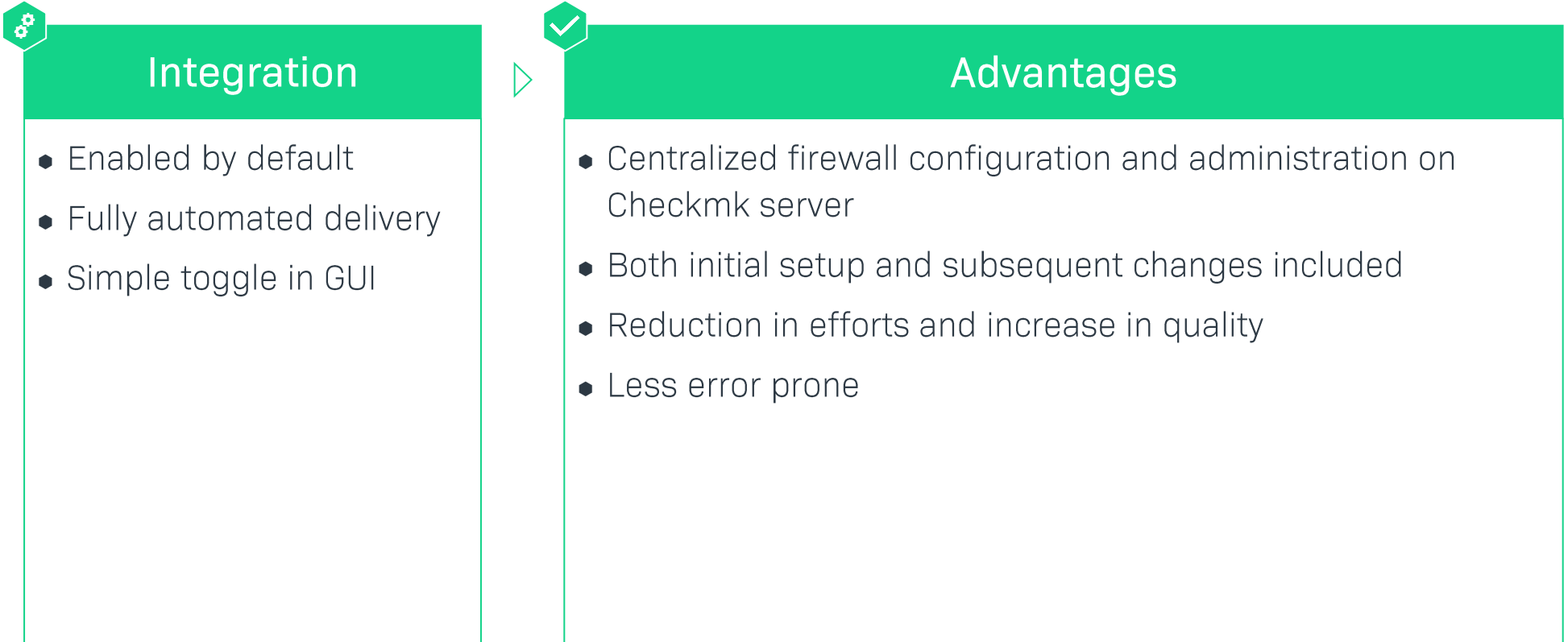3. WINDOWS ROADMAP AFTER 1.7

tribe**29**
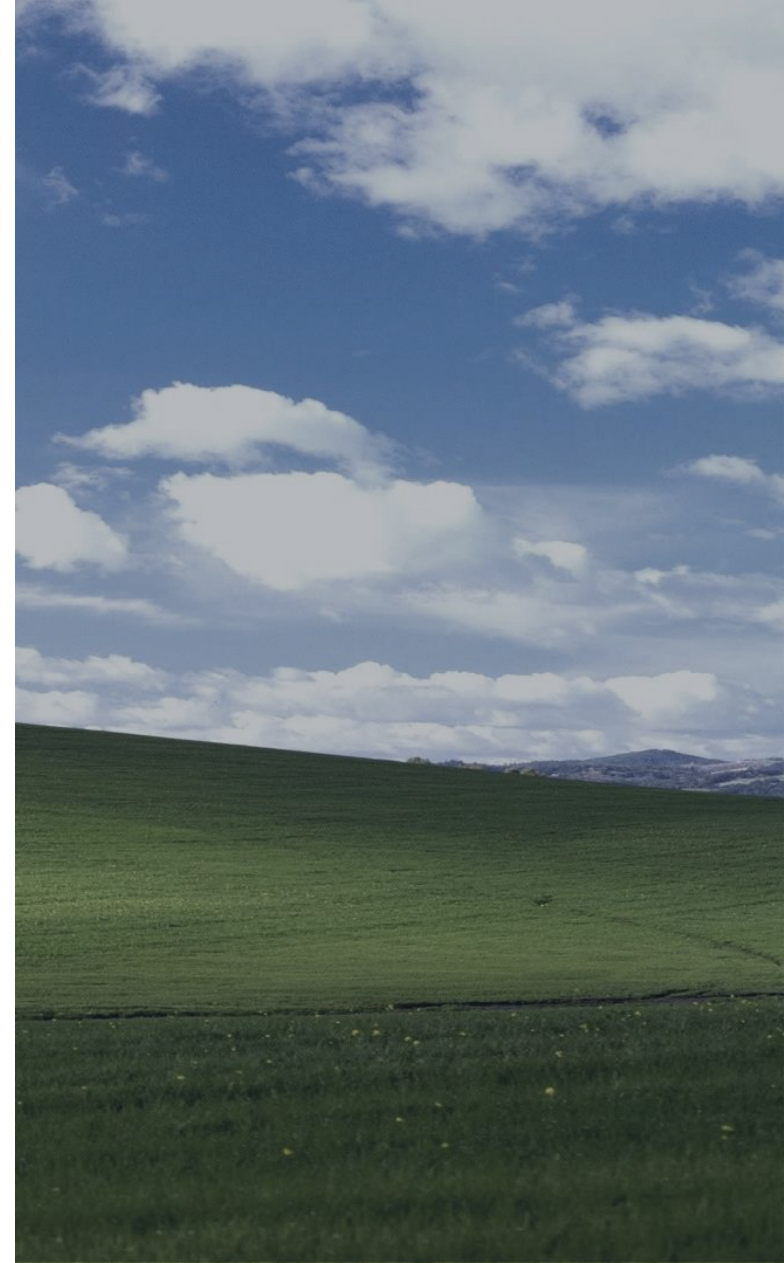
New Features for Windows agent 1.7

Native Python plug-in support

Automatic firewall configuration

Execute plugins with specific permission

Control removal of agent

tribe**29**

Native Python plug-in support

Packaging

- Python 3.8
- Defined set of useful modules
- Configurable

Advantages

- Unified Python preconditions on every Windows host
- Plugins can be created in Python
- Cross platform plugins are possible
- Increased reliability and performance
- Standard plugins (logwatch, agentupdater, etc.) can be delivered without pyinstaller,
  - no more issues with AV
  - increased transparency

tribe**29**

Automatic firewall configuration

Integration

- Enabled by default
- Fully automated delivery
- Simple toggle in GUI

Advantages

- Centralized firewall configuration and administration on Checkmk server
- Both initial setup and subsequent changes included
- Reduction in efforts and increase in quality
- Less error prone

tribe**29**

Execute plugins with specific permission

Specific permission

- Define user group to obtain specific permissions
- Alternatively specify required credentials
- Fully automated execution

Groups

- No credentials in config files on Checkmk server and host
- Definition of correct user group is sufficient
- ActiveDirectory not supported

Specific

- No limitation for specific permissions, e.g. ActiveDirectory is supported
- Credentials in plain text in Checkmk and host

tribe29

Control removal of agent

Deinstallation

- Remove own files per default – „smart clear"

- Simple toggle in GUI for full removal or full preservation

- Fully automated execution

Advantages

- Full control over agent / removal behavior

- Clean status / installation

- User files can be preserved or fully removed if wanted

tribe**29**

Agenda

1. LESSONS LEARNT SINCE RELEASE

2. NEW FEATURES FOR WINDOWS AGENT 1.7

3. **WINDOWS ROADMAP AFTER 1.7**

tribe29

Focus on Windows Application Monitoring

Windows Application Monitoring

New applications

- Microsoft 365
- IIS
- …

Improvements

- Exchange
- Hyper-V
- …

Cross Platform Monitoring

New

- Db2
- mongoDB
- SAP (maybe)
- mysql (maybe)
- …

Windows Agent

Improvements

- Diagnostic
- Performance
- Features
- …

It's your ideas and requirements that drive us!

Let us know by posting your wishes in our Slack channel

Any questions?

tribe**29**

Thank you

tribe29 GmbH
Kellerstraße 29
81667 München
Deutschland

Web — tribe29.com
E-Mail — mail@tribe29.com