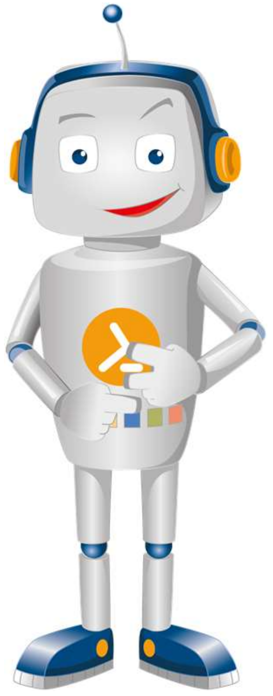
ScriptRunner®

Using PowerShell scripts with more security

Make PowerShell a real solution. For you and your team.

Heiko Brenn | Head of International Business

www.scriptrunner.com



Logicstics

ScriptRunner®

- Duration: approx. 45 minutes
- Phones are muted during this webinar
- You can pose questions via the chat function of GoToWebinar
- We will answer your questions at the end of the presentation
- You will get access to the presentation slides and the webinar recording
  => Double Opt-In required!

Short profile Heiko Brenn

- Product Expert & Head of International Business
- In the IT industry for 25+ years
- Many years of experience as
  - Administrator
  - Consultant
  - Product Manager
- Responsible for EMEA and North America
  - Technical Sales
  - Consulting
  - Partner Management
- Contact information
  - Phone: +49-162-4879156 and +1-6469806339
  - Email: heiko.brenn@scriptrunner.com
  - Linkedin: www.linkedin.com/in/HeikoBrenn
  - Twitter: twitter.com/heikobrenn
  - GitHub: github.com/HeikoBrenn

Agenda

ScriptRunner®

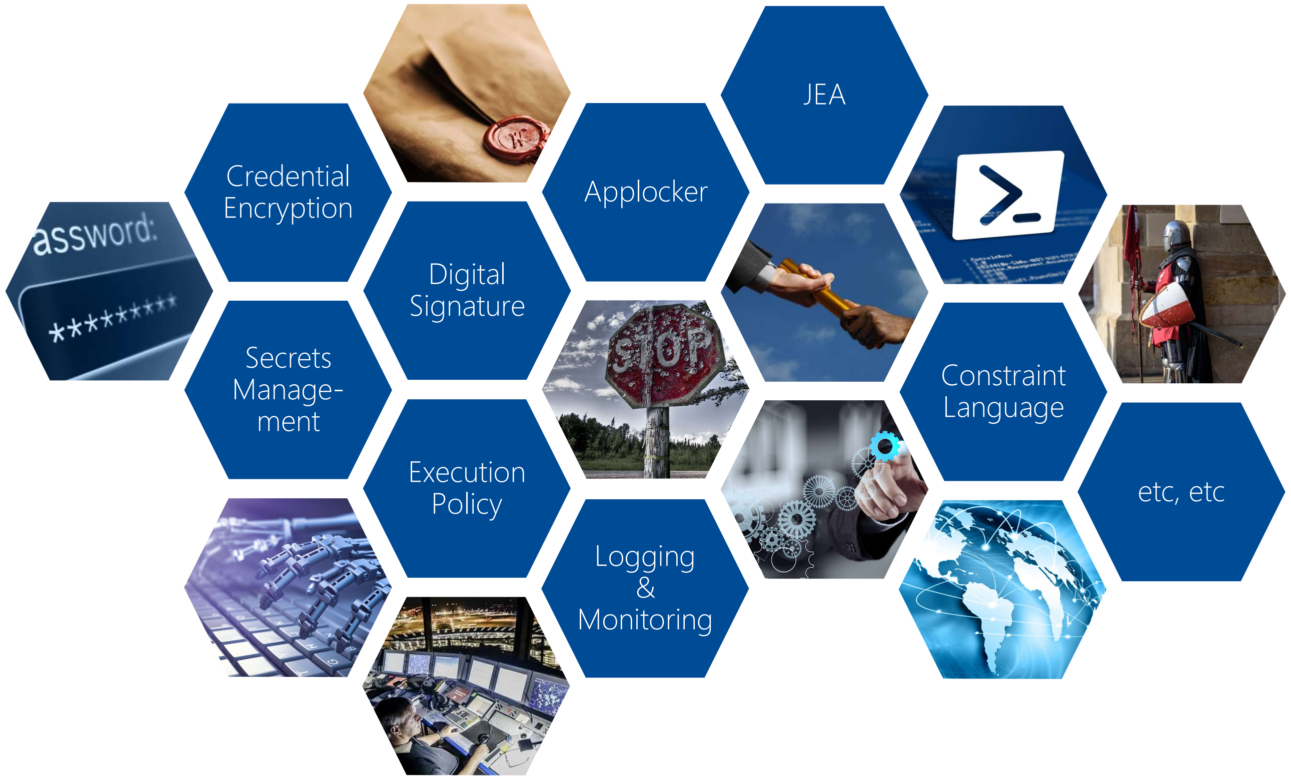
The different aspects of Security and PowerShell

How ScriptRunner enhances PowerShell Security

The different aspects of Security and PowerShell

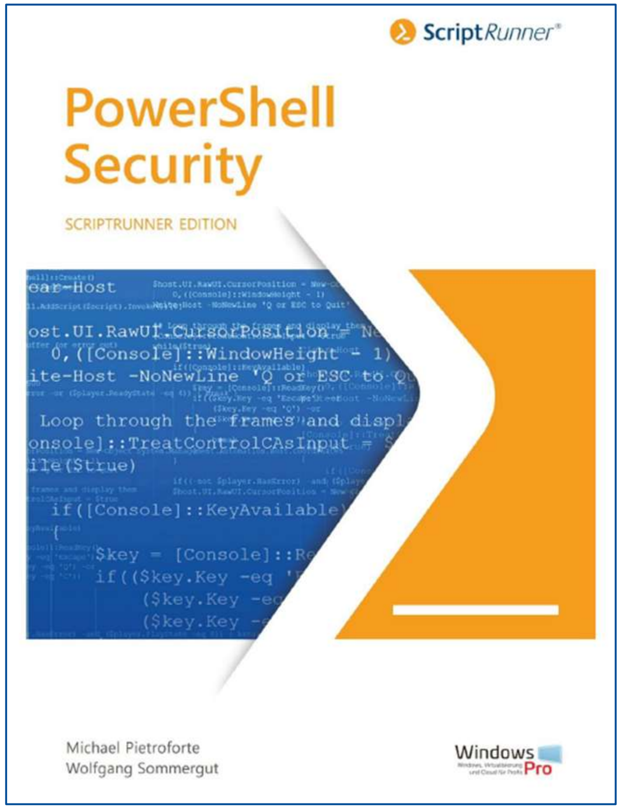
PowerShell and Security - a wide area

ScriptRunner®



PowerShell Security eBook

- Covers all relevant security aspects
- Great detailed content (157 pages)
- Joint project of WindowsPro, 4sysops and ScriptRunner
- Get it for free
- https://lp.scriptrunner.com/de/powershell-security-guide
- English version available soon (you will be notified)


ScriptRunner

PowerShell Security

SCRIPTRUNNER EDITION

Michael Pietroforte
Wolfgang Sommergut

Windows Pro

Execution Policy

ScriptRunner®

- Simple control to protect from accidental execution of code
- Get-ExecutionPolicy
- Set-ExecutionPolicy
- Restricted - No Script either local, remote or downloaded can be executed on the system.
- AllSigned - All script that are ran require to be digitally signed.
- RemoteSigned - All remote scripts (UNC) or downloaded need to be signed.
- Unrestricted - No signature for any type of script is required. User gets warning.
- Bypass -Nothing is blocked and there are no warnings or prompts.
- Undefined – Default policy is set (Restricted)
- GPO overwrites local settings
- Recommendation: Configure via GPO
- Enable through GPO
  - Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell
- Remember: There are many ways to surpass the execution policy

Digitale Signature

- Digitale Signatures answer two questions:
  - Who has created the PowerShell script? (Authentication)
  - Has the script been changed after the signing process? (Integrity)
- Use existing certificate
- Create self signed cert with New-SelfSignedCertificate
- Set-AuthenticodeSignature -FilePath C:\test\local_script.ps1 -Certificate (Get-ChildItem -Path Cert:\CurrentUser\My\ -CodeSigningCert)
- Scripts have to be “re-signed” after every change
- PowerShell detects script code in signature block

Logging & Monitoring

- Module Logging - Pipeline execution events for members of the specified modules are recorded in the Windows PowerShell log in Event Viewer
- PowerShell Script Block Logging - Logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log
- PowerShell Transcription - Captures the input and output of Windows PowerShell commands into text-based transcripts. (local path or UNC)
  - Start-Transcript
  - Stop-Transcript
  - Default path: *"%userprofile%\documents"*
- Tracing and analyzing attacks
- Enable through GPO
  - Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell

Constrained Language

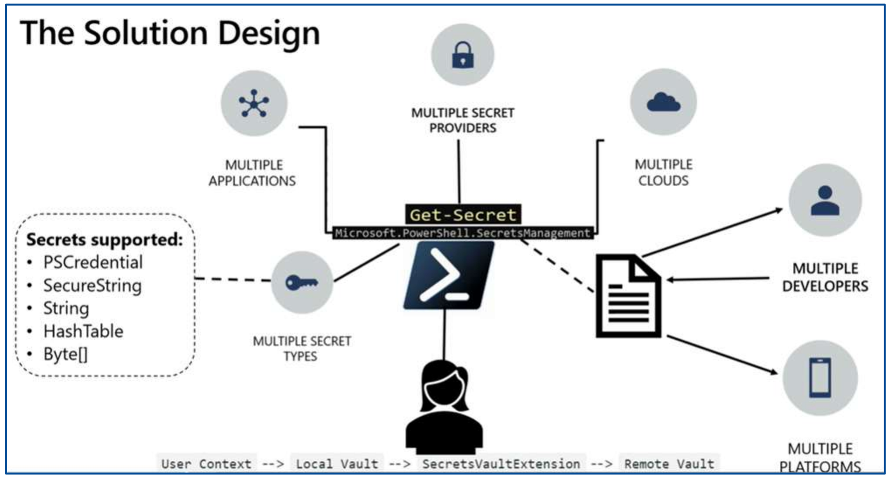
- PowerShell can be used in different languages modes
  - FullLanguage
  - ConstrainedLanguage
  - RestrictedLanguage
  - NoLanguage
- Session based
- $ExecutionContext.SessionState.LanguageMode = "ConstrainedLanguage„
  - Permits all Windows cmdlets and all PowerShell language elements, but it limits permitted types.
- Use in combination with Applocker or Device Guard

Credentials

- One of the biggest challenges in PowerShell security
- PSCredentials requires username and password
- User and password in scripts is absolutely no-go
- Credentials in scripts or user interaction prohibit secure delegation and automation
- Reading encrypted passwords from files requires access to these files for every execution
- Password file works only on the same machine
- Password change scenarios?! Password rotation? Delegation?

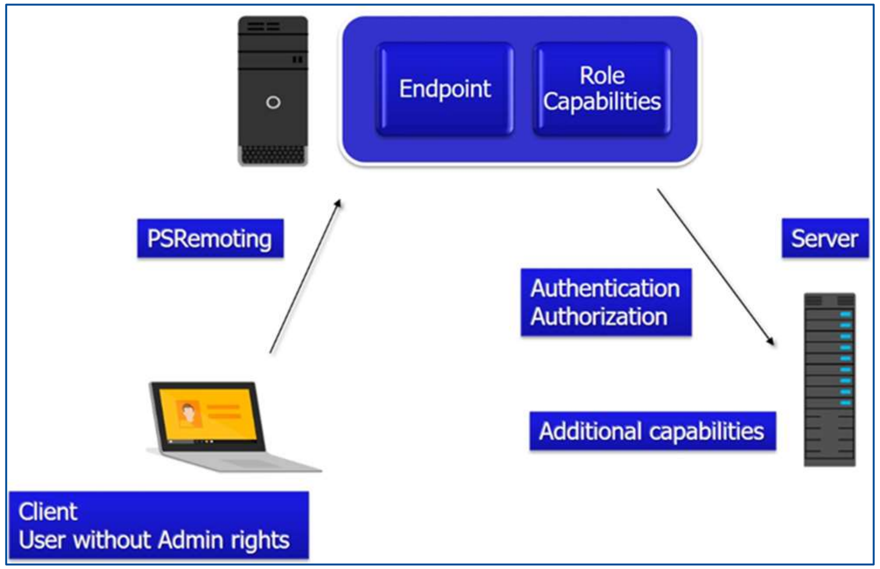
Secrets Management Module

- Requires PowerShell 7
- Uses Windows Credential Store
- Uses local user context
- Can be extended with custom vaults



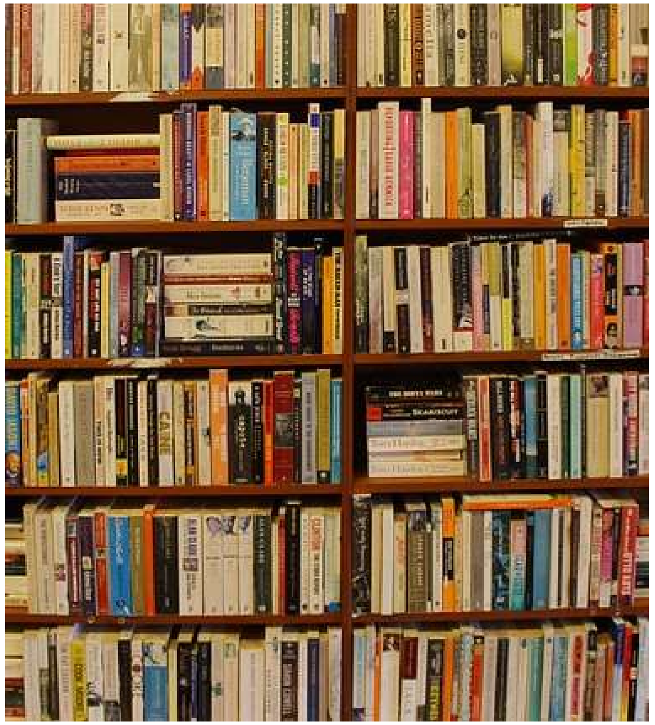
JEA

- Main goal is limited privileges for PowerShell Remoting
- Requires PowerShell 5.0 or higher
- Default since Windows Server 2016 and Windows 10
- Role-based access control (RBAC) endpoints
- Allows only execution of configured commands and parameters (Whitelisting)
- Session Configuration file (Who is allowed to connect to an endpoint)
- Role Capability file(s) (What tasks are allowed)
- When you delegate to helpdesk, etc., users still have to know PowerShell



Ressources

- https://blogs.msdn.microsoft.com/daviddasneves/2017/05/25/powershell-security-at-enterprise-customers/
- https://devblogs.microsoft.com/powershell/powershell-the-blue-team/
- https://www.digitalshadows.com/blog-and-research/powershell-security-best-practices/
- https://cqureacademy.com/blog/cybersecurity-talk/jeffrey-hicks
- https://blog.netspi.com/15-ways-to-bypass-the-powershell-execution-policy/
- https://www.darkoperator.com/blog/2013/3/5/powershell-basics-execution-policy-part-1.html
- https://github.com/dlwyatt/PolicyFileEditor
- https://docs.microsoft.com/en-us/powershell/module/pkiclient/new-selfsignedcertificate
- https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-6
- https://sid-500.com/2017/10/26/how-to-digitally-sign-powershell-scripts/
- https://docs.microsoft.com/de-de/powershell/wmf/5.0/audit_script
- https://devblogs.microsoft.com/powershell/powershell-constrained-language-mode/
- https://docs.microsoft.com/de-de/powershell/module/microsoft.powershell.core/about/about_language_modes?view=powershell-5.1
- https://blogs.technet.microsoft.com/ashleymcglone/2016/08/30/powershell-remoting-kerberos-double-hop-solved-securely/
- https://sid-500.com/2018/02/11/powershell-implementing-just-enough-administration-jea-step-by-step
- https://www.red-gate.com/simple-talk/sysadmin/powershell/powershell-just-enough-administration/



Demo:
PowerShell Security Options

How ScriptRunner enhances PowerShell Security

With great Power(Shell) comes great responsibility

ScriptRunner®

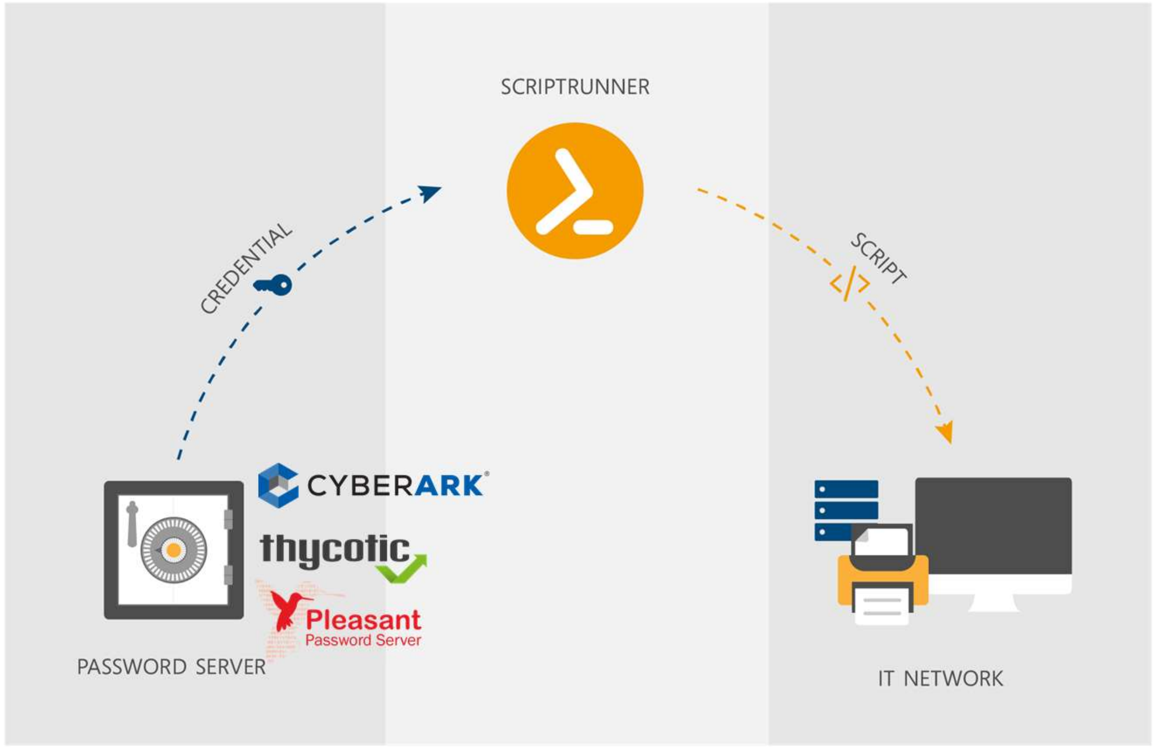
Wouldn't it be great, if you could...

End the script anarchy and have a secure single source of truth for your PowerShell scripts	Manage PowerShell credentials centrally and secure	Avoid granting privileged permissions to users	Run and monitor PowerShell in a central and secure environment	Delegate PowerShell execution safely to helpdesk & end users

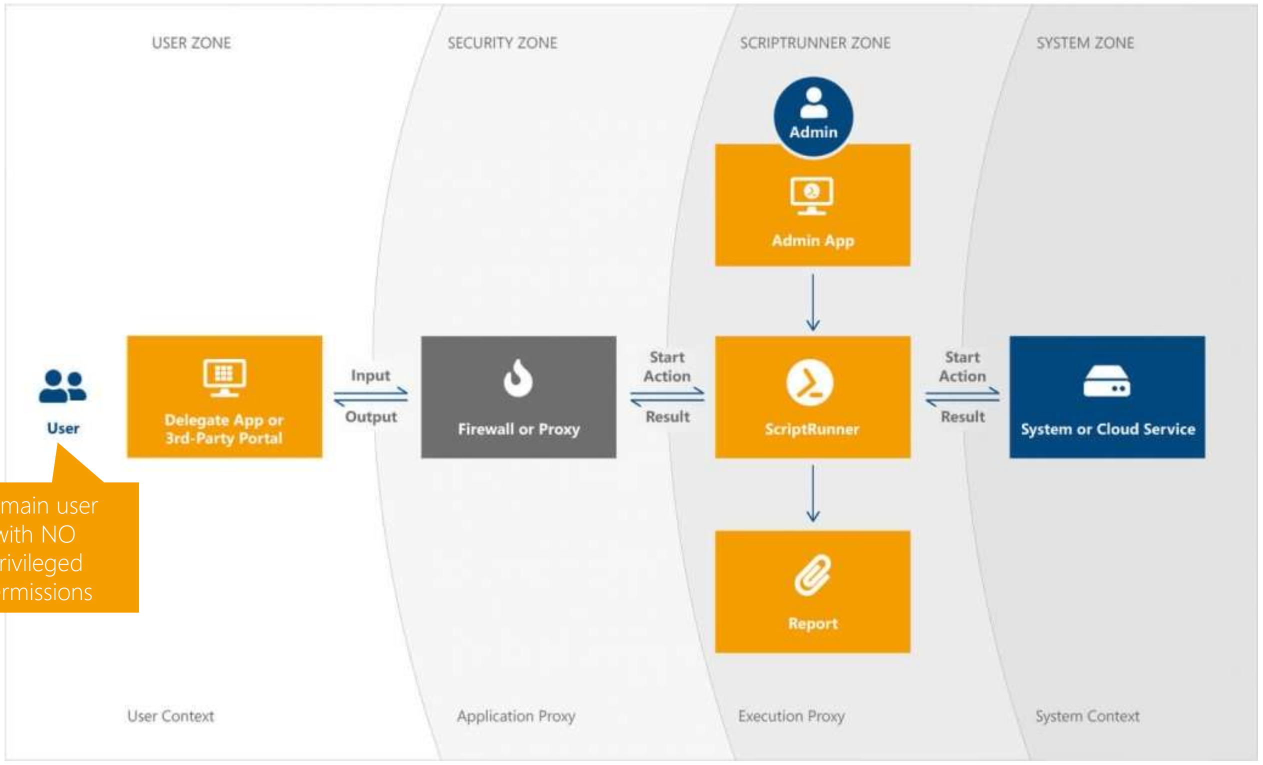
Secure PowerShell Lifecycle

Password Server Support

- Centralized password safes
  - CyberArk Password Vault
  - Pleasant Password Server
  - Thycotic Secret Server
- No credentials are stored locally
- Automatic password rotation
- Easy One secure password repository for multiple ScriptRunner servers



Secure Delegation



Domain user with NO privileged permissions

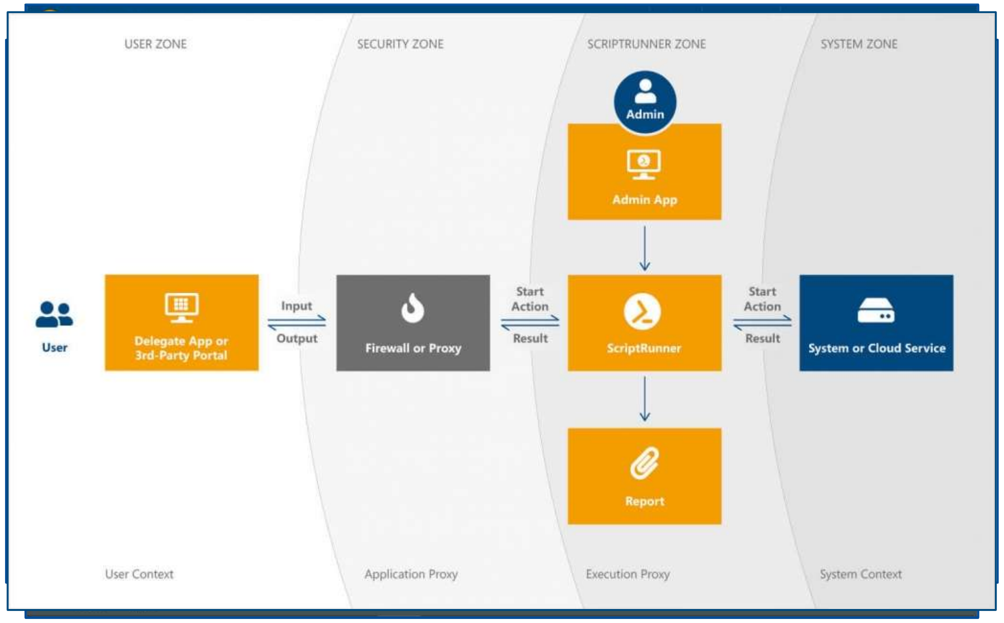
https://www.scriptrunner.com/de/software/system/

Demo: How ScriptRunner enhances PowerShell Security

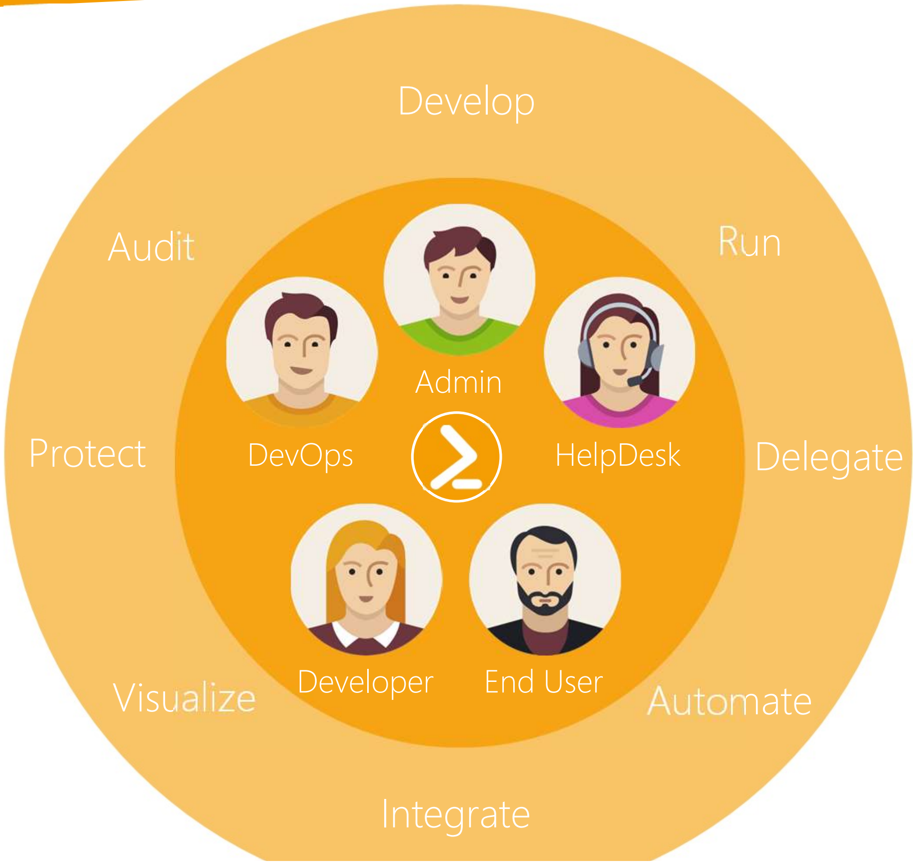
Achieve More With PowerShell In 5 Steps

ScriptRunner®

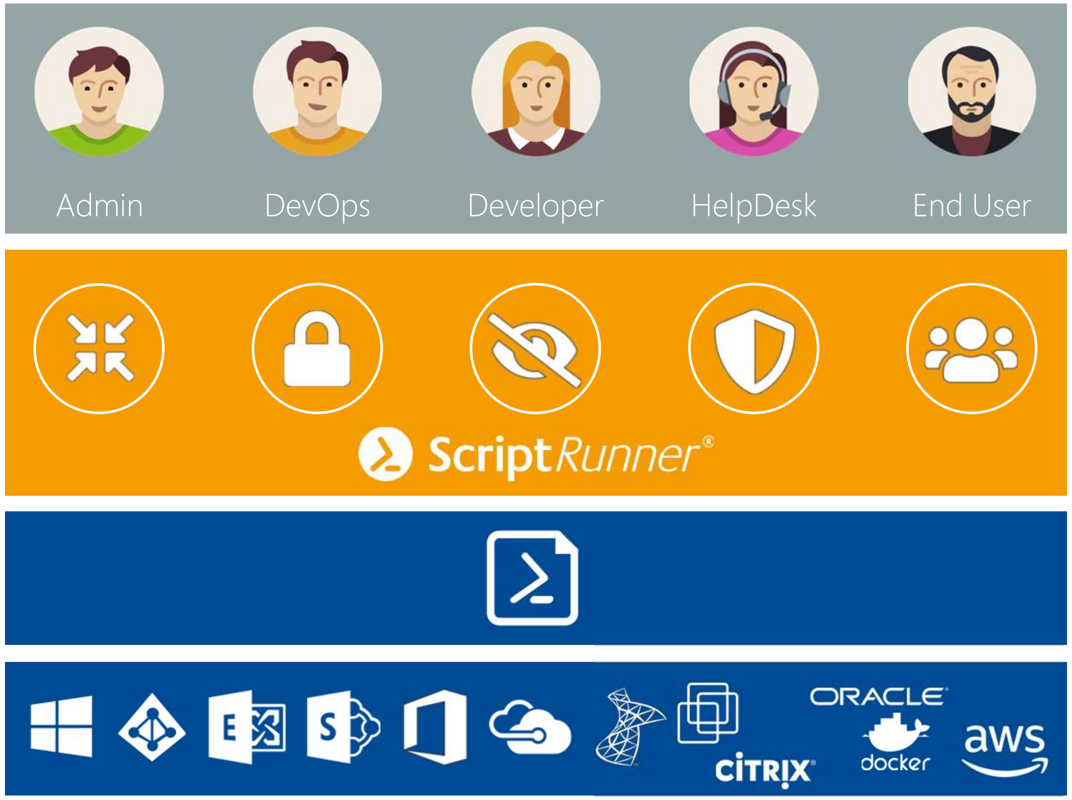
- Centralize your PowerShell scripts
- Manage credentials & permissions securely
- Automatically transform PowerShell scripts into Web GUIs
- Delegate recurring tasks to help desk and end users
- Integrate with ITSM, Monitoring & Workflow systems and more



ScriptRunner – Your Smart PowerShell Control Center



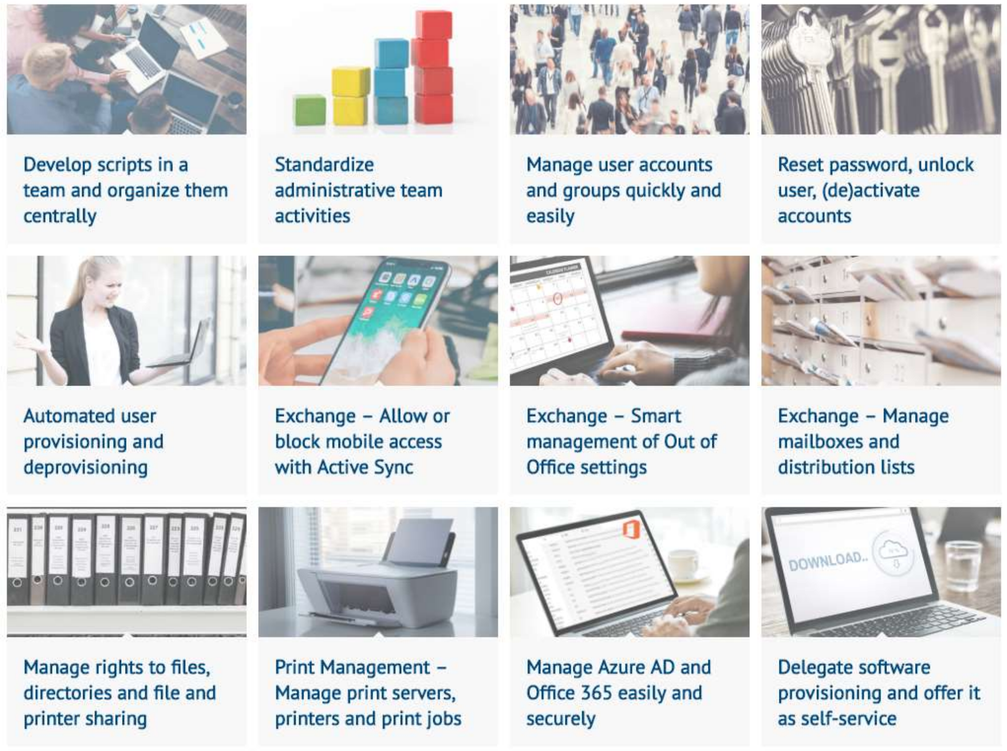
ScriptRunner – Make PowerShell A Real Solution



ScriptRunner – Sample scenario

Actions	Create New Mailbox
Queries	Select OU
Targets	Exchange, Exchange Online
Scripts	New-Mailbox.ps1
Credentials	Service account with necessary permissions
Delegation	Helpdesk user, End user

ScriptRunner – Practical Examples and Use Cases



Develop scripts in a team and organize them centrally

Standardize administrative team activities

Manage user accounts and groups quickly and easily

Reset password, unlock user, (de)activate accounts

Automated user provisioning and deprovisioning

Exchange – Allow or block mobile access with Active Sync

Exchange – Smart management of Out of Office settings

Exchange – Manage mailboxes and distribution lists

Manage rights to files, directories and file and printer sharing

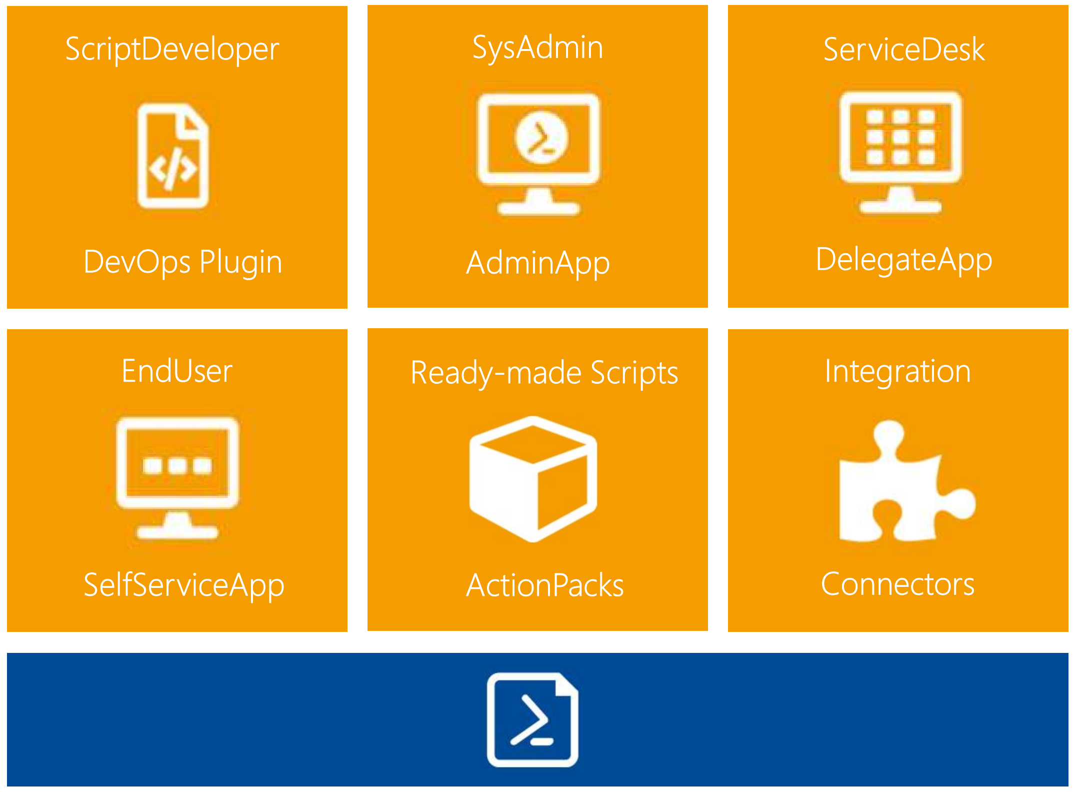
Print Management – Manage print servers, printers and print jobs

Manage Azure AD and Office 365 easily and securely

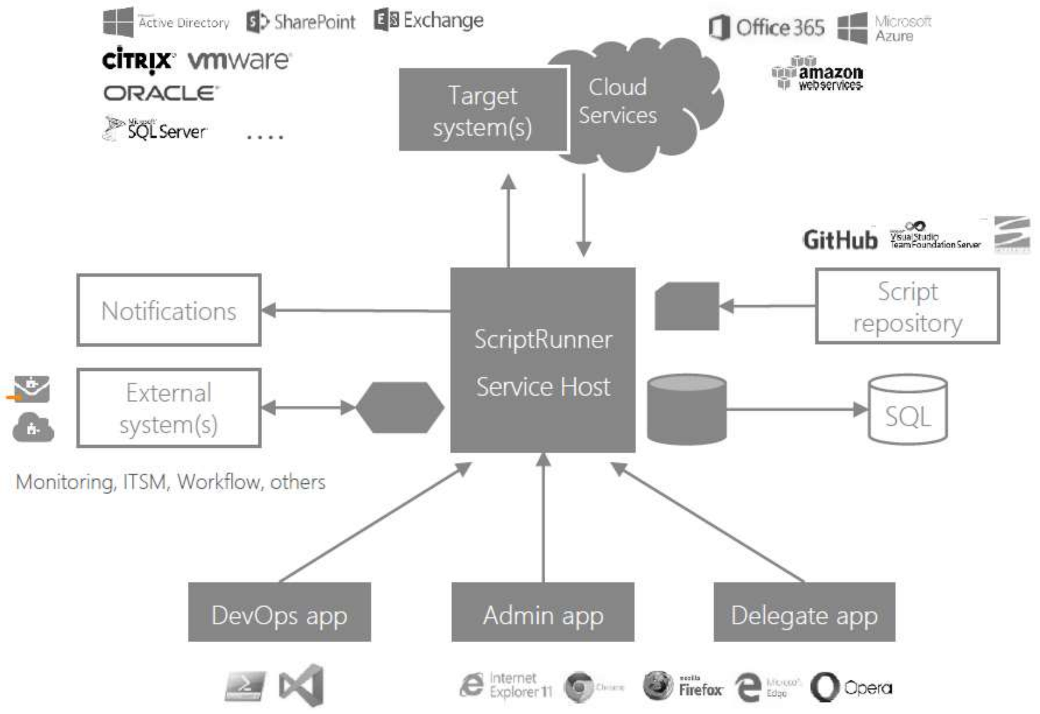
Delegate software provisioning and offer it as self-service

https://www.scriptrunner.com/en/practical-examples/

ScriptRunner – The components



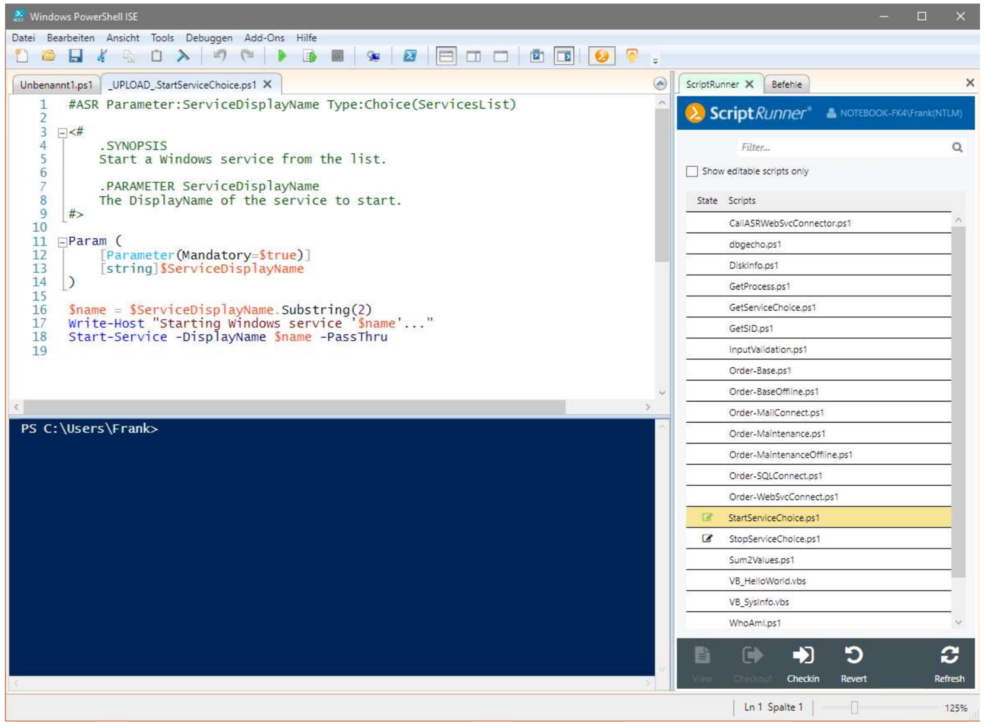
ScriptRunner – How the components play together



https://www.scriptrunner.com/en/software/system/

ScriptDeveloper – DevOps Plugin

- ISE Plugin
- Team-based script development
- Central script repository
- Filters
- Check-in with history
- Check-out
- GitHub integration
- TFS integration
- More information
  - https://www.scriptrunner.com/en/software/scripts/



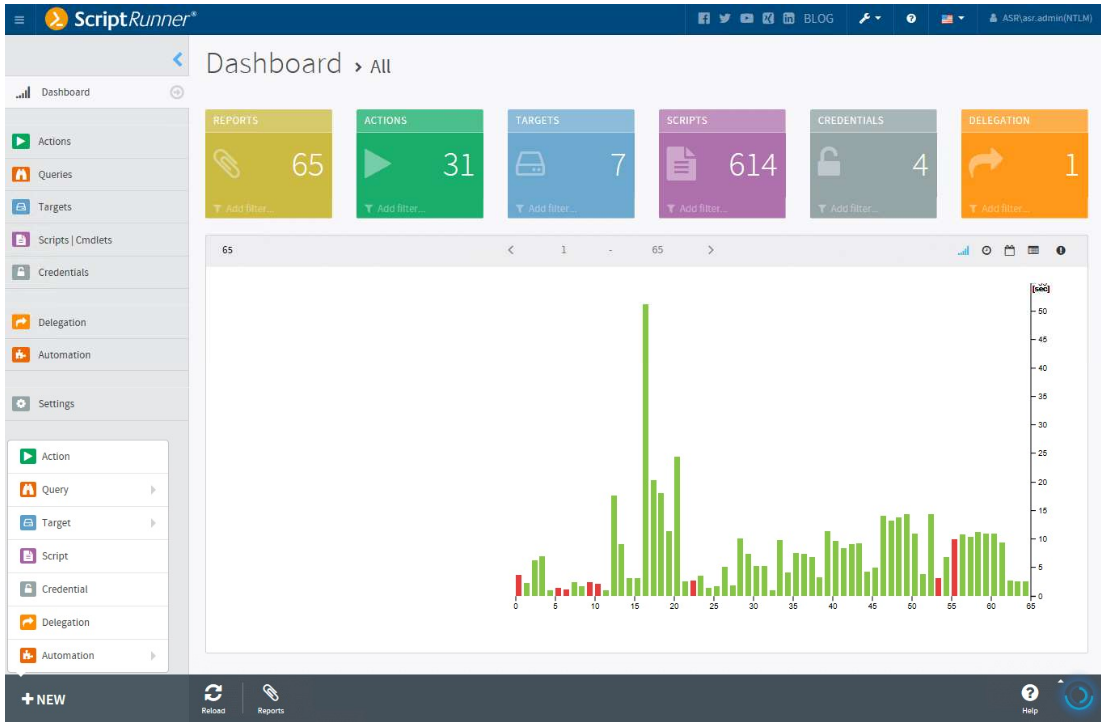
```
#ASR Parameter:ServiceDisplayName Type:Choice(ServicesList)

<#
    .SYNOPSIS
    Start a Windows service from the list.

    .PARAMETER ServiceDisplayName
    The DisplayName of the service to start.
#>

Param (
    [Parameter(Mandatory=$true)]
    [string]$ServiceDisplayName
)

$name = $ServiceDisplayName.Substring(2)
Write-Host "Starting Windows service '$name'..."
Start-Service -DisplayName $name -PassThru

```

```
PS C:\Users\Frank>
```

State	Scripts
	CallASRWebSvcConnector.ps1
	dbgecho.ps1
	DiskInfo.ps1
	GetProcess.ps1
	GetServiceChoice.ps1
	GetSID.ps1
	InputValidation.ps1
	Order-Base.ps1
	Order-BaseOffline.ps1
	Order-MailConnect.ps1
	Order-Maintenance.ps1
	Order-MaintenanceOffline.ps1
	Order-SQLConnect.ps1
	Order-WebSvcConnect.ps1
✎	StartServiceChoice.ps1
✎	StopServiceChoice.ps1
	Sum2Values.ps1
	VB_HelloWorld.vbs
	VB_SysInfo.vbs
	WhoAmI.ps1

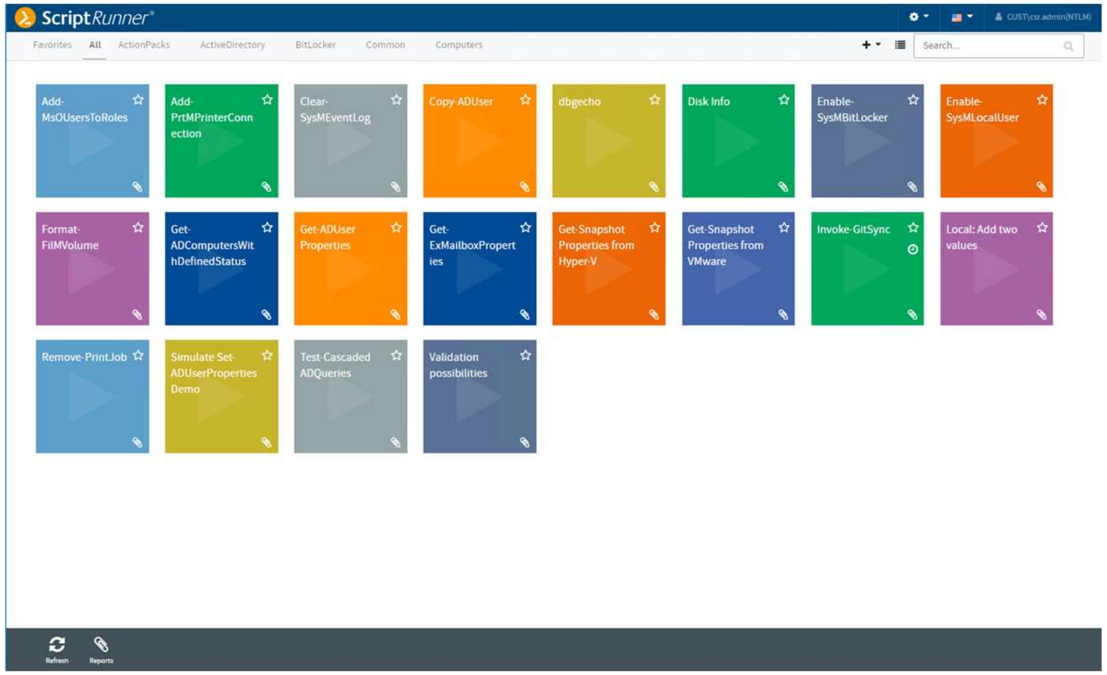
SysAdmin – Admin App

- A web GUI for PowerShell
- Dashboard for all activities
- Create ScriptRunner actions
- Manage and test queries
- Target configuration
  - Direct local
  - PowerShell remoting
  - Implicit remoting
- [Secure delegation of ScriptRunner actions]()
- Scheduled script execution
- Secure credential handling
- Configure automation connectors
- Organizing by tags
- Reports and Logging
- More information
  - https://www.scriptrunner.com/en/software/web-apps



ServiceDesk – DelegateApp

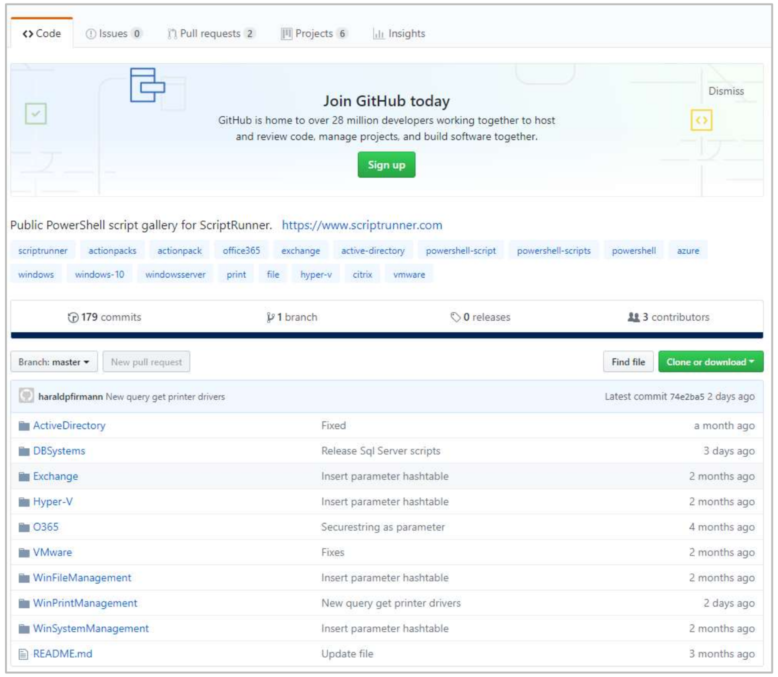
- A web GUI for PowerShell
- Execute PowerShell scripts in the browser
- Delegate specific ScriptRunner actions to team members, helpdesk or endusers
- No administrative permissions for users required
- Parameters for script execution can be hidden
- Input dialogs are automatically created from PowerShell script
- Script execution logging and reporting
- More information
  - https://www.scriptrunner.com/en/software/web-apps



Ready-made Scripts – ActionPacks

ScriptRunner®

- Easy implementation of many use cases
- Out of the box scripts for
  - Active Directory
  - Office 365
  - Exchange
  - VMWare
  - Hyper-V
  - Citrix
  - File-/PrintServer
- Scripts and templates for partner products
  - Paessler PRTG
  - Matrix42
  - Nagios
  - Automic ONE
- More informationen
  - https://github.com/scriptrunner/ActionPacks
  - https://www.scriptrunner.com/en/software/script-sammlungen/



Join GitHub today

GitHub is home to over 28 million developers working together to host and review code, manage projects, and build software together.

Public PowerShell script gallery for ScriptRunner. https://www.scriptrunner.com

scriptrunner actionpacks actionpack office365 exchange active-directory powershell-script powershell-scripts powershell azure windows windows-10 windowsserver print file hyper-v citrix vmware

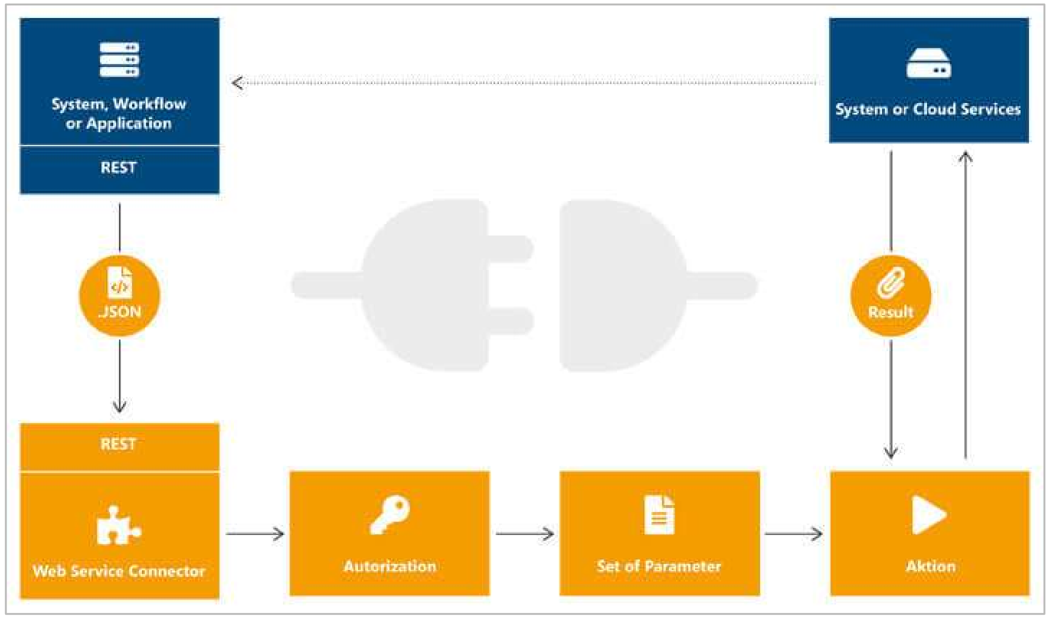
179 commits 1 branch 0 releases 3 contributors

haraldpfirmann New query get printer drivers Latest commit 74e2ba5 2 days ago

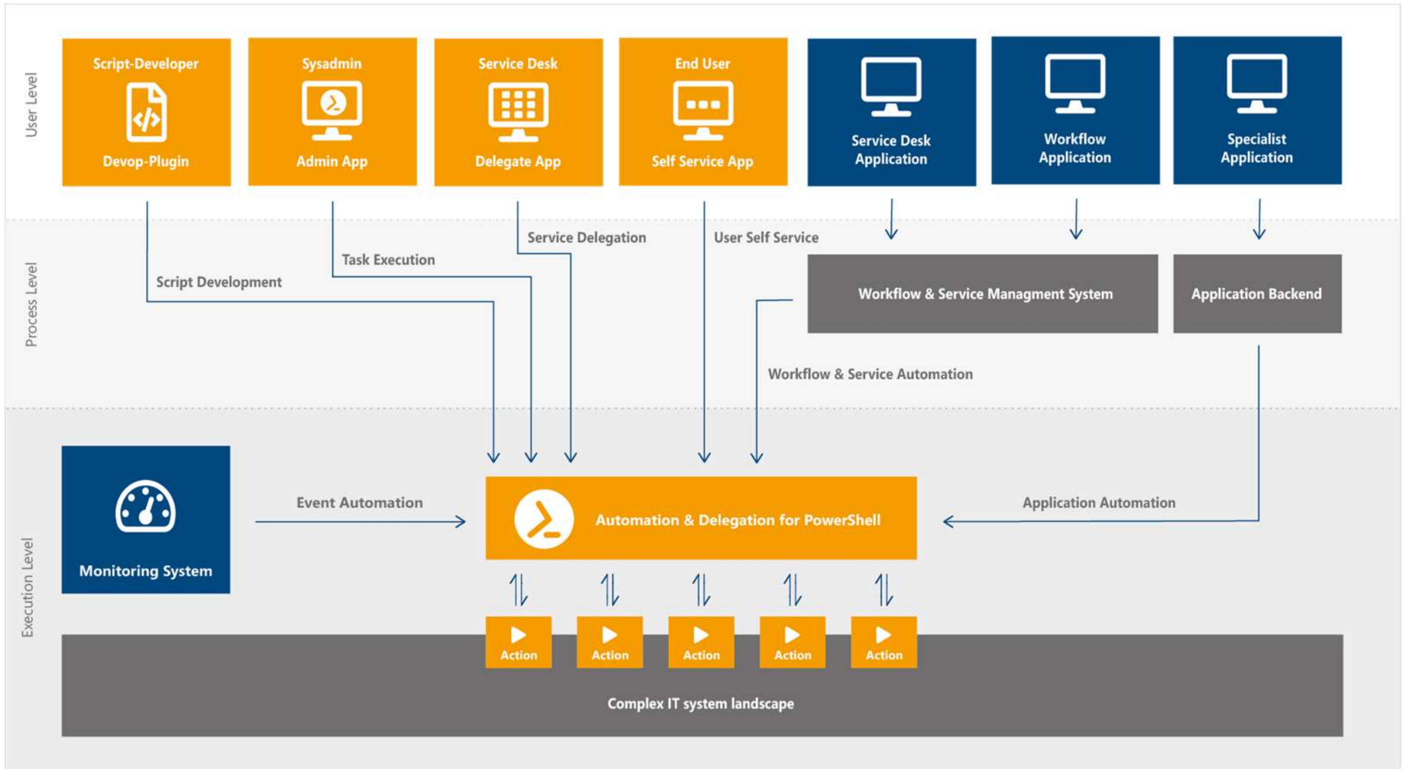
ActiveDirectory	Fixed	a month ago
DBSystems	Release Sql Server scripts	3 days ago
Exchange	Insert parameter hashtable	2 months ago
Hyper-V	Insert parameter hashtable	2 months ago
O365	Securestring as parameter	4 months ago
VMware	Fixes	2 months ago
WinFileManagement	Insert parameter hashtable	2 months ago
WinPrintManagement	New query get printer drivers	2 days ago
WinSystemManagement	Insert parameter hashtable	2 months ago
README.md	Update file	3 months ago

Integration – Add new functions with connectors

- 3rd party systems automatically trigger ScriptRunner Actions
  - Monitoring Systems
  - IT Service Management
  - Business Workflow
  - Applications
  - Paessler PRTG
  - ServerEye
  - Nagios
- Password server integration
  - CyberArk
  - Pleasant
  - Thycotic
- More information
  - https://www.scriptrunner.com/en/software/automation-connector/



ScriptRunner – The Full Picture



https://www.scriptrunner.com/en/software/system/

ScriptRunner test report fom a Microsoft MVP

ScriptRunner®

Adam Bertram aka Adam The Automator
Microsoft MVP Cloud and Datacenter Management

"ScriptRunner is a master of organizing, categorizing and delegating scripts."

"ScriptRunner is a real DevOps tool for PowerShell scripters."

"Compared to large automation platforms, ScriptRunner is significantly cheaper."

"to get the same functionality of ScriptRunner, it would require several applications to get a similar feature set."

"If you are looking into automating your administration and support processes easily and securely, you will find a powerful and professional tool here."

https://www.adamtheautomator.com/scriptrunner-bringing-powershell-to-devops/

Use cases with with and without ScriptRunner

ScriptRunner®

Case	Done by Admin (2nd/3rd Level)	Delegated with ScriptRunner to ServiceDesk, TeamLead or EndUser
Creating an user in AD	5 min	1 min
Reset User Password	2 min	1 min
Change User Props	4 min	1 min
Change of permissions	5 min	1 min
Create Mailbox	4 min	1 min
Change Mailbox Props	5 min	1 min
Set Out-of-office	not available	1 min Service Desk or TeamLead
User Statistics	10 min	0 min Service Desk (automatically)
Mailbox Statistics	10 min	0 min Service Desk (automatically)

Most of the cases are already included in the ScriptRunner Action Packs. By using the Action Packs you avoid 50 up to 250 hours script development time.

Get your free PowerShell poster

ScriptRunner®

Windows PowerShell
www.scriptrunner.com
ScriptRunner®
Make PowerShell a real solution
TURN PAGE
STRINGS AND EXPRESSIONS
COMPARISON OPERATORS
INPUT AND OUTPUT COMMANDLETS
IMPORTANT NAVIGATION COMMANDLETS
GET HELP
PIPELINING
POWERSHELL DATA TYPES
POWERSHELL SCRIPTING LANGUAGE
USING .NET FRAMEWORK CLASSES
CONFIGURING AND USING NETWORKS
ACTIVE DIRECTORY (AD)
IMPORTANT PIPELINING COMMANDLETS
POWERSHELL CLASSES
OBJECT-ORIENTED ACCESS TO PIPELINE OBJECTS
CONFIGURING POWERSHELL
ACCESS TO WMI
PROCESSES, SERVICES, EVENTS, PERFORMANCE INDICATORS
SOFTWARE INSTALLATION
USING MODULES

https://lp.scriptrunner.com/en/powershell-poster

Next Steps

ScriptRunner®

Read the LinkedIn article „2020 – Finally the year of IT automation?“ https://bit.ly/2NNkc88

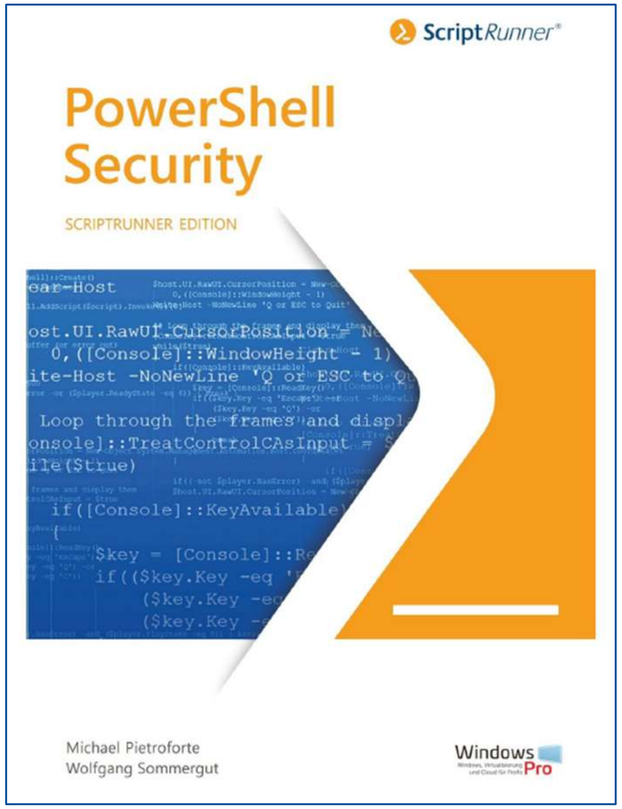
Start testing ScriptRunner: lp.scriptrunner.com/en/demo-download

Book a online demo session with me: lp.scriptrunner.com/meetings/heiko-brenn/demo-en

Start using hundreds of ready-made PowerShell scripts: https://github.com/scriptrunner/ActionPacks

PowerShell Security eBook

- Covers all relevant security aspects
- Great detailed content (157 pages)
- Joint project of WindowsPro, 4sysops and ScriptRunner
- Get it for free
- https://lp.scriptrunner.com/de/powershell-security-guide
- English version available soon (you will be notified)



Thank you.

www.scriptrunner.com

ScriptRunner – Make PowerShell a real solution. For you and your team.

© ScriptRunner Software GmbH
Ludwig-Erhard-Straße 2 | 76275 Ettlingen | Germany

Tel: +49 (0) 7243 34887-0
Mail: info@scriptrunner.com