

NIC  
EMPOWER

---

November 13-15, Oslo Spektrum

Jannik Reinhard & Florian Salzmann

Top 10 Hardening Tips for Your Enterprise Clients

## About "Florian Salzmänn"

---

### Focus

Endpoint Management / Intune

### From

Switzerland CH

### My Blog

scloud.work



### Hobbies

Travel ✈️  
Tech 🖥️  
Wine 🍷

### Contact

@FlorianSLZ



# About "Jannik Reinhard"

## Focus

AI 🤖, Workspace 🏢, Cloud ☁

## From

Germany 🇩🇪

## My Blog

Jannikreinhard.com



## Certifications

Dual MVP + many MS Certifications



## Hobbies

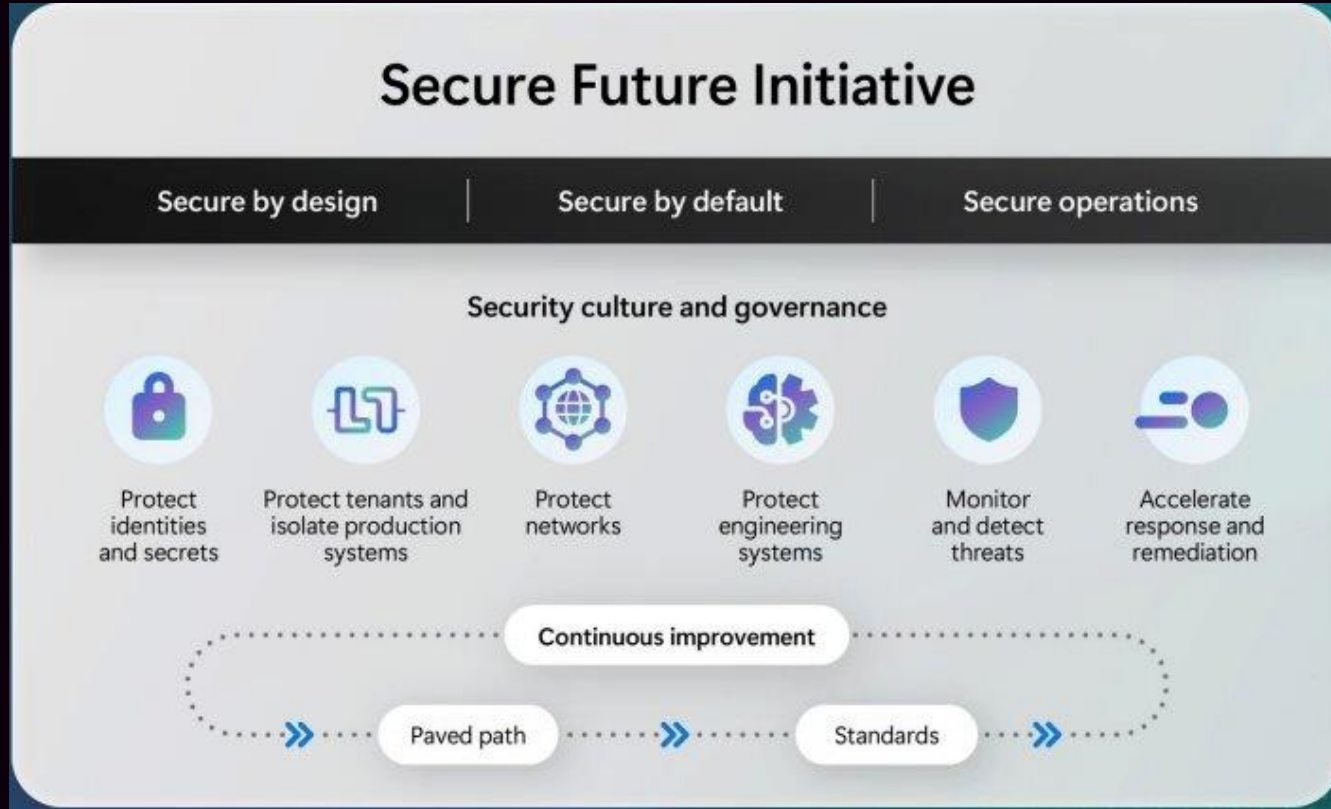
Various Sports 🚴🏊⚽  
Blogging 📝  
Speaking 🎤  
Traveling ✈

## Contact

- X (formerly Twitter) 🐦
- LinkedIn 💼
- Blog 📝
- Email ✉

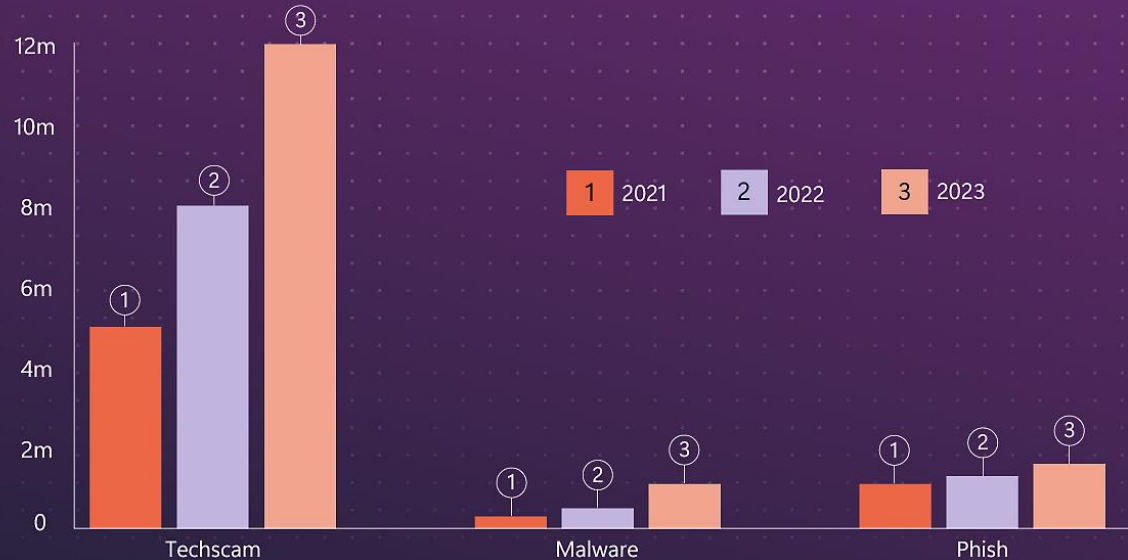


# High Increasing of Threats



# Why Is Security on Your Endpoints Important?

Daily malicious traffic volume (millions)



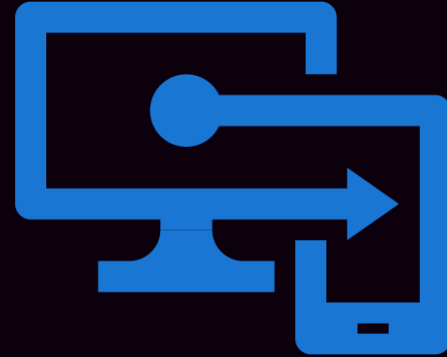
The daily volume of techscam traffic has escalated dramatically, skyrocketing since 2021, a stark contrast compared to malware and phishing over the same period.

Source: SmartScreen log data

## Our Focus



Windows 11



Intune

# Some Basics we assume you already have

- Secure Boot
- BitLocker Encryption
- Remote Desktop is Disabled  
*(RDP = Ransomware Deployment Protocol)*
- Endpoint Detection and Response (EDR)



# Tip #1 - Windows Hello for Business

Enable secure, user-friendly authentication through PINs and biometrics.

- Safer than traditional passwords - PINs are device-specific and backed by TPM.
- Supports multi-factor authentication (MFA)

## Tip #2 - Attack Surface Reduction (ASR)

Reduce potential exploitation paths by blocking risky activities.

- Apply ASR rules via Microsoft Defender for Endpoint to control actions like running macros or launching executables from email attachments.
- Utilize audit mode to measure impact before enforcing.



Only available with  
Defender as active AV

# ASR Report Demo



Investigations



Explorer



Review



Campaigns



Threat tracker



Exchange message trace



Attack simulation training



Policies &amp; rules



Cloud apps



Cloud discovery



Cloud app catalog



OAuth apps



Files



Activity log



Governance log



Policies



Reports



Audit



Health



Permissions



Settings



More resources



Customize navigation

Reports &gt; Attack surface reduction rules

Detections

Configuration

Add exclusions

Review possible breach activity detected by attack surface reduction rules on your devices. [Learn more about the rules](#)

Filters: Rules: Standard protection



Date: 13/10/2024-12/11/2024



Select rules: Any



Add filter



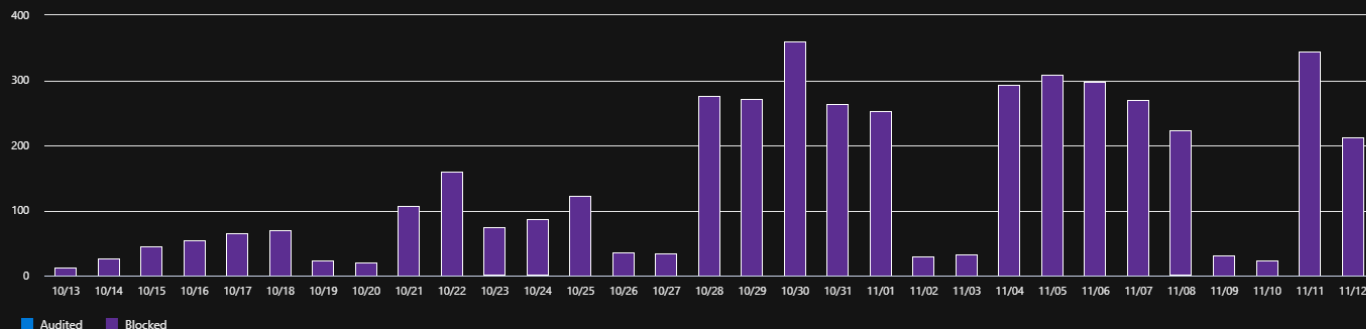
Reset all

Audited detections

4

Blocked detections

4421



Export

4425 items

Search

GroupBy

Detected file	Detected on	Blocked/Audited?	Rule	Source app	Device	Device group	User	Publisher
<input type="checkbox"/> svchost.exe	12 Nov 2024 15:04	Blocked	Block credential ste...	svchost.exe		Unknown Group	SYSTEM	Microsoft Corporat...
<input type="checkbox"/> svchost.exe	12 Nov 2024 15:04	Blocked	Block credential ste...	svchost.exe		Unknown Group	SYSTEM	Microsoft Corporat...
<input type="checkbox"/> svchost.exe	12 Nov 2024 15:01	Blocked	Block credential ste...	svchost.exe		Unknown Group	SYSTEM	Microsoft Corporat...
<input type="checkbox"/> svchost.exe	12 Nov 2024 14:59	Blocked	Block credential ste...	svchost.exe		Unknown Group	SYSTEM	Microsoft Corporat...
<input type="checkbox"/> svchost.exe	12 Nov 2024 14:58	Blocked	Block credential ste...	svchost.exe		Unknown Group	SYSTEM	Microsoft Corporat...
<input type="checkbox"/> svchost.exe	12 Nov 2024 14:58	Blocked	Block credential ste...	svchost.exe		Unknown Group	SYSTEM	Microsoft Corporat...
<input type="checkbox"/> svchost.exe	12 Nov 2024 14:56	Blocked	Block credential ste...	svchost.exe		Unknown Group	SYSTEM	Microsoft Corporat...

Detections Configuration Add exclusions

Rules

Standard protection All

Device configuration overview

All exposed devices18

Devices with rules not configured18

Devices with rules in audit mode0

Devices with rules in warn mode0

Devices with rules in block mode163


Identify and fix devices with limited protection due to missing prerequisites or misconfigured rules. [Learn about prerequisites](#)


186 items Search

Device	Overall configuration	Rules in block mode	Rules in audit mode	Rules in warn mode	Rules turned off	Rules not applicable	Unknown	Device ID
	Rules in block mode	15	0	0	1	0	0	560c476253f2b743...
	Rules in block mode	15	0	0	1	0	0	03ee94e82e076391...
	Rules in block mode	15	0	0	1	0	0	15d5840196b8088...
	Rules off	0	0	0	15	1	0	baefee810dccd66...
	Rules in block mode	15	0	0	1	0	0	20b2909b4b622c9...
	Rules in block mode	12	1	0	0	3	0	3ceb919630aaca91...
	Rules in block mode	15	0	0	1	0	0	860bff7871289b8b...
	Rules in audit mode	0	1	0	15	0	0	ccd45e9d2c696965...
	Rules in audit mode	0	1	0	15	0	0	c2ad20cc8979a0d2...

Select detected files to exclude, see how excluding them might impact detections, and export the list to update your policies. [Learn more](#)

38 items

 Search

 Filter

Filters: Rules: All

<input type="checkbox"/> File name	Detections	Devices
<input type="checkbox"/> cmd.exe	3998	7
<input type="checkbox"/> svchost.exe	3954	146
<input type="checkbox"/> cagent32.exe	236	1
<input type="checkbox"/> HPFirmwareInstaller.exe	208	15
<input type="checkbox"/> WaAppAgent.exe	79	12
<input type="checkbox"/> msixexec.exe	57	11
<input type="checkbox"/> LITSSvc.exe	30	1
<input type="checkbox"/> msedgewebview2.exe	26	1
<input type="checkbox"/> Acrobat.exe	16	3
<input type="checkbox"/> ProcessManager.exe	13	9
<input type="checkbox"/> Au_.exe	12	11

## Summary & expected impact

Adding files to exclude from attack surface reduction rules can minimize unwanted detections. [Learn more](#)

### Summary

Files selected

0

Select files to exclude to simulate impact.



# ASR\_Rules\_Policy\_Clients

Attack Surface Reduction Rules



Delete

Configuration settings [Edit](#)

^ Defender

Block execution of potentially obfuscated scripts ⓘ Block

ASR Only Per Rule Exclusions ⓘ

Block Office communication application from creating child processes ⓘ Block

ASR Only Per Rule Exclusions ⓘ

C:\Program Files (x86)\inPuncto\System32\biz2Validator\_Start.exe

Block all Office applications from creating child processes ⓘ Block

ASR Only Per Rule Exclusions ⓘ

C:\Program Files\FLIR Systems\FLIR Word Add-in\bin\FLIR Report Studio.exe, C:\Program Files\FLIR Systems\FLIR Word Add-in\bin\Flir.LicenseCheck.exe

Block Win32 API calls from Office macros ⓘ Block

ASR Only Per Rule Exclusions ⓘ

# Tip #3 - Windows Firewall

Prevent unauthorized network access by enforcing firewall rules.

- Try to avoid separate profiles (private, public, ~~domain~~) for different environments.
- Block always (Zero-Trust)
- Ensure security baseline settings prevent local modifications to firewall settings.



# Firewall Profiles

If you reeeeeeeeeeeeeeealy need different Rulsets:

[Switch to Private Firewall profile on AAD joined when connected to specific network. - CCMEXEC.COM - Enterprise Mobility](#)

# Tip #4 - Account Lockout Policies

Mitigate brute-force attacks on login endpoints

Windows 11 22H2+ Defaults are good,  
**but won't be set if you upgrade!**

Will help you in a (CIS) Audit: [1.2.2 Ensure 'Account lockout threshold' is set to '10 or fewer... | Tenable®](#)

# Tip #5 - Windows LAPS (Local Administrator Password Solution)

Securely manage local admin passwords on endpoints

- Enforces unique passwords per device, rotated automatically
- Stores passwords securely Entra
- Prevents lateral movement

# LAPS Demo

WIN-LAPS - Microsoft Intune

DEV-W11-001 - Microsoft Intune

scloud/scripts/WIN-S-D-LAPS

Devices - Microsoft Entra admin

entra.microsoft.com/#view/Microsoft\_AAD\_Devices/DevicesMenuBlade/~./DeviceSettings/menuld/Devices

Microsoft Entra admin center

Search resources, services, and docs (G+)

florian@dev.scloud.work  
DEV S CLOUD (DEVSCLOUD.WORK)

Home > Users > Devices

Devices | Device settings

DEV scloud - Microsoft Entra ID

Overview

All devices

Manage

Device settings

Enterprise State Roaming

BitLocker keys (Preview)

Local administrator password recovery

Activity

Audit logs

Bulk operation results (Preview)

Troubleshooting + Support

New support request

Diagnose and solve problems

<< Save Discard Got feedback?

Users may register their devices with Microsoft Entra

All None

Learn more on how this setting works

Require Multifactor Authentication to register or join devices with Microsoft Entra

Yes No

We recommend that you require Multifactor Authentication to register or join devices with Microsoft Entra using Conditional Access. Set this device setting to No if you require Multifactor Authentication using Conditional Access.

Maximum number of devices per user

50

Local administrator settings

Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)

Yes No

NIC

EMPOWER

# Tip #6 - Application Control for Business

Control which applications can run on your endpoints

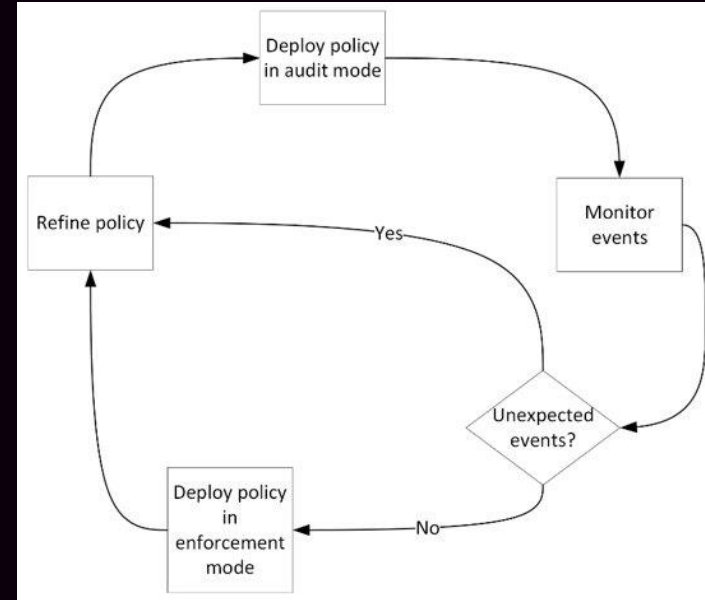
- Also named Windows Defender Application Control (WDAC)
- Successor of AppLocker
- Minimize Shadow-IT
- Start with basic control, such as restricting to known safe apps, and gradually move to stricter policies
- Use "Managed Installer"

# WDAC vs AppLocker

Capability	WDAC	App Locker
Platform support	Available on Windows 10, Windows 11, and Windows Server 2016 or later.	Windows 7 / Windows Server 2008R2 and later
Management	<ul style="list-style-type: none"><li>- Intune (Application Control for Business)</li><li>- Configuration Manager</li><li>- GPO</li><li>- Script</li></ul>	<ul style="list-style-type: none"><li>- Intune (OMA-URI &amp; XML)</li><li>- Configuration Manager</li><li>- GPO</li><li>- Script</li></ul>
Per-user and Per-user group rules	Not available (policies are device-wide).	Available on Windows 8+.
Per App rules	Available	Not available
Managed installer	Available	Not available
Reputation based intelligence (ISG)	Available	Not available
Multiple Policy Support	Available	Not available

# WDAC Implementation

- Creation of the final policy set requires several iterations
- Don't try to much at once

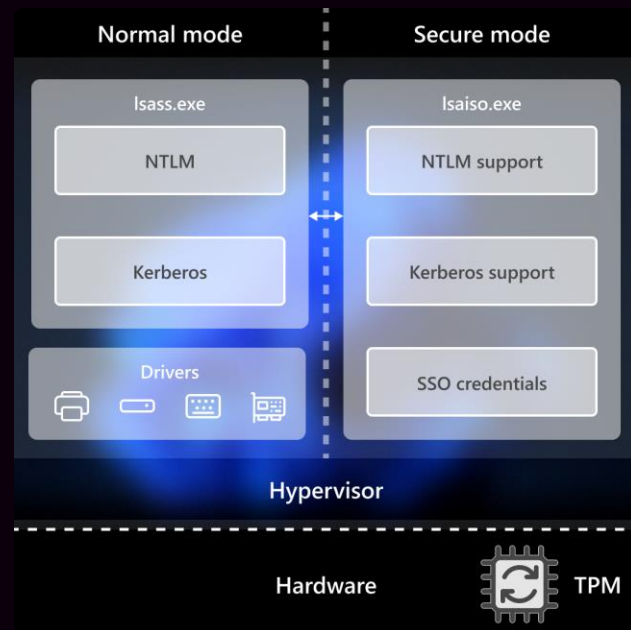




# Tip #7 - Credential Guard

Protect against credential theft, especially pass-the-hash attacks

- Enabled by default on **new** Windows 11 installations
- Requires Secure Boot, TPM, and Virtualization-Based Security



# Tip #8 - Tamper Protection

Prevent unauthorized changes to security configurations

- Locks down Defender settings to prevent disabling protection
- Ensures critical settings like real-time protection remain enabled

# Tip #9 – Consider Passwordless

Move beyond passwords to strengthen security and improve user experience

- Windows Hello for Business
- FIDO2 Keys
- Web-based login
- Smart Cards

# Tip #10 - Conditional Access

Strengthen access control with identity-based conditions

- Use Conditional Access to enforce MFA for specific apps or access scenarios
- Apply policies for sensitive applications and external connections
- Make sure your first login on a new device **always** required MFA

## Bonus Tip

# Security Baselines

Establish a consistent, secure configuration across all devices

- Use Microsoft, CIS, or community-based baselines like OpenIntuneBaseline
- Baselines simplify configuration and ensure compliance with best practices
- **Regularly review baselines as they are updated to reflect new threats**



[SkipToTheEndpoint/OpenIntuneBaseline:](#)  
[Community-driven baseline to accelerate Intune adoption and learning.](#)

# Conclusion and Q&A

- A lot is on by default (but only for new staged devices)
- Don't try to implement all at once
- Review regularly



Thank you!



NIC  
EMPOWER

November 13-15, Oslo Spektrum