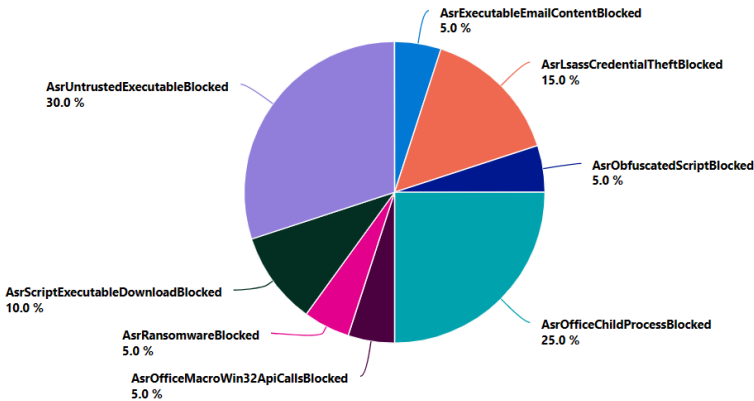


# Microsoft Defender for Endpoint, Attack Surface Reduction rules

Attack Surface Reduction (ASR) rules are a set of security policies that are designed to reduce the potential attack surface of an operating system. In this sheet, I am going to share KQL use cases with graph for ASR rules.

ActionType name	Details	Example
<b>AsrOfficeChildProcessBlocked</b>  AsrLsassCredentialTheftBlocked AsrScriptExecutableDownloadBlocked .....	These ActionTypes capture ASR rules blocking activities. In particular, if you want to capture all ASR rule activities, then the "startswith" operator is a great choice.	DeviceEvents   where Timestamp > ago(30d)   where ActionType startswith "asr"   extend Parsed = parse_json(AdditionalFields)   where Parsed.IsAudit == "false"
<b>AsrOfficeChildProcessAudited</b>  AsrLsassCredentialTheftAudited AsrScriptExecutableDownloadAudited .....	These ActionTypes capture ASR rules auditing activities. In particular, if you want to capture all ASR rule activities, then the "startswith" operator is a great choice.	DeviceEvents   where Timestamp > ago(30d)   where ActionType startswith "asr"   extend Parsed = parse_json(AdditionalFields)   where Parsed.IsAudit == "true"

```
// ASR rules blocking activities
DeviceEvents
| where Timestamp > ago(30d)
| where ActionType startswith "asr"
| extend Parsed = parse_json(AdditionalFields)
| where Parsed.IsAudit == "false"
| summarize count() by ActionType
| render piechart
```



```
// ASR rules Auditing activities
DeviceEvents
| where Timestamp > ago(30d)
| where ActionType startswith "asr"
| extend Parsed = parse_json(AdditionalFields)
| where Parsed.IsAudit == "true"
| summarize count() by ActionType
| render piechart
```

```
// A graph showing ASR rules block activities per day
DeviceEvents
| where Timestamp > ago(30d)
| where ActionType startswith "asr"
| extend Parsed = parse_json(AdditionalFields)
| where Parsed.IsAudit == "false"
| summarize Email = countif(ActionType in ("AsrExecutableEmailContentBlocked", "AsrOfficeCommAppChildProcessBlocked")),
Script = countif(ActionType in ("AsrObfuscatedScriptBlocked", "AsrScriptExecutableDownloadBlocked")),
WMI = countif(ActionType in ("AsrPersistenceThroughWmiBlocked", "AsrPsexecWmiChildProcessBlocked")),
OfficeApp = countif(ActionType in ("AsrOfficeChildProcessBlocked", "AsrOfficeMacroWin32ApiCallsBlocked",
"AsrExecutableOfficeContentBlocked", "AsrOfficeProcessInjectionBlocked")),
3rdPartyApp = countif(ActionType == "AsrAdobeReaderChildProcessBlocked"),
WindowsCredentials = countif(ActionType == "AsrLsassCredentials = "AsrLsassCredentialTheftBlocked"),
PolymorphicThreats = countif(ActionType in ("AsrUntrustedExecutableBlocked", "AsrUntrustedUsbProcessBlocked",
"AsrRansomwareBlocked", "AsrVulnerableSignedDriverBlocked")) by bin(Timestamp, 1d)
| render columnchart
```

