



Skrifstofan í skýinu



Steingrímur Óskarsson - Tæknistjóri



Skýjamyndun

 Hjá mér
 Í skýinu

On-prem

IaaS

PaaS

SaaS

| | | | |
|--------------|--------------|--------------|--------------|
| Forrit | Forrit | Forrit | Forrit |
| Gögn | Gögn | Gögn | Gögn |
| Runtime | Runtime | Runtime | Runtime |
| Middleware | Middleware | Middleware | Middleware |
| Stýrikerfi | Stýrikerfi | Stýrikerfi | Stýrikerfi |
| Hypervisor | Hypervisor | Hypervisor | Hypervisor |
| Netþjónar | Netþjónar | Netþjónar | Netþjónar |
| Gagnageymsla | Gagnageymsla | Gagnageymsla | Gagnageymsla |
| Netlag | Netlag | Netlag | Netlag |



Microsoft fends off 7 trillion cyberthreats per day

“The only way a company can process 7 trillion events per day is through automation and big data analytics” – Matthew Rathbun CISO of Microsoft Azure - 2018

Hvað er vandamálið ?

81% af fyrirtækjum sem eru hökkuð í skýinu er framkvæmt með stolnum lykilorðum eða með veikum augljósum lykilorðum sem eru marg notuð.

"Verizon breach report 2018"

“Hackers don’t break in, they login”

- CISO, Cisco

Hvað er til ráða ?

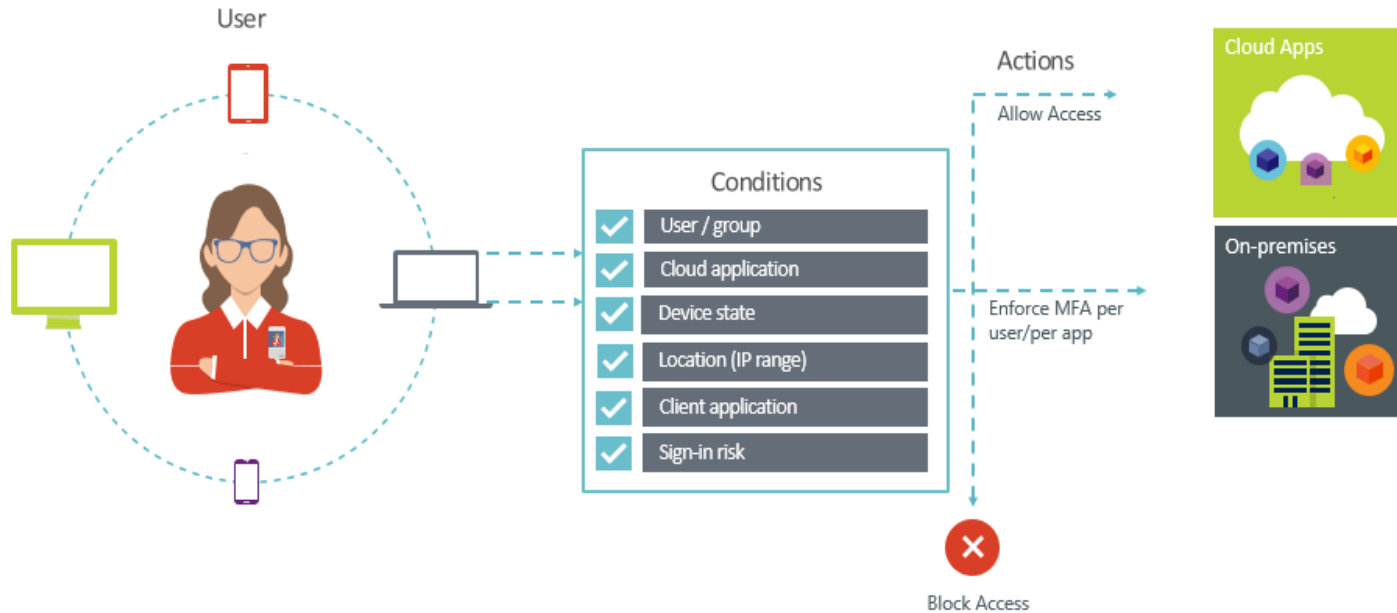
Notendanafn og lykilorð eitt og sér á aldrei að vera nóg, við viljum að meira þurfti til svo að notandinn fái aðgang (MFA, Intune, Conditional Access)

Viðkvæm gögn ber að aðgangstýra og dulkóða (Azure Information Protection)

Beinar ráðleggingar um öryggisumbætur í umhverfinu okkar. (Microsoft Defender Advanced Threat Protection)

Aukin yfirsýn á gögnum, þjónustum og öðrum skýjaþjónustum (Cloud App Security)

Azure MFA, Intune og Conditional Access.



Azure Information Protection (AIP)

Sensitivity: **Viðkvæmar innanhússupplýsingar** ✎

Viðkvæmar innanhússupplýsingar - Viðkvæm innanhússkjöl sem mega alls ekki fara út úr húsi eiga heima undir þessu öryggisstigi. Skjöl eru læst þannig að einungis Advania notendur geta lesið skjölin. Eingöngu eigandi skjalsins getur breytt því.
Áðeins hægt að lesa skjalið án netaðgangs í einn dag.
Permission granted by: steingrimur.oskarsson@advania.is

Send

To...

Cc...

Subject

Attached

 greiðsluupplýsingar.docx
65 KB

Sensitivity: **Not set** | Persónulegt | Almenn vinnuskjal | Viðkvæmar... | Viðkvæmur Póstur ~... | **[REDACTED]**

Send

To...

Cc...

Subject

FILE

MESSAGE

INSERT

OPTIONS

FORMAT TEXT

REVIEW

Clipboard

Cut
Copy
Paste
Format Painter

Calibri (Boc) 11 A⁺ A⁻ | [List Icons] | [Color Icons]

B I U [Color Icons] [List Icons] | [Align Icons]

Basic Text

Address Book
Check Names

Names

Attach File
Attach Item
Signature

Include

Follow Up
High Importance
Low Importance

Assign Policy

Tags

Policy Tip: This message may contain sensitive information. Your organization won't allow this message to be sent.

The following recipients are not authorized to receive this email. sean.mcneill@live.com ✕ sean.mcneill@catapultsystems.com ✕

To send this message, you must **override** your organization's policy.

These recipients are outside your organization: sean.mcneill@live.com ✕ sean.mcneill@catapultsystems.com ✕

Send

From: karenb@meccatapult.onmicrosoft.com

To: sean.mcneill@live.com; sean.mcneill@catapultsystems.com;

Cc:

Subject: Hush

Dan Jump's SSN 564-78-2234

Microsoft Defender ATP



Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations



NEXT GENERATION PROTECTION

Protect against all types of emerging threats



ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks



AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale



SECURITY POSTURE

Track and improve your organization security posture



ADVANCED HUNTING

Advanced threat hunting

Microsoft Defender ATP

Remediation options

Option 1 - Set the following Group Policy:

Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require use of specific security layer for remote (RDP) connections

To the following value: *SSL (TLS 1.0)*

Option 2 - Set the following registry value:

HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\SecurityLayer

To the following REG_DWORD value: *2*

Exposed machines

Cloud App Security









Safnar atvikaskráningum frá O365, öðrum kerfum og eldvegg á útstöðvum í gegnum Windows ATP

Sýnir hvaða skýjalausnir er verið að nota

Tilbúnaðar reglur fyrir óeðlilega viðburði eins og t.d. mikið magn af skjölum afritað, óeðlilegar innskráningar, mikið verið að nota skýjalausnir sem eru ekki samþykktar og margt fleira

Gefur mikinn sýnileika á hvað er að gerast í tölvukerfum fyrirtækis

Cloud App Security

| Browse by category: To | | 41 - 60 of 16,288 apps | | New policy from search + | | |
|-------------------------------------|------|--|----------------------|---------------------------------------|--------------------------|----------------|
| Search for category... | | App | Score ▼ | Actions | | |
| Hosting services | 3.2K |  Hewlett Packard Enterprise IT services | 8 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ⋮ |
| IT services | 1.8K |  Adobe Document Cloud Cloud storage | 8 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ⋮ |
| Accounting and finance | 1.4K |  Freshdesk Customer support | 8 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ⋮ |
| E-commerce | 759 |  Lithium Operations management | 8 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ⋮ |
| Business management | 734 |  Google Hangouts Personal instant messaging | 8 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ⋮ |
| Human-resource managem... | 693 |  Navex Global Security | 8 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ⋮ |
| Marketing | 623 |  SAP HANA Data analytics | 8 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ⋮ |
| CRM | 526 |  TrueScreen Human-resource management | 8 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ⋮ |
| Productivity | 517 | | | | | |
| Operations management | 470 | | | | | |
| Health | 440 | | | | | |
| Security | 418 | | | | | |
| Content management | 373 | | | | | |
| News and entertainment | 363 | | | | | |
| Collaboration | 361 | | | | | |
| Data analytics | 335 | | | | | |



Freshdesk is a cloud-based customer support software that lets you support customers through traditional channels like phone and email, social channels like Facebook and Twitter, and your own branded community.

1 GENERAL

Category: [Customer support](#)

Headquarters: [United States](#)

Data center: [United States](#)

Hosting company: [Amazon Web Services](#)

Founded: [2010](#)

Holding: [Private](#)

Domain: [1](#) [freshdesk.com](#), [freshdesk.io](#), [freshcollab.com](#)

Terms of service: [freshworks.com/terms/](#)

Domain registration: [May 10, 2004](#)

Consumer popularity: [10](#)

Privacy policy: [freshdesk.com/privacy/](#)

Login URL: [freshdesk.com/login](#)

Vendor: [Freshworks](#)

Data types: [—](#)

Disaster Recovery Plan

20 SECURITY

Latest breach: [—](#)

Data at rest encryption method: [AES](#)

Multi-factor authentication

IP address restriction

User audit trail

Admin audit trail

Data audit trail

User can upload data

Data classification

Remember password

User-roles support

File sharing

Valid certificate name

Trusted certificate

Encryption protocol: [TLS 1.2](#)

Heartbleed patched

HTTP security headers

Supports SAML

Protected against DROWN

Penetration Testing

Requires user authentication

Password policy

6 COMPLIANCE

ISO 27001

ISO 27018

ISO 27017

ISO 27002

FISMA

FISMA

GAAP

HIPAA

IAEA 3402

IFAR

SOC 1

SOC 2

SOC 3

SOX

SP 800-53

ISAE 16

Safe Harbor

PCI DSS version: [1](#)

GDPR

FedRAMP level: [Not supported](#)

CSA STAR level

Privacy Shield

FRIEC

GAPP

COBIT

COPPA

FERPA

HTRUST CSF

Tencho Forum Commitments

20 LEGAL

Data ownership

DMCA

Data retention policy: [Deleted within 3 months](#)

GDPR readiness statement


GDPR - Right to erasure

GDPR - Report data breaches

GDPR - Data protection

GDPR - User ownership

Cloud App Security – tilbúnar reglur.

| | | | | |
|---|--|---------------|---|--|
|  | Leaked credentials When cybercriminals compromise valid passwords of legitimate users, they often share those credentials. This is usually done by posting them publicly on the dark web or pa... | 0 open alerts |  |  Threat detection |
|  | Logon from a risky IP address Alert when a user logs on to your sanctioned apps from a risky IP address. By default, the Risky IP address category contains addresses that have IP address tags of Anonymo... | 0 open alerts |  |  Threat detection |
|  | Mass download by a single user Alert when a single user performs more than 10 downloads within 5 minutes. | 0 open alerts |  |  Threat detection |
|  | Publicly shared confidential files | 0 matches |  |  Compliance |
|  | Malware detection [Disabled] This detection scans files in your cloud apps and runs suspicious files through Microsoft's threat intelligence engine to determine whether they are associated with known mal... | 0 matches |  |  Threat detection |
|  | Data exfiltration to unsanctioned apps This policy is automatically enabled to alert you when a user or IP address is using an app that is not sanctioned to perform an activity that might be an attempt to exfiltrate i... | 0 open alerts |  |  Threat detection |
|  | Multiple delete VM activities This policy profiles your environment and triggers alerts when users perform multiple delete VM activities in a single session with respect to the baseline learned, which could... | 0 open alerts |  |  Threat detection |
|  | Suspicious inbox manipulation rule This policy profiles your environment and triggers alerts when suspicious inbox manipulation rules are set on a user's inbox. This may indicate that the user account is compro... | 0 open alerts |  |  Threat detection |

Cloud App Security – tilbúnar reglur.

Alerts

- Create an alert for each matching event with the policy's severity

[Save as default settings](#) | [Restore default settings](#)

- Send alert as email ⓘ

soc@advania.is ✕

- Send alert as text message ⓘ

+3548764858 ✕

Daily alert limit

- Send alerts to Flow
[Create a playbook in Flow](#)

Governance

All apps ⌵

Office 365 Require user to sign in again, Suspend user ⌵

- Suspend user
- Require user to sign in again

Erum við berskjölduð í skýinu ?



Takk fyrir.