

AZURE FRAUD PROTECTION OVERVIEW

Azure CoC



AGENDA

- ▶ Azure customers' security risks
- ▶ Azure Fraud protection measures in ACMP
- ▶ Azure Fraud monitoring and response
- ▶ Azure Fraud Protection Summary
- ▶ Azure Value-Add services campaign launch



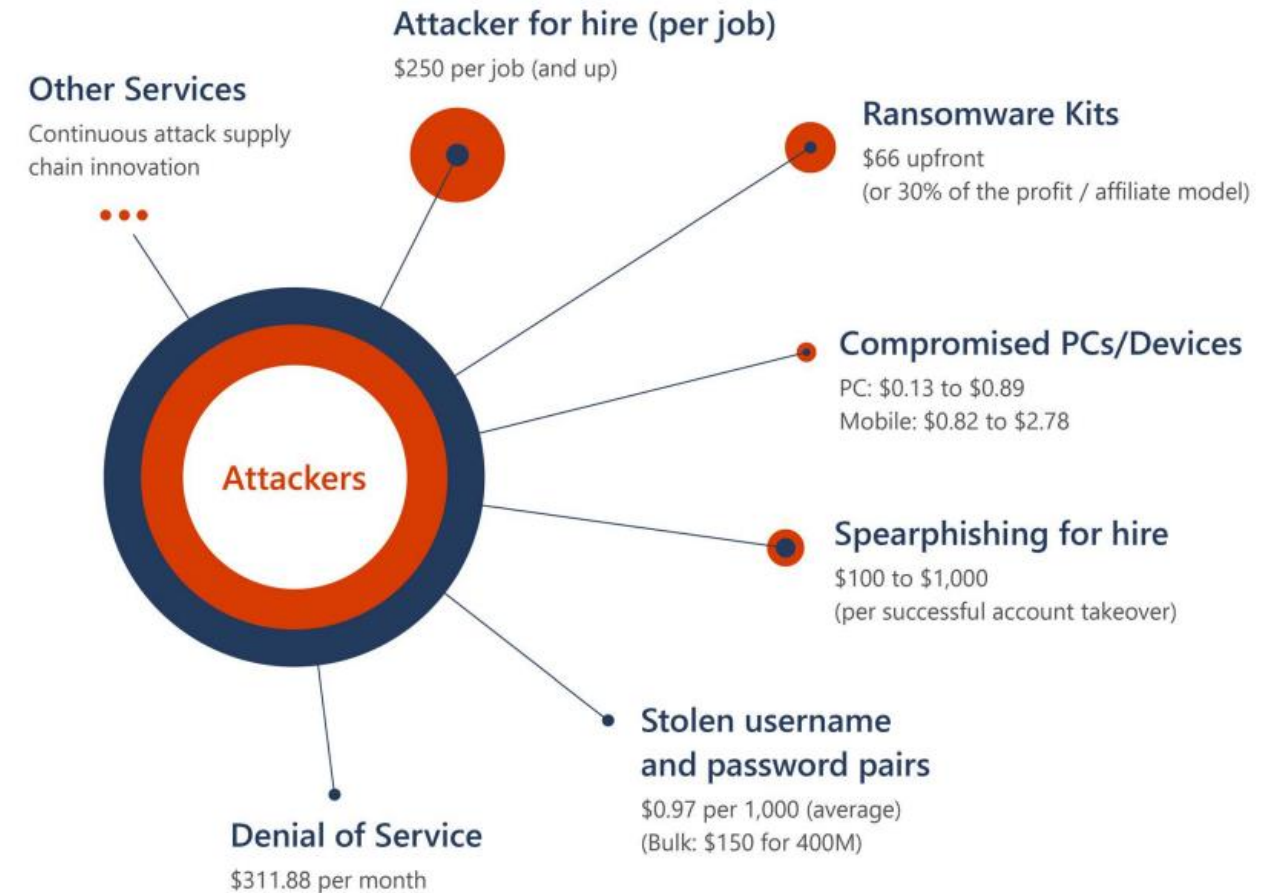
CUSTOMERS' RISKS



CYBERTHREAT: NOT IF, BUT WHEN?

- ▶ Identity and password/phishing attacks are cheap, and on the rise. Why would an attacker break in when they can log in?
- ▶ Distributed denial of service (DDoS) attacks are cheap for unprotected sites—about \$300 USD/month.
- ▶ Cobaltstrike and ransomware kits are one of the many types of attack kits designed to enable low-skill attackers to perform more sophisticated attacks.

Average prices of cybercrime services for sale




CYBERSECURITY HYGIENE

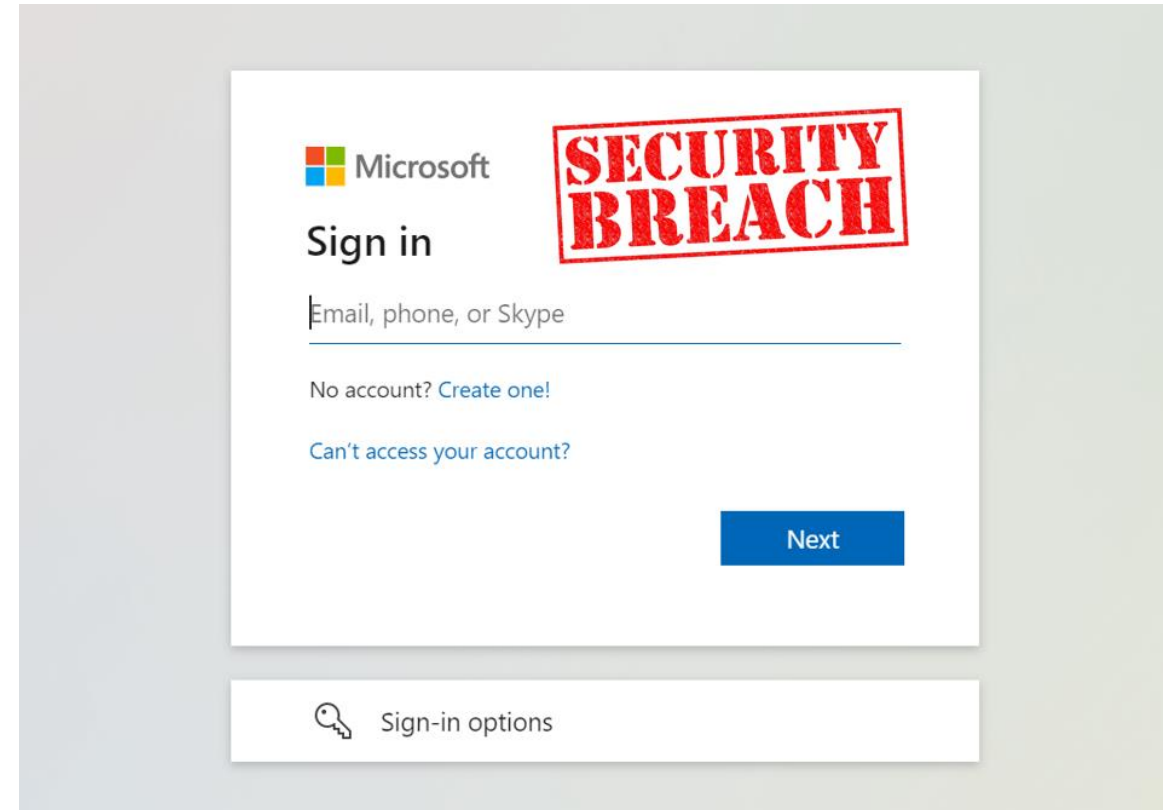
The cybersecurity bell curve:

Basic security hygiene still protects against 98% of attacks



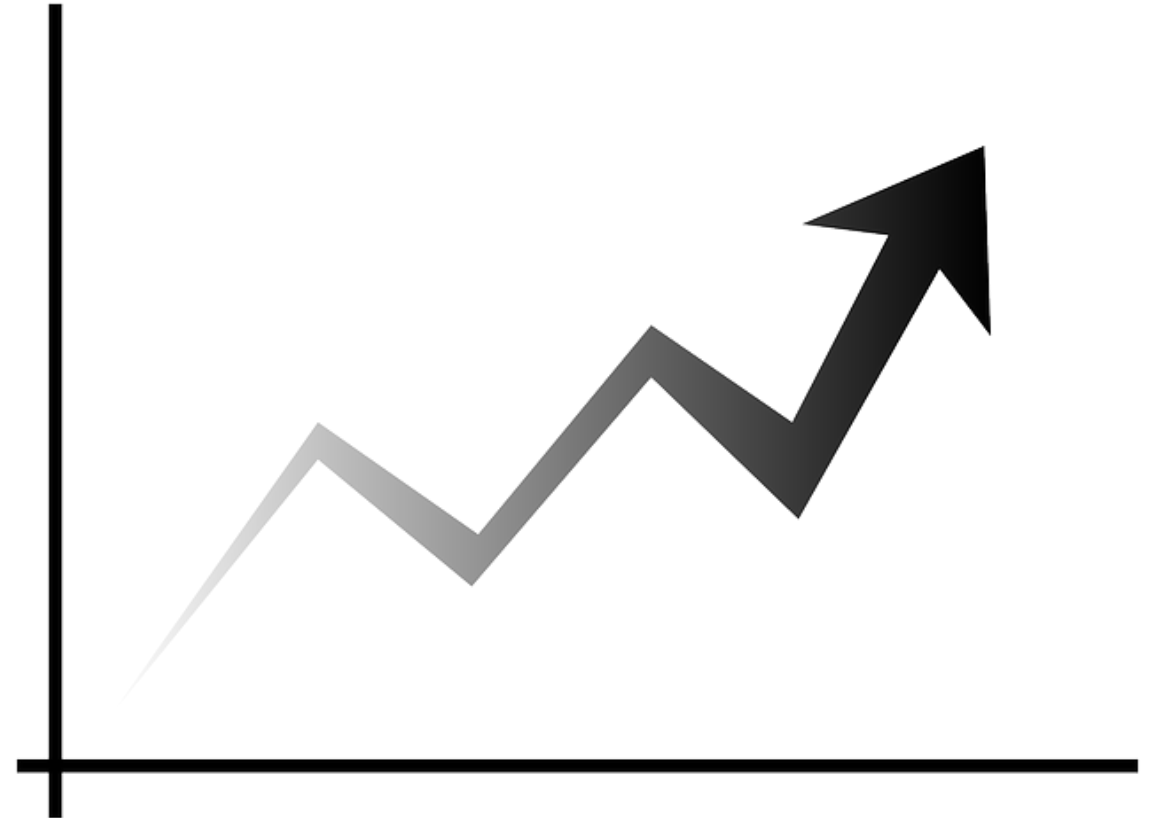
ATTACK EXAMPLE

- ▶ SMB customer
- ▶ Owner user account compromised (single authentication, no MFA/CA)
- ▶ External users invited
- ▶ Provisioning NV-series VMs -> Crypto mining
- ▶ Azure Consumed revenue 



RISKS

- ▶ Small customer = Big customer
- ▶ Azure consumption increase 1000X in days
- ▶ No credit from the Microsoft side
- ▶ End customer insolvency
- ▶ Risk to You (Partner) -> Risk to Provider
- ▶ 4 out of 5 customers have privileged accounts without MFA/CA enabled.



FRAUD PROTECTION MEASURES

- ▶ Prevent
 - ▶ Security defaults
 - ▶ Azure Policies
 - ▶ MFA validation to assign access rights during the Azure plan provisioning
 - ▶ Microsoft Security report
- ▶ Detect
 - ▶ Consumption forecast, thresholds, and notifications
 - ▶ Fraud monitoring
- ▶ Respond
 - ▶ Fraud response
 - ▶ Automation to block or revert unauthorized services





MICROSOFT SECURITY DEFAULTS



MICROSOFT SECURITY DEFAULTS

- ▶ The goal is to ensure that all organizations have at least a basic
- ▶ Security defaults make it easier to help protect your organization preconfigured security settings:
 - ▶ Requiring all users to register for Azure AD Multi-Factor Authentication
 - ▶ Requiring administrators to do multi-factor authentication.
 - ▶ Requiring users to do multi-factor authentication when necessary.
 - ▶ Blocking legacy authentication protocols.
 - ▶ Protecting privileged activities like access to the Azure portal.



MICROSOFT SECURITY DEFAULTS

▶ Who's it for?

- ▶ Organizations who want to increase their security posture, but don't know how or where to start.
- ▶ Organizations using the free tier of Azure Active Directory licensing.

▶ Who should use Conditional Access?

- ▶ If you're an organization currently using Conditional Access policies, security defaults are probably not right for you.
- ▶ If your organization has complex security requirements, you should consider Azure Active Directory Premium licenses and Conditional Access.

▶ Enabling security defaults

- ▶ If your tenant was created on or after October 22, 2019, security defaults may be enabled in your tenant. To protect all of our users, security defaults are being rolled out to all new tenants at creation.

AZURE SECURITY DEFAULTS

The screenshot shows the Azure Active Directory 'Properties' page for a tenant named 'ALSO WVD Demo (DO NOT DELETE)'. The left-hand navigation pane has 'Properties' selected. The main content area displays various tenant properties such as Name, Country or region, Location, Notification language, Tenant ID, Technical contact, Global privacy contact, and Privacy statement URL. At the bottom of this section, there is a link 'Manage security defaults' which is circled in red. To the right of the properties, a panel titled 'Enable security defaults' contains a description of security defaults and a toggle switch labeled 'Enable security defaults', which is also circled in red.

This is a simulated email from Microsoft. The header shows the Microsoft logo and the email address 'kelly@outlook.com'. The subject is 'Reduce the risk of attack'. The body text states: '99.9% of organization account compromise could be stopped by using multifactor authentication. Enable security defaults to apply Microsoft's best security practices.' It then says 'Once enabled' and 'We will ask everyone in you organization to register for multifactor authentication on the Microsoft Authenticator app.' A grey box below this text says 'Security defaults will be enabled automatically for your organization in 14 days.' At the bottom are two buttons: 'Ask later' and 'Enable security defaults'.

This is a simulated notification window from Microsoft Azure. It has a blue header with the Microsoft Azure logo. The main text says 'More information required' and 'Your organization needs more information to keep your account secure'. It offers a link to 'Skip for now (14 days until this is required)' and another to 'Use a different account'. There is a 'Learn more' link and a 'Next' button at the bottom right.



AZURE POLICIES



AZURE POLICIES

- ▶ Preventive measures for deploying high-cost Virtual Machines:
 - Prevent deployment of Standard_N GPU family of virtual machines
 - Prevent deployment of Standard_H family of virtual machines
 - Prevent deployment of Spot virtual machines
 - Prevent deployment of Azure batch accounts
 - Prevent deployment of new Virtual machine scale sets
- ▶ Deployed in a way to prevent exceptions from compromised global admin accounts
- ▶ Deployed for all (existing and new) Azure Plan subscriptions
- ▶ Will not stop or interfere with existing virtual machines in the subscription
- ▶ Timed exceptions for the deployment of new virtual machines
- ▶ Timed exceptions will be initiated from ACMP (UI or API) with full logging





MFA VALIDATION



MFA VALIDATION

- ▶ Prevent granting access rights to users without MFA enabled
- ▶ We prevent Azure provisioning if we can't check MFA statuses.

The screenshot shows the 'Permissions Management (END CUSTOMER)' section of the Azure Plan (Microsoft) interface. The interface has a top navigation bar with tabs: 'Select service', 'Terms and Conditions', 'Configuration', 'Permissions' (active), and 'Order review'. Below the navigation bar, the title 'Azure Plan (Microsoft)' is followed by a dropdown arrow and 'PERMISSION MANAGEMENT (END CUSTOMER)'. The main content area is divided into several sections:

- Grant End Customer Permissions ***: A checkbox is checked. Below it, a note states: 'Use this checkbox to add endcustomer permissions. If you do not wish to add customer permissions simply uncheck the checkbox.'
- Permission information (End Customer)**: A text block stating: 'Below you can see all the users of the end customer company admin group. Please select the users that should get AOBO rights to the initial subscription created during Azure Plan creation.'
- Permission level (End Customer) ***: A dropdown menu is set to 'Owner'.
- Assignee (End Customer) ***: A text block stating: 'Users are being populated based on following rules:' followed by a list of rules:
 - Only user that are members of the Global administrator group are considered.
 - Only users that have a completed MFA configuration will be displayed.
 - Only authenticator applications are considered as a secure MFA configuration
 - Users with MFA set up using SMS or Phone will not be displayed.
 - No users will be displayed if customer has removed indirect provider permissions.
- Available items**: A list box with a search bar and a 'Select all' link at the bottom.
- Selected items**: A list box with a search bar and a 'Select all' link at the bottom.

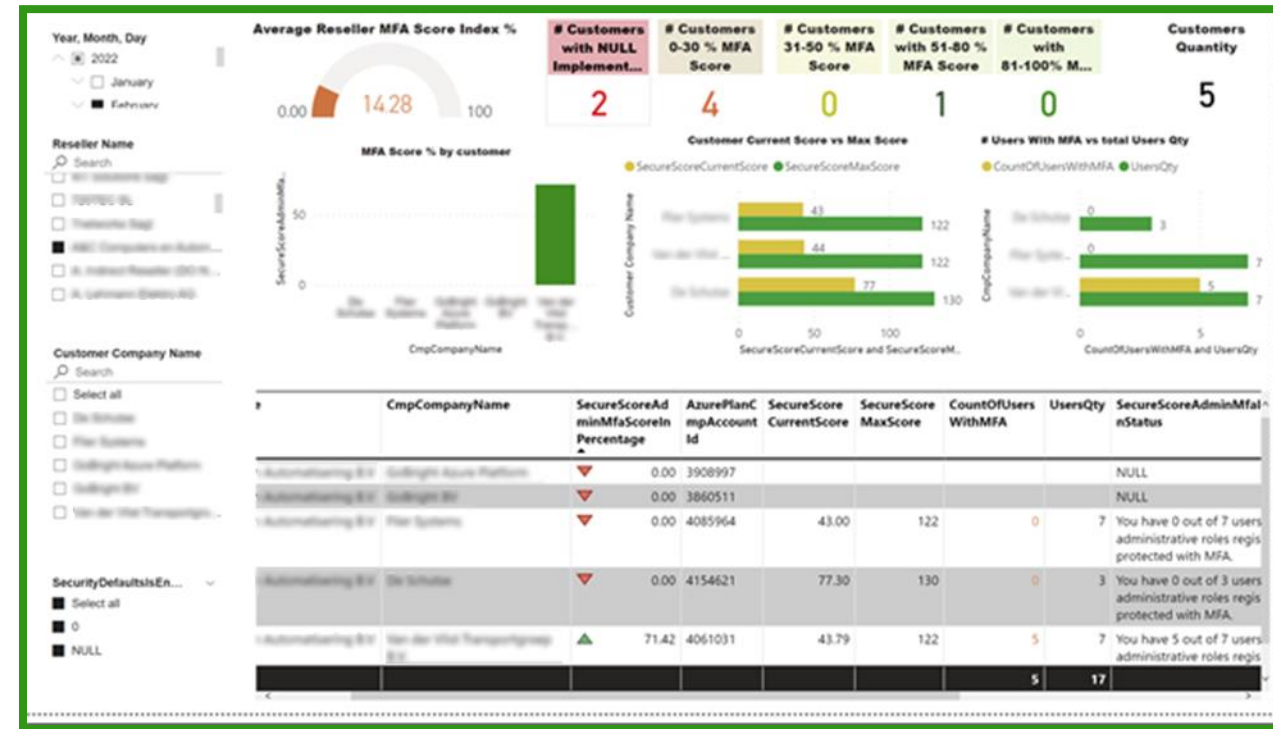


MICROSOFT SECURITY REPORT



MICROSOFT SECURITY REPORT

- ▶ Partner-level report in ACMP
- ▶ Overview of MFA and security score on partner level
- ▶ MFA and security score details on the customer level
- ▶ Updated on a scheduled basis (3 times per week)





AZURE CONSUMPTION FORECAST AND THRESHOLD



THRESHOLDS, FORECAST, AND NOTIFICATIONS

- ▶ View a monthly forecast indicating the consumption trend for your Azure Plan subscription
- ▶ Create a threshold limit that triggers an email notification, if predicted to be exceeded
- ▶ Updated four times a day

CONFIGURATION

PERMISSIONS

AZURE INSIGHTS FOR ENDCUSTOMER

SERVICE INFO

AVAILABLE

</

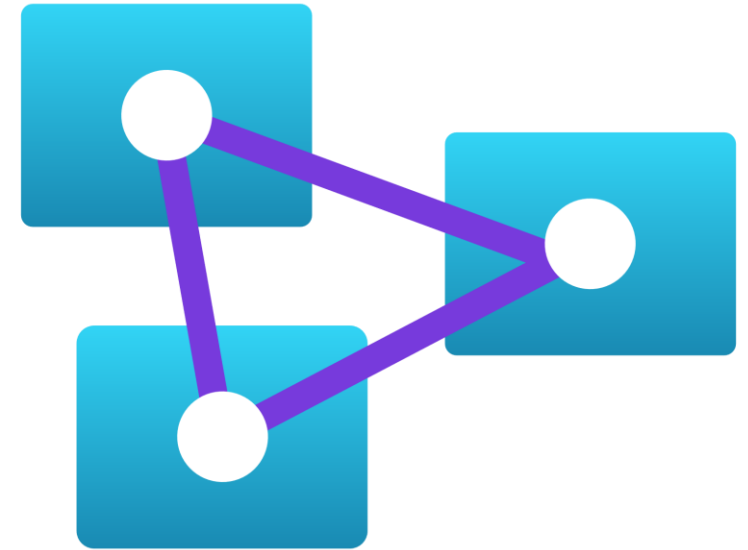


FRAUD MONITORING AND RESPONSE



FRAUD MONITORING AND RESPONSE

- ▶ Detect events inside Azure subscriptions
- ▶ Analyse events and resources
- ▶ Display fraud monitoring results in a dashboard
- ▶ Flagged fraud events are mitigated by Also Azure support team involving Microsoft, the partner, and the customer



FRAUD MONITORING AND RESPONSE



ALSO CLOUD MARKETPLACE FORECAST ALERT

YOUR SET AZURE PLAN THRESHOLD HAS BEEN EXCEEDED. THIS IS NOT AN INVOICE. BELOW IS A SUMMARY OF CURRENT CONSUMPTION. EXPECTED TOTAL BY END OF MONTH IS ON THE BOTTOM OF PAGE.

Azure subscription	Azure subscription id	Service Name	Resource Type	End Customer Total
Azure_		Visual Studio Subscription	marketplace/account	37878.08
Azure_		SQL Database	microsoft.sql/servers	310.09
Azure_		Log Analytics	microsoft.insights/components	0
Azure_		Advanced Data Security	microsoft.sql/servers	0
Azure_		Bandwidth	microsoft.storage/storageaccounts	0
Azure_		Storage	microsoft.storage/storageaccounts	0
Azure_		Azure App Service	microsoft.web/sites	0
Azure_		Bandwidth	microsoft.web/sites	0
Azure_		Functions	microsoft.web/sites	0

Current endcustomer charges: 38188.17 NOK
Forecasted endcustomer total: 38206.45 NOK



QUESTIONS & ANSWERS



LINKS

Strengthen cybersecurity with a free subscription to Azure AD Premium Plan 2

<https://docs.microsoft.com/en-us/partner-center/announcements/2021-october#12>

Introduction to granular delegated admin privileges (GDAP)

<https://docs.microsoft.com/en-us/partner-center/gdap-introduction>

Security defaults in Azure AD

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

Thresholds on azure plan subscriptions in ACMP

<https://support.ccpaas.net/display/ACA/Create+usage+threshold+for+Azure+Plan>

How to manage Azure policies in ACMP:

<https://support.ccpaas.net/display/ACA/Manage+Azure+fraud+policy>

Microsoft Security Report in ACMP:

<https://support.ccpaas.net/display/ACA/Microsoft+Security+Report>

Application and service principal objects in Azure Active Directory

<https://learn.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals>

