



LAKEFOREST

C O N S U L T I N G



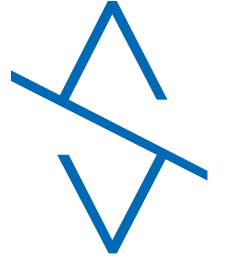
LAKEFOREST

C O N S U L T I N G

Azure Security

Kaido Järvemets

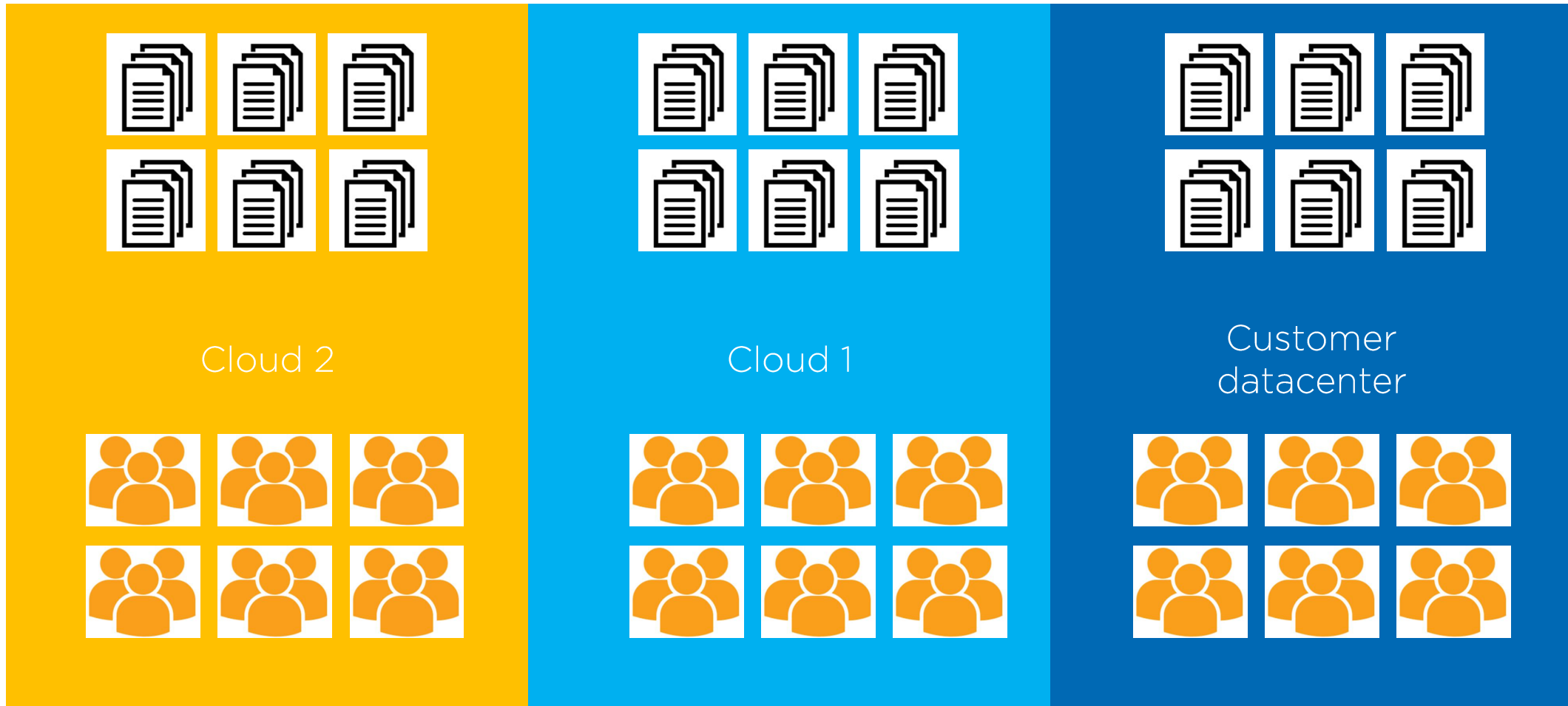
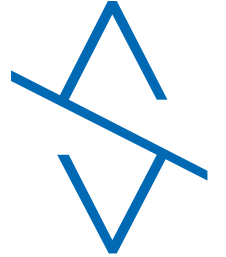
Life before cloud



Customer datacenter



Life with different cloud services



RANSOMWARE ATTACK



You only have 3 days to submit the payment, or your files will be lost.

Time Left

02:23:59:06



2. December 2020, 10:21 AM
3 min reading

Cybercriminals attack three ministries

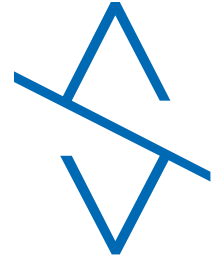


Karel Reisenbuk



Head of RIA's cybersecurity service Lauri Aasmann described all three attacks as very serious incidents.
PHOTO: Mihkel Maripuu

The State Information System's Authority (RIA) discovered three similar attacks against Estonian IT infrastructure in November that also left perpetrators with people's personal information. The Health Board will notify people whose data was compromised.





BleepingComputer ✓

@BleepinComputer

Ransomware threat surge, Ryuk attacks about 20 orgs per week -
[@Ionut_Ilascu](#)



Ransomware threat surge, Ryuk attacks about 20
orgs per week
bleepingcomputer.com

Microsoft: Some ransomware attacks take less than 45 minutes

Microsoft goes over the recent malware trends in its new "Digital Defense Report."



By [Catalin Cimpanu](#) for [Zero Day](#) | September 29, 2020 --
15:33 GMT (16:33 BST) | Topic: [Security](#)

Monthly volume and diversity of signals used by Microsoft security operations

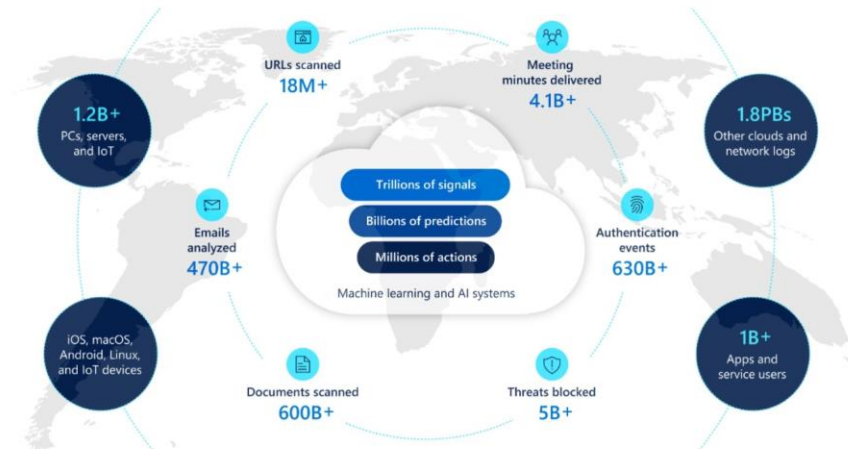
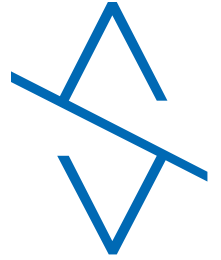


Image: Microsoft

2500 dollars only for DA account!



SELLING Access to Australia Insurance Corp Network
by itrade4living - 10 hours ago



itrade4living

M.V.P User

10 hours ago

Selling Access to Australia Insurance Corp Network - Domain Admin Authority.

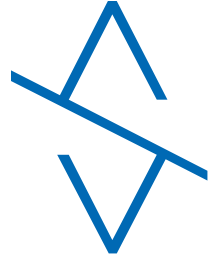
(US \$5.46bn INSURANCE PREMIUM WRITTEN PER ANNUM ACROSS WBN)

Price \$2500

Escrow accepted

PM if interested

Internal threats



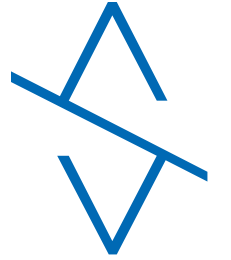
Cisco engineer resigns then nukes 16k WebEx accounts, 456 VMs



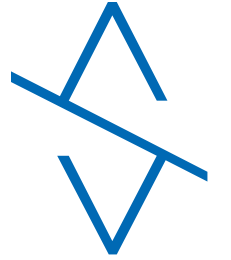
By [Sergiu Gatlan](#)

August 28, 2020 10:30 AM





What can we do to avoid such incidents?



In most of the cases we are
failing to detect known attack
frameworks and tools!

Most of the customers



Solution A

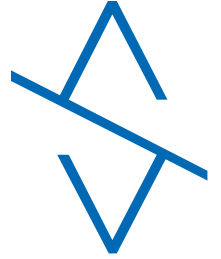
Solution B

Solution C

Solution D

No integration between the solutions

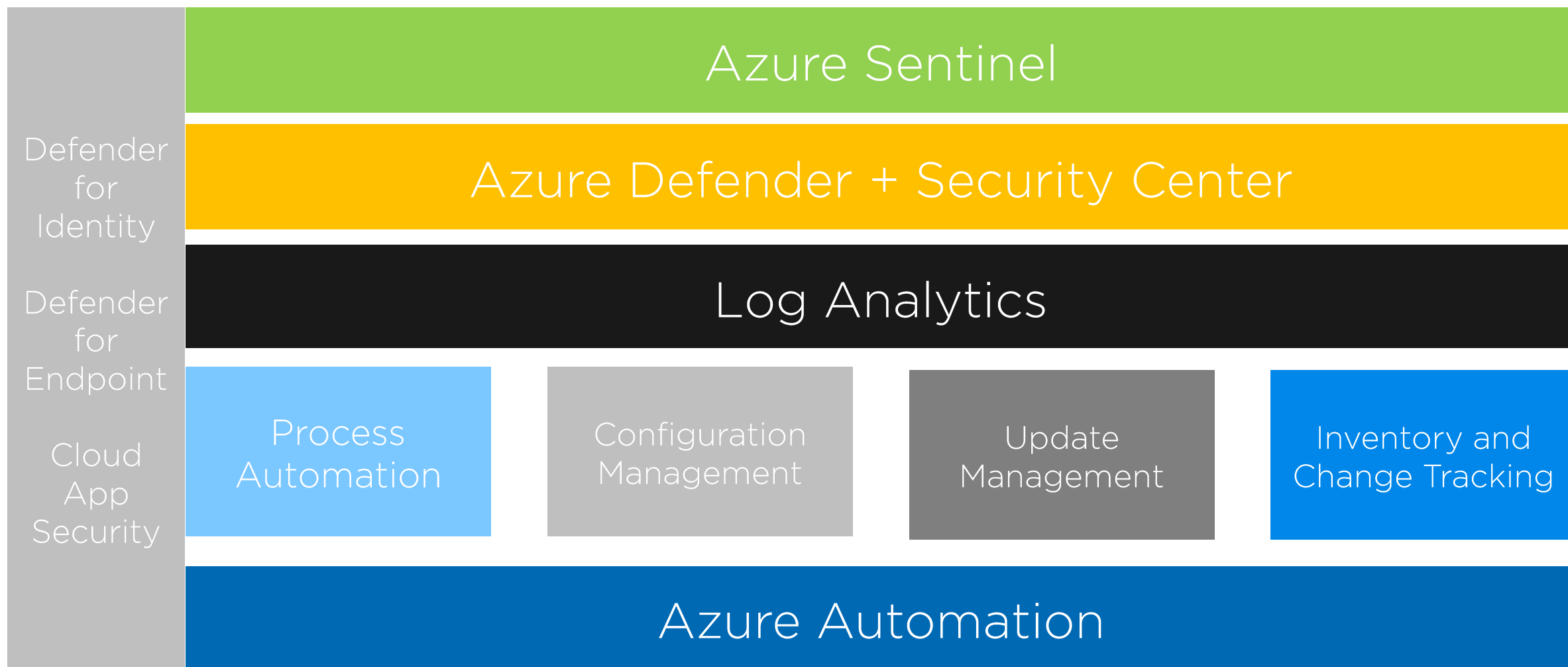
From Azure....



- We can implement different security and management solutions and we are able to get full visibility across the datacenters
 - All solutions are fully integrated each other – just plug and play
 - We can cover every single endpoint and server in a datacenter
 - Not only limited with a customer datacenter(s)
- Security is built-in, not Bolted on
- It is easy to scale out and in
- Easy to implement and small customer footprint
- We can provide tools for the whole IT department! Not only for security department



Azure Security and Management Solutions



360-degree overview

Azure Active Directory

Defender for Identity

Azure Automation

Defender for Endpoint

Log Analytics

Defender for Cloud Apps

Defender for Cloud

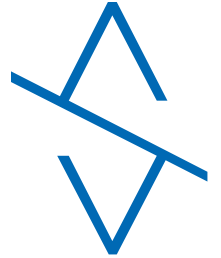
Microsoft Sentinel





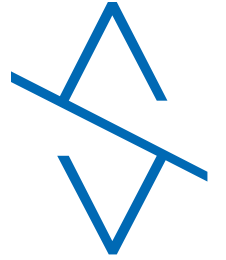
What have we
learned?

Key learning points

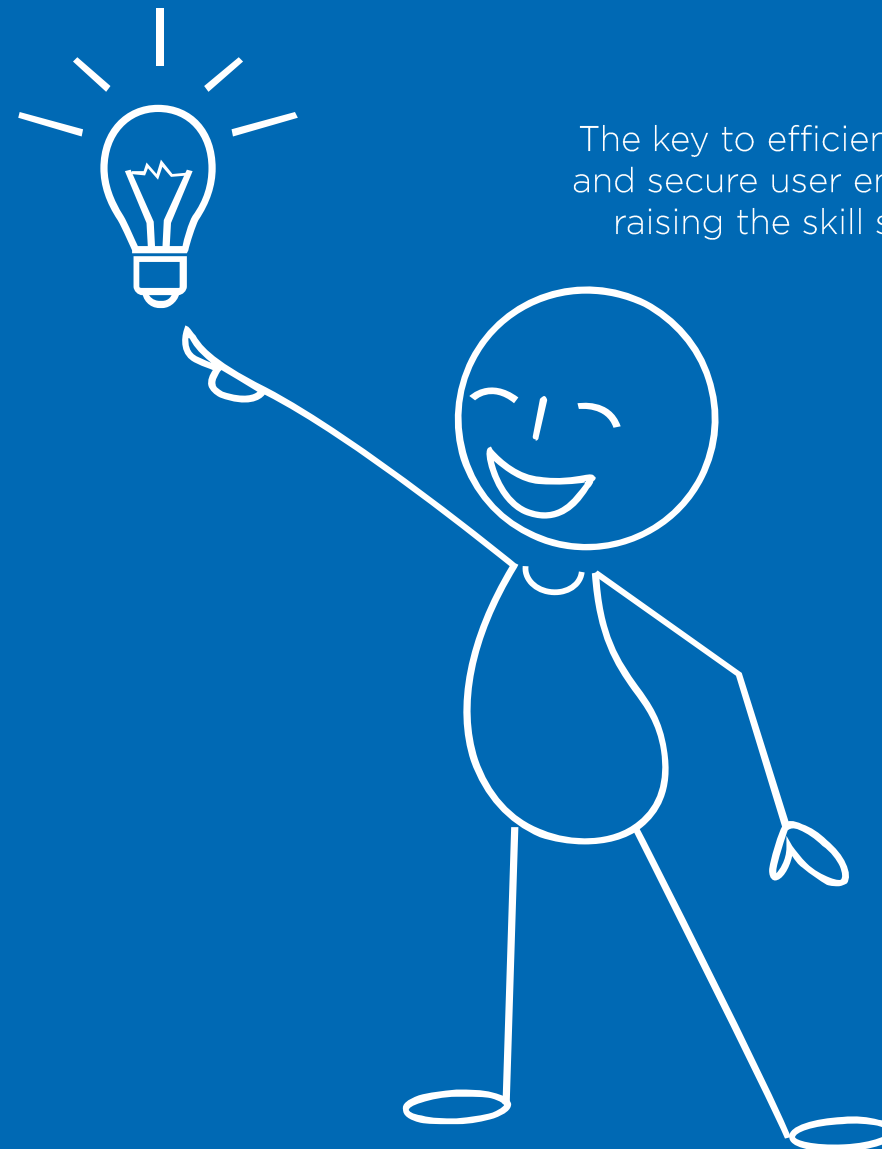
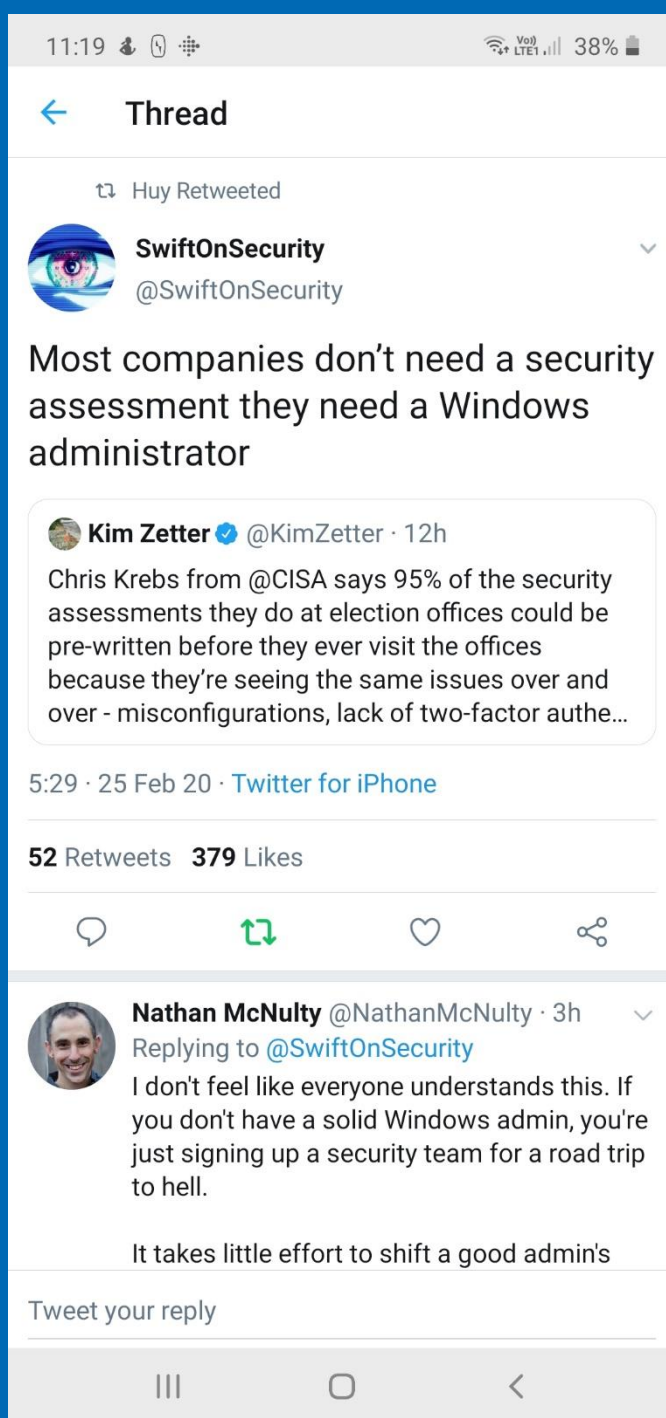


- Increased overview and 24/7 Monitoring
 - Cloud and on-premises
- Better risk management
 - Defender for Cloud – CIS benchmarks
 - Defender for Endpoint - Threat and Vulnerability Management
- Improved security
 - 360-degrees overview – every server and device is covered
- Better resource management
 - We know our pain points and it is easier to track changes and improvements

Key learning points #2



- Better overview about Shadow IT
 - Defender for Endpoint and Defender for Cloud Apps
- We have managed to detect different attack
 - Internal and external ones (for example HAFNIUM etc)
- Improved patching and datacenter management
- Better incident management across the company
- More efficient compared to the on-premises solutions



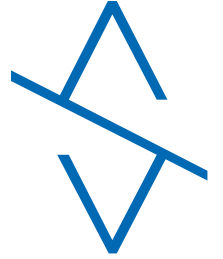
The key to efficient, effective, consistent, and secure user environment begins with raising the skill set of administrators!





What are the
benefits?

Benefits



- Defender for Endpoint
- Defender for Cloud
- Microsoft Sentinel



Better
Secure Baseline

Recommendations

Are we good?



RESOURCE SECURITY HYGIENE

Recommendations

Compute & apps

Networking

IoT Hubs & resources

Data & storage

Identity & access

Security solutions

ADVANCED CLOUD DEFENSE

Adaptive application controls

Just in time VM access

Adaptive network hardening

File Integrity Monitoring

THREAT PROTECTION

Security alerts

Security alerts map (Preview)

Is the new Secure Score preview experience clear to you? ☐ Yes ☐ No

Increase your score by remediating the recommendations within the controls below. To get the max score, fix all recommendations for all resources in a control.

Search recommendations

Controls

> Enable MFA

> Remediate security configurations

Monitoring agent should be installed on your machines Completed

Vulnerabilities in security configuration on your machines should be remediated

> Apply system updates

> Enable auditing and logging

> Implement security best practices

> Encrypt data in transit Completed

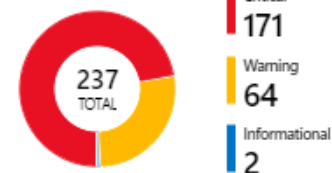
> Apply adaptive application control Completed

> Enable encryption at rest Completed

> Enable endpoint protection Completed

> Manage access and permissions Completed

Failed rules by severity



Operating system (237) Web (0)

Search recommendations...

Ccelid	↑↓	Name
AZ-WIN-00026		Ensure 'Audit Group Membership' is set to 'Success'
AZ-WIN-00088		Windows Firewall: Domain: Allow unicast response
AZ-WIN-00088		Windows Firewall: Domain: Allow unicast response
AZ-WIN-00089		Windows Firewall: Private: Allow unicast response
AZ-WIN-00089		Windows Firewall: Private: Allow unicast response
AZ-WIN-00090		Windows Firewall: Public: Allow unicast response
AZ-WIN-00090		Windows Firewall: Public: Allow unicast response
AZ-WIN-00111		Audit MPSSVC Rule-Level Policy Change
AZ-WIN-00111		Audit MPSSVC Rule-Level Policy Change

Automated audits

CIS 1.1.0, ISO 27001, etc



Security Center | Regulatory compliance

Search (Ctrl+/) «

Download report Manage compliance policies

Regulatory compliance assessment

Regulatory standards compliance status

Azure CIS 1.1.0 (New) 15 of 28 passed controls

Azure CIS 1.1.0 11 of 14 passed controls

PCI DSS 3.2.1 10 of 38 passed controls

SOC TSP 1 of 13 passed controls

To add regulatory compliance standards, click Manage compliance policies above. [Send us feedback](#)

Azure CIS 1.1.0 PCI DSS 3.2.1 ISO 27001 SOC TSP Azure CIS 1.1.0 (New)

Under each applicable compliance control is the set of assessments run by Security Center that are associated with that control. If they are all green, it means those assessments are currently passing; this does not represent a partial view of your overall compliance status.

☐ Expand all compliance controls

1. Identity and Access Management

2. Security Center

3. Storage Accounts

4. Database Services

5. Logging and Monitoring

6. Networking

7. Virtual Machines

8. Other Security Considerations

9. AppService

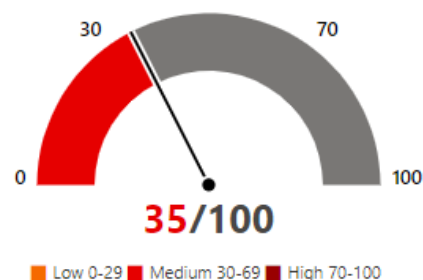
Defender for Endpoint



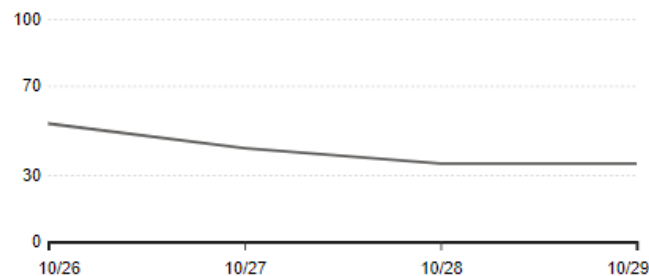
Organization exposure score

Exposure score

This score reflects the current exposure associated with devices in your organization ⓘ



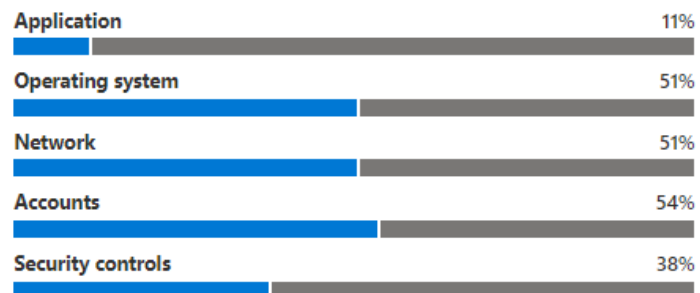
Exposure score over time ▼ 18 Last 4 days



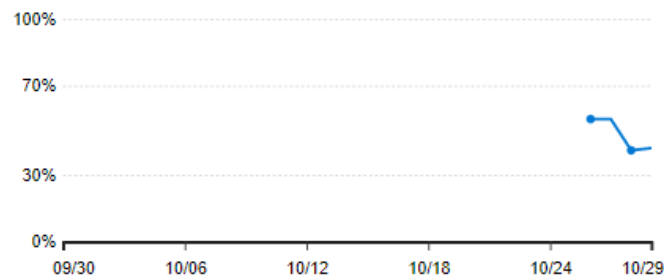
Microsoft Secure Score for Devices

Your score for devices: 42% 271 / 653

This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls ⓘ



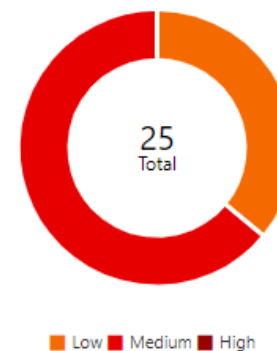
Your score for devices over time ▼ 13 Last 4 days



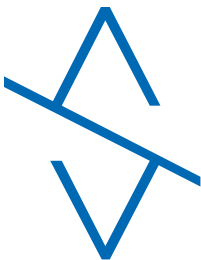
Device exposure distribution

Exposure distribution

Exposed devices are easy targets for cybersecurity attacks. Ensure that these devices can receive security updates, have critical security controls, and are properly configured.



Defender for Cloud Apps



Cloud Discovery

[?](#) [Continuous report](#) Win10 Endpoint Users [Timeframe](#) Last 30 days [⋮](#)

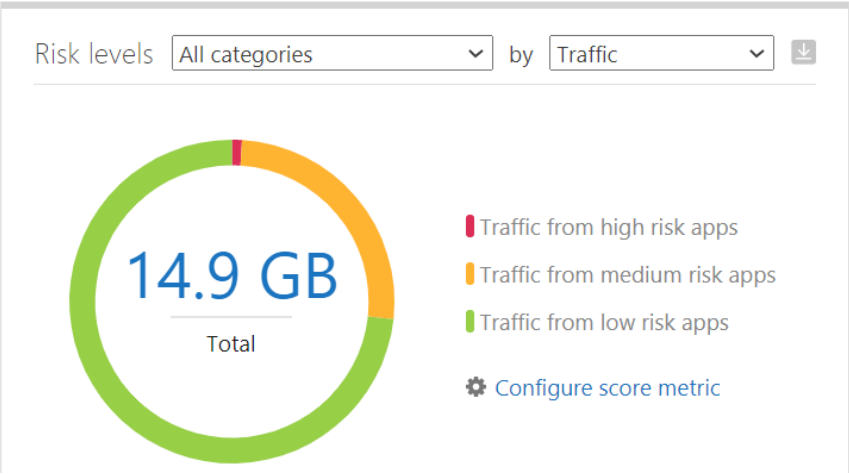
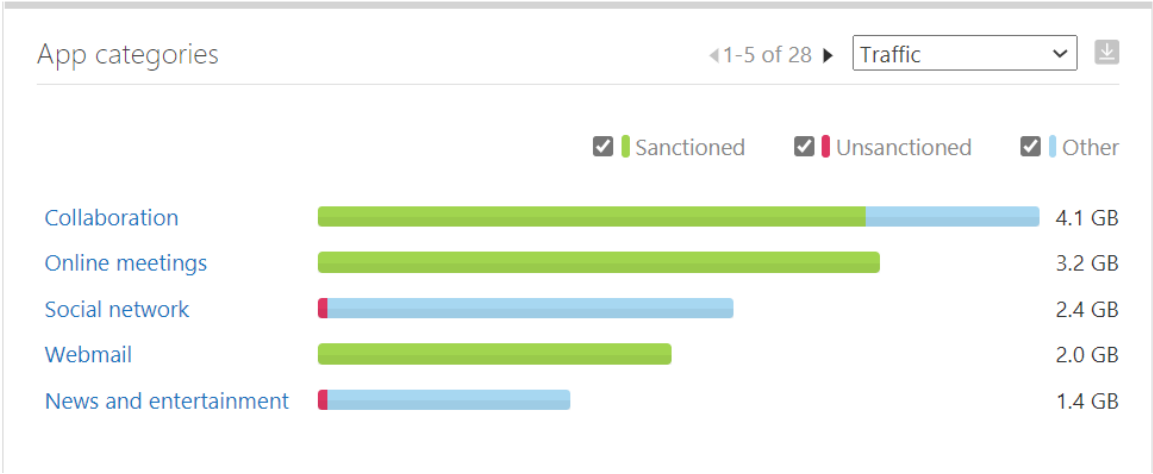
Dashboard	Discovered apps	IP addresses	Users	Devices	Updated on Oct 30, 2020
-----------	-----------------	--------------	-------	---------	-------------------------

Apps	IP addresses	Users	Devices	Traffic
40	59	6	6	14.9 GB ↑ 5.7 GB ↓ 9.2 GB

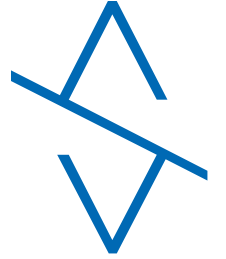
Cloud Discovery open alerts [+ Create policy](#)

2 Cloud Discovery alerts

0 Suspicious use alerts

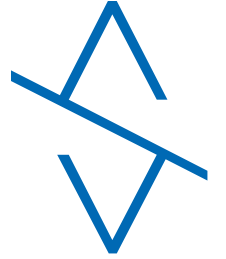


Defender for Cloud Apps #2



App	Score ▼	Traf...	Upload	Transa...	Users	IP add...	Devices	Last seen...	Actions
 Microsoft Shar... Collaboration	10	3.1 GB	2.4 GB	1.2K	3	16	3	Oct 30, 2...	  
 Microsoft Offi... Productivity	10	467 KB	34 KB	2	1	1	1	Oct 6, 2020	  
 Microsoft Exch... Webmail	10	2.0 GB	787 MB	11.6K	5	52	6	Oct 30, 2...	  
 Microsoft One... Cloud storage	10	333 KB	—	10	2	2	2	Oct 30, 2...	  

Microsoft Sentinel Workbooks



Insecure Protocols

Subscription

Visual Studio Ultimate wit... ▼

Workspace

visualAuditing ▼

TimeRange

Last 24 hours ▼

Show Help ⓘ

Yes

No

Change Log

Summary



LDAP

NTLM

SMB

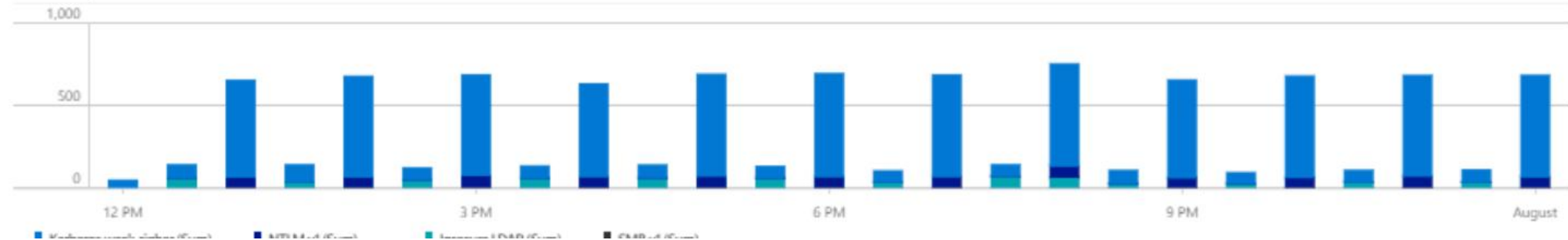
Kerberos

WDigest

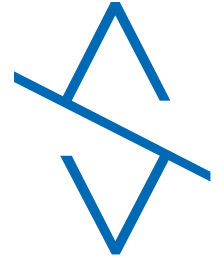
AAD Legacy Auth

Group: Summary

Summary of Insecure Protocols: Last 24 hours



Update Management



Home > Resource groups > RG-PROD-IT-AZ-MANAGEMENT-TIER-0-WE > PROD-IT-TIER-0-AUTOMATION-WE



PROD-IT-TIER-0-AUTOMATION-WE | Update management

Automation Account

Search (Ctrl+/)



Schedule update deployment



Add Azure VMs



Add non-Azure machine



Manage machines



Overview



Activity log



Access control (IAM)



Tags



Diagnose and solve problems

Configuration Management



Inventory



Change tracking



State configuration (DSC)

Update management



Update management

Non-compliant machines ⓘ

1
out of 1

Machines need attention (1) ⓘ

Critical and security
Other
Not assessed

1
0
0

Missing updates (13)

Critical
Security
Others

4
2
7

Failed update deployments ⓘ

4
out of 4 in the past thirty
days

Machines (1)

Missing updates (13)

Deployment schedules

History

Filter by name

Compliance: All



Platform: All



Operating system

Machine name

Compliance

Platform

Operating system

Critical missing up...

Security missing u...

DC01.LakeForestConsultin ⓘ Non-compliant
Azure Arc: RG-PROD-IT-Az as of 10/30/2020, 6:38

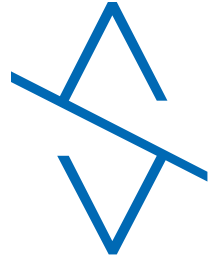
Non-Azure

Windows

4

2

Inventory and Change tracking



[Home](#) > [Resource groups](#) > [RG-PROD-IT-AZ-MANAGEMENT-TIER-0-WE](#) > [PROD-IT-TIER-0-AUTOMATION-WE](#)



PROD-IT-TIER-0-AUTOMATION-WE | Inventory

Automation Account



+ Add Azure VMs

[Add non-Azure machine](#)

[Manage machines](#)

[Log Analytics](#)

[Edit Settings](#)

+ Create



Overview



Activity log



Access control (IAM)



Tags



Diagnose and solve problems

Configuration Management



Inventory



Change tracking

New software ⓘ

1

Last 24 hours

Machines reporting ⓘ

1

Last 24 hours

Machines(1)

Software(55)

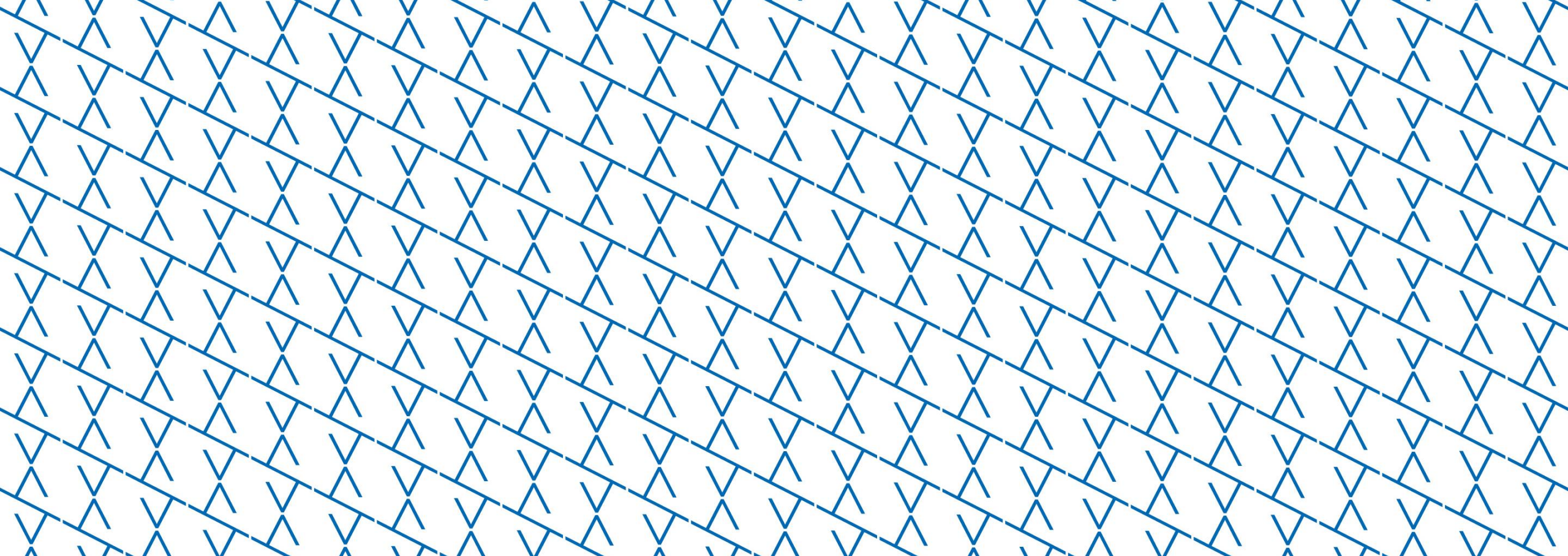
Files(0)

Windows Registry(130)

Windows Services(222)

Linux Daemons(0)

Machine	Operating System	Version	Platform
DC01.LakeForestConsulting.com	Windows	10.0	Non-Azure



DEMO: Azure Security



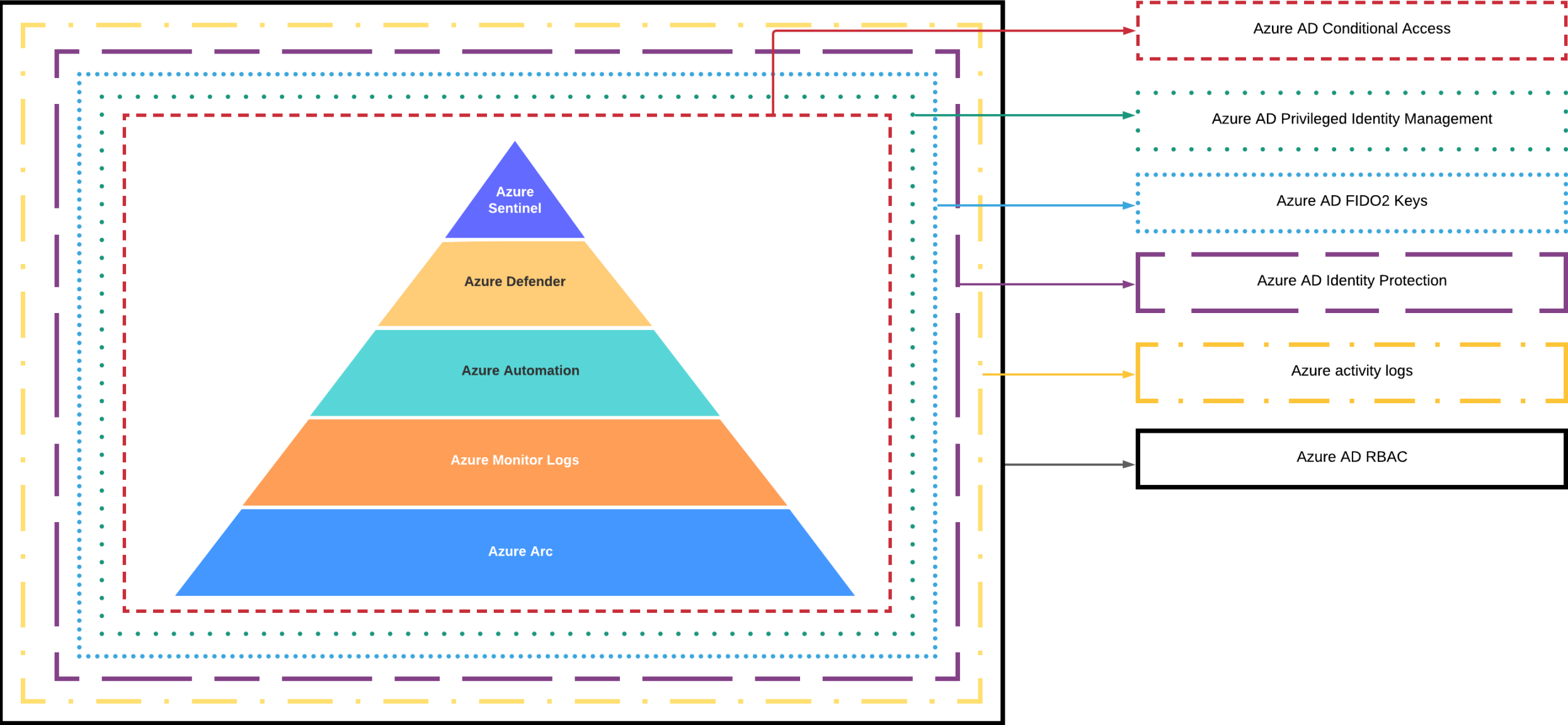


Protecting the Keys to the Kingdom

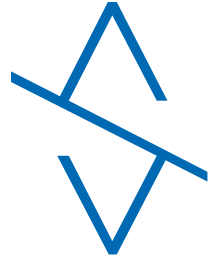
Azure Administrative Model

Azure Administrative model

Kaido Järvemets

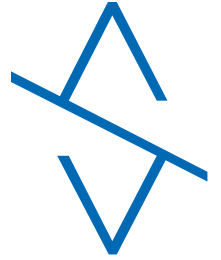


Protecting the Kingdom



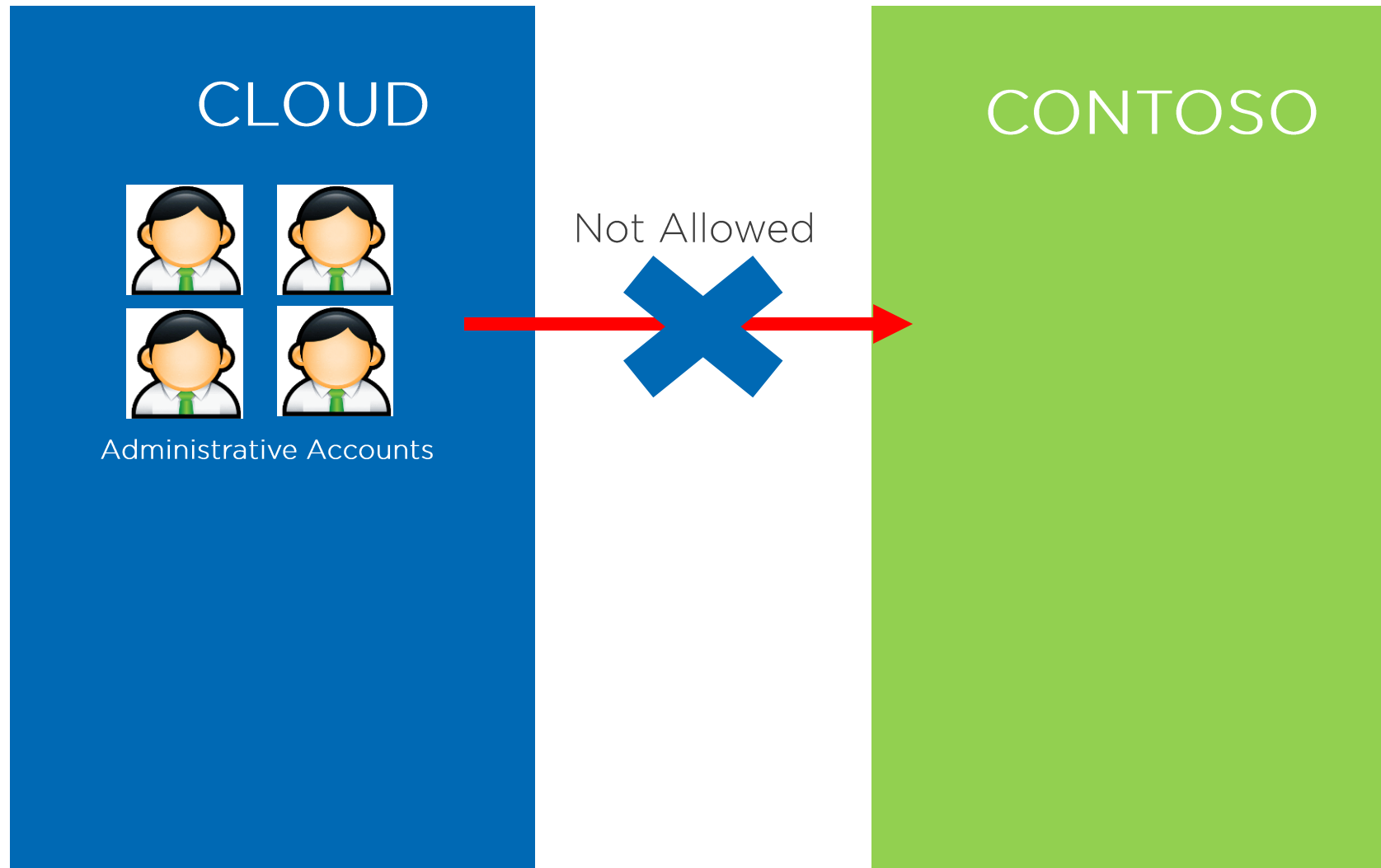
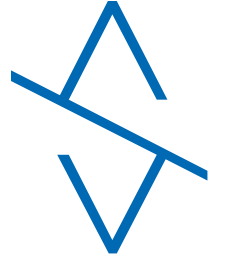
- What do we want?
 - Every administrator is a standard user
 - Access to data and services requires you do request permissions
 - Highly privileged permissions are only with approvals
 - Every action and query is audited

Protecting the Kingdom #2

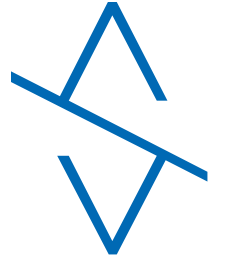


Service	Azure AD Premium P2 / Microsoft 365 E5 / Enterprise Mobility +Security E5	Azure AD Premium P1 / Microsoft 365 E3 / Enterprise Mobility +Security E3
Conditional Access	Yes	Yes
Multi-factor Authentication	Yes	Yes
Identity Protection	Yes	No
Privileged Identity Management	Yes	No

Protecting the Kingdom #3



Protecting the Kingdom #4



Privileged Identity Management

Identity Protection

Conditional Access

Multi-factor
Authentication



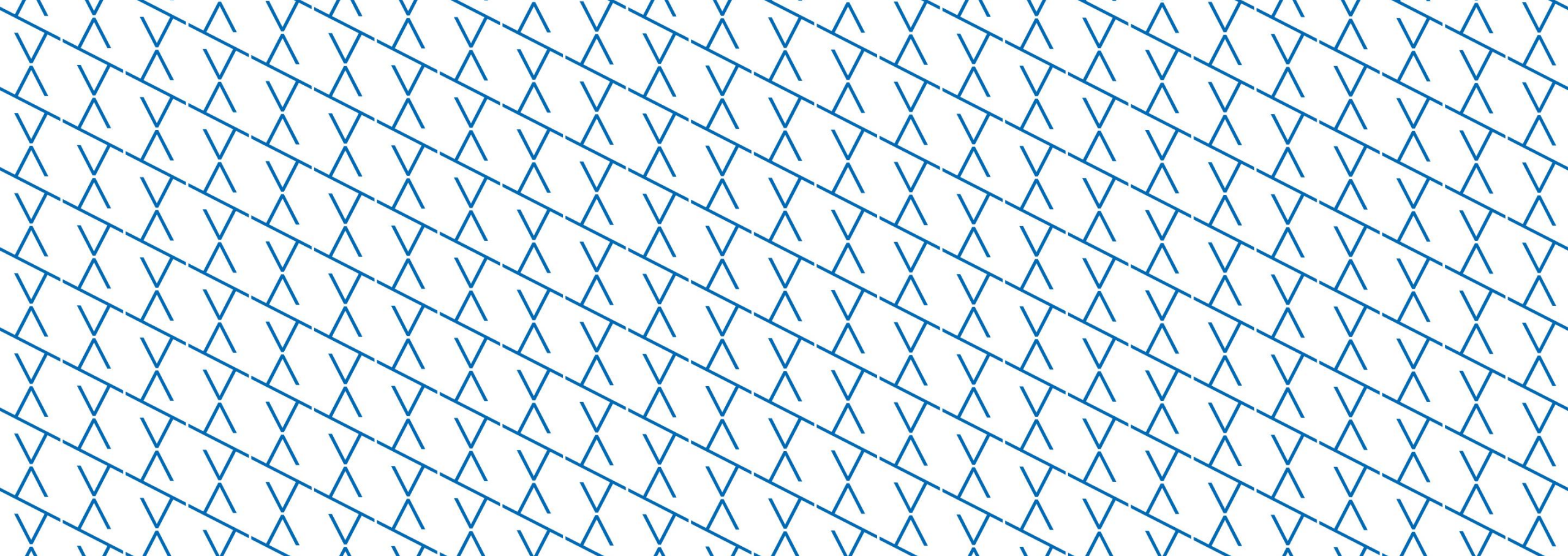


Protect your digital world with YubiKey

Stop account takeovers, go passwordless and modernize your multifactor authentication. Get the world's leading security key for superior security, user experience and return on investment.

[Watch video](#)

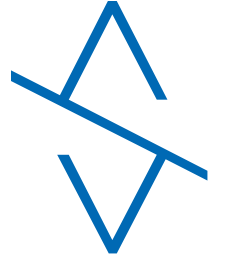




DEMO: Protecting the Kingdom



Our proposal



- Conduct 3 months Proof of Value
- You will learn what you can really do with Azure security and management solutions
 - Better understanding and overview
 - How Microsoft does thing differently
 - Weak points and how to improve internal security



```
operation = "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation = "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation = "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True  
  
selection at the end - add  
ob.select= 1  
when ob.select=1  
text.scene.objects[0].name  
"Selected" + str(modifier  
copy.context.selected  
data.objects[0].name  
print("please select exactly  
OPERATOR CLASSES  
es.Operator:  
or to the sele  
mirror_x"
```

Thank you!

LakeForest Consulting