Cybersecurity

Kelsey Hilton & Patrick Henry

Cloudy with a Chance of Compromise

KEYS CONFERENCE

1

DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting based on ideas from this presentation.
- **This presentation contains the opinions of the presenters.**
  Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
  Unauthorized release of this information is prohibited.

2

Kelsey Hilton

PMP, PMI-ACP, Project Manager

CoNetrix Security

Patrick Henry

CISSP, CISA, Audit & Security Consultant

CoNetrix Security

3

Why We Are Here

- We want share cloud security basics
- We you to learn from our struggles
- We like to have fun

4

What is the cloud?

Seriously, what is the cloud? Typical environments we see.

1. On Premises
2. Hybrid
3. Fully Hosted

5

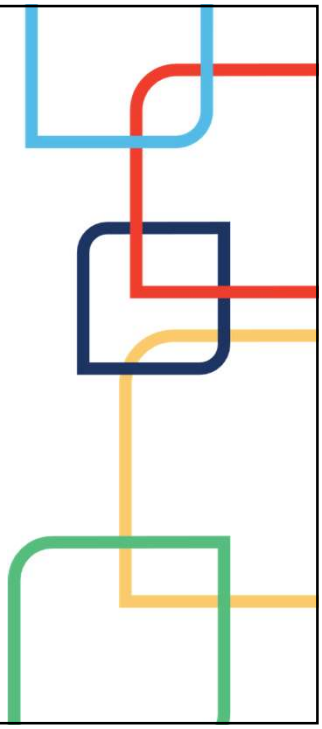
Quiz time!

What is the cloud for you?

6

Four Lessons About Cloud Security

Learned from building audit work programs



7

Lessons Learned

1

2

3

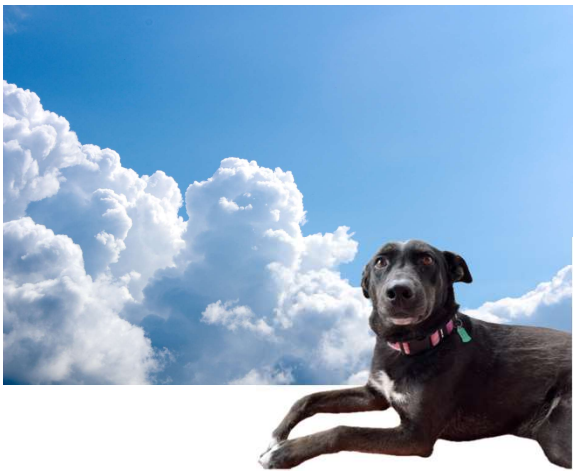
4

Simplify the Complex

8

Ambiguous Language

When you say cloud, do you mean this?



9

When you say cloud,

Or this?

Public Cloud

Private Cloud

Multicloud

Hybrid Cloud

Community Cloud

10

When you say cloud,

Or this?

11

Banned Word List

- Parameter
- Azure
- Cloud
- Scanning
- Virtual

12

Parameters?

13

Banned Word List

- Parameter
- Azure
- Cloud
- Scanning
- Virtual

14

Positive Feedback IRL

IRL = In Real Life

I'd like to propose cloud be added to the word ban list 😄

Done!

I really like it, it's helped some conversations already just to work through ambiguity

💔 1

I'm glad it helps 🙃

Kelsey Hilton 3/4/2024 5:08 PM
This, of course, is only a solution for customers that are using LAPS.

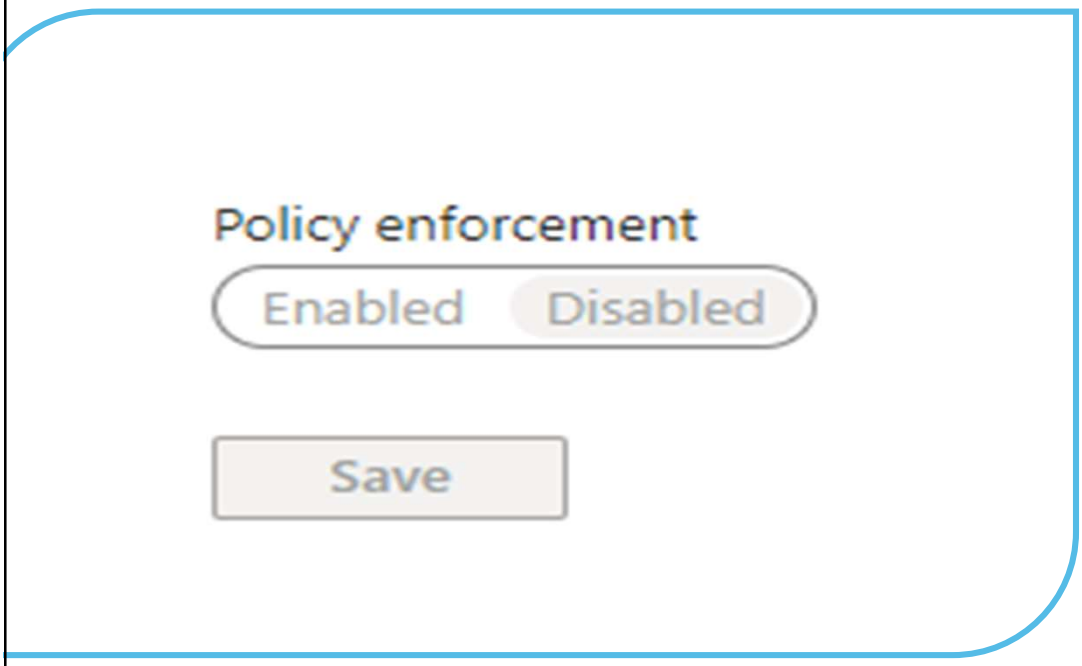
EntraID LAPS to be even more specific

💔 1

15

Enabled or Disabled?

It's blown up 1000% and still hard to tell

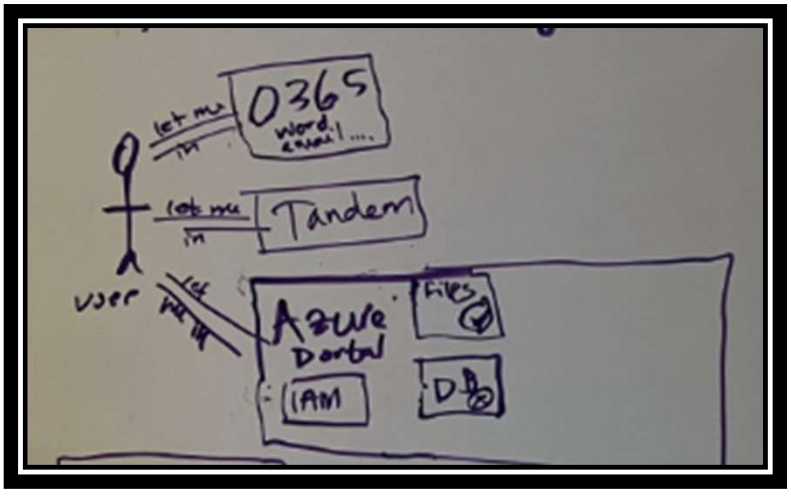


16

17

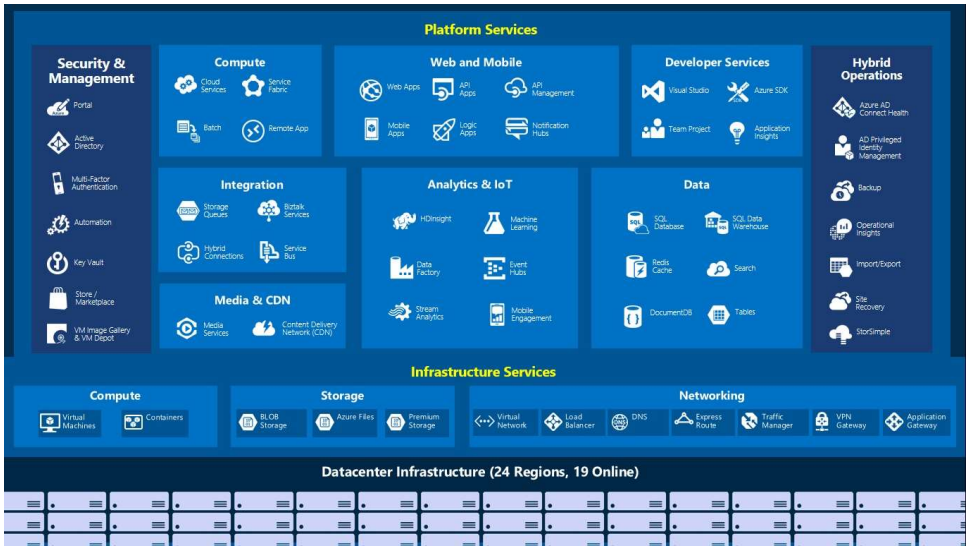
Use Pictures

Stick figures are encouraged



18

Azure

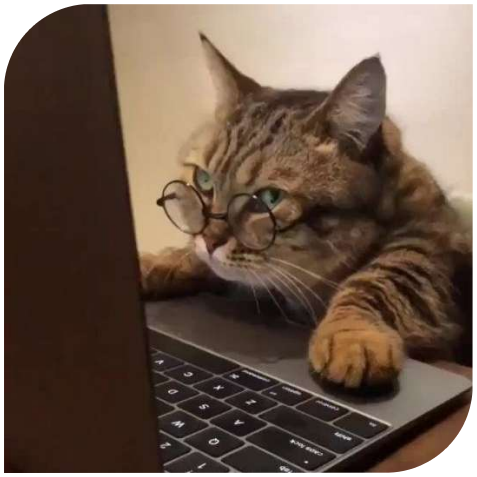


19

Azure Compute Services

20

Simplify the Complex



- Be specific with your language
- Use pictures to communicate
- Train towards missing skills
  - Microsoft Learn
  - AWS Training
- ~~Comparison~~

21

Lessons Learned

1 Simplify the Complex

2 Security Principles Mindshift

3

4

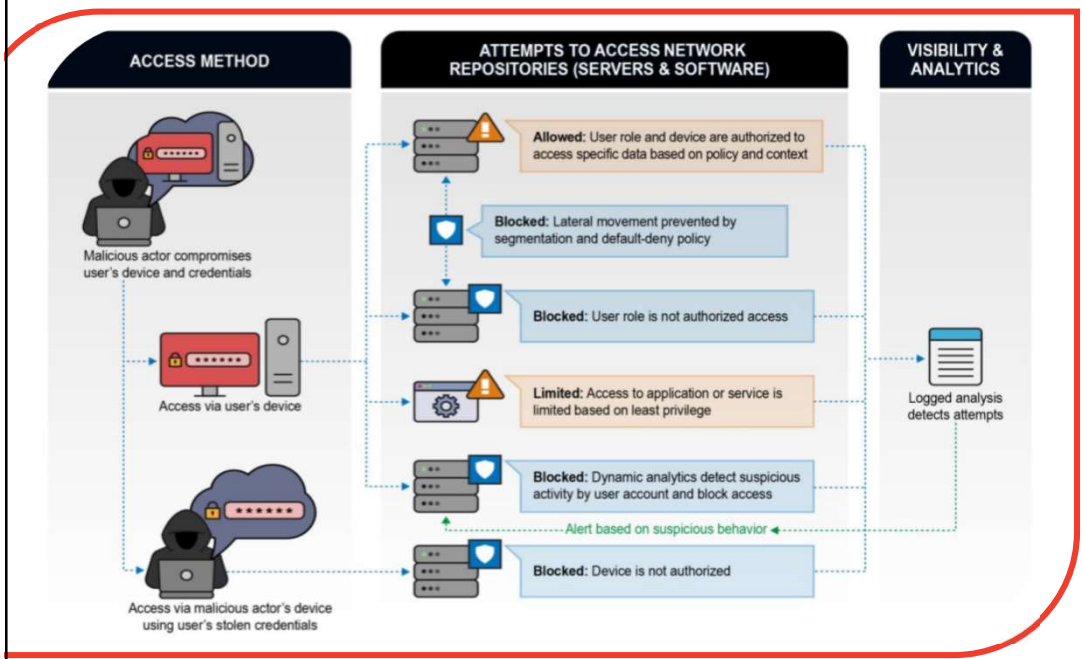
22

Traditional Security vs. Zero Trust

Traditional Security

Zero-Trust

23



Conditional Access

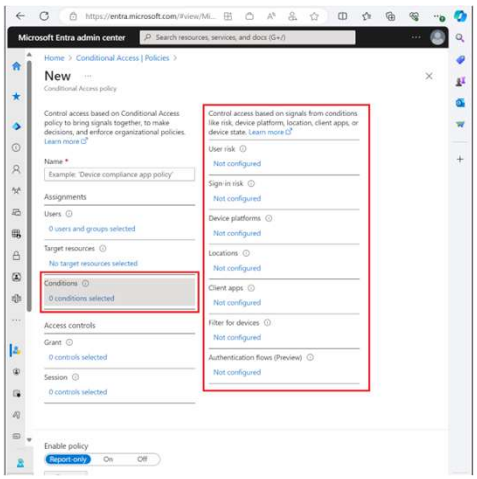
The framework for cloud security

https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

24

Conditional Access Policies

Examples of commonly applied policies

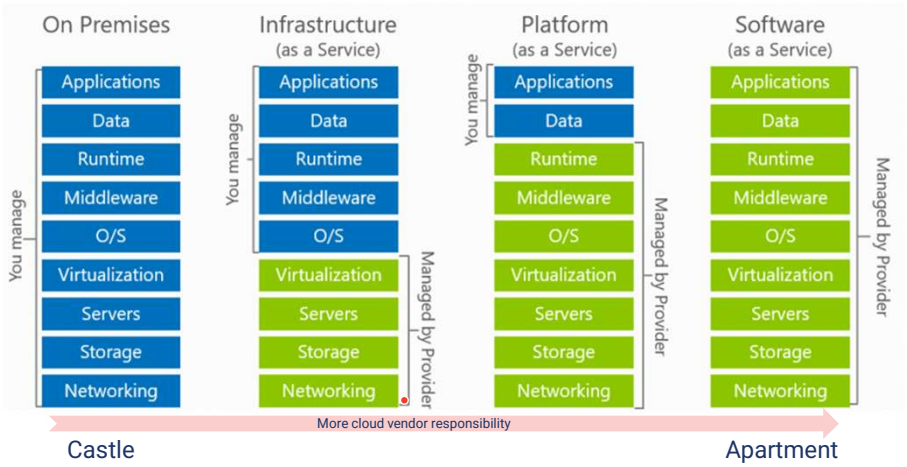


- Require multifactor for sensitive tasks
- Blocking or granting access from specific locations
- Blocking risky sign-in behaviors
- Require compliant devices

25

Shared Responsibility Model

Different concept, same analogy



26

Conquering the Mindshift

- Know the differences
- Understand your options
- Ensure your plan meets your organization's needs

27

Lessons Learned

1 Simplify the Complex

2 Security Principles Mindshift

3 Embrace Change

4

28

Continuous Change

The only constant

- Cloud services evolve rapidly
- User interface reorganization
- Configuration drift

29

Announcements

Migration of Audit p
Center to Purview Co
Microsoft
Azure AD

Things to look forward to in the new Outlook for Windows

Windows Local Administrator Password Solution with Microsoft Entra ID now Generally Available!

Prompt users for reauthentication on sensitive apps and high-risk actions with Conditional Access

By Alex Weinert
Published Feb 26 2024 09:00 AM 12.3K Views

We're c
name, N

Announcement date: January 9, 2023

Estimated date for change: March 2024

The Defender for Cloud Containers Vulnerability Assessment powered by Qualys is now on a retirement path completing on **March 1st, 2024**. If you're currently using container vulnerability assessment powered by Qualys, start planning your transition to Vulnerability assessments for Azure with Microsoft Defender Vulnerability Management.

30

Change again? But, why?

31

Progress Can Feel Like

A turtle sliding down a slippery slope

32

Tips for Managing the Change

It's a journey, not a destination

- Identify what is most important
- Sign up for change notifications
- Regularly review your cloud environments
- Breathe

33

Lessons Learned

1	2	3	4
Simplify the Complex	Security Principles Mindshift	Embrace Change	We Don't Know What We Don't Know

34

We Don’t Know What We Don’t Know

- Education, research and more education
  - Understanding how it works requires testing and research
- Licensing is complex
  - Free, P1, P2, Microsoft 365 E3 and E5

35

Vulnerability Scanning in the Cloud

36

Cloud Vulnerability Scanning Issues

We had no idea

- Zero-trust kills authenticated scanning
- Vulnerability scans vs. compliance scans
- Review reporting services and conditional access policies

37

Beware of Best Practice Recommendations!

```
CIS 1.1.3 Ensure that between two and four global admins are designated.
```

- Does 2 to 4 admins work for everyone?
- Remember your break glass account.

38

Tips for Discovering What You Don't Know

- Stay curious and open-minded
- Leverage your knowledgeable vendors
- Know your organization

39

Takeaways

40

See you next year for part two.

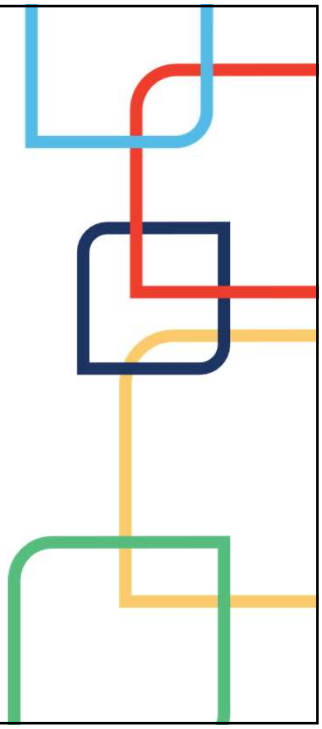
41

Resources

- Baseline configuration help
  - https://setup.microsoft.com/entra/microsoft-entra-id-setup-guide
  - CIS Azure Foundations
  - CIS M365 Foundations
- Stay updated
  - https://azure.microsoft.com/en-us/updates/
  - https://admin.microsoft.com/Adminportal/Home#/MessageCenter
- Training
  - Learn about Training by Role or Solution | Digital and Classroom Training | AWS (amazon.com)
  - Azure on Microsoft Learn | Microsoft Learn
  - https://www.cisa.gov/news-events/alerts/2024/03/07/cisa-and-nsa-release-cybersecurity-information-sheets-cloud-security-best-practices

42

Questions?



43

THANKS FOR JOINING!

Cloudy with a Chance of Compromise

Kelsey Hilton
PMP, PMI-ACP
Project Manager
CoNetrix Security
khilton@conetrix.com

Patrick Henry
CISSP, CISA
Audit & Security Consultant
CoNetrix Security
phenry@conetrix.com

KEYS CONFERENCE

44