RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CSV-W04

SaaS Attacks Happen: How Cloud Scale Changes the Security Game

Sara Manning Dawson

Group Program Manager
Office 365 Security Engineering
@SManningDawson

#RSAC

Goals

How can the unique properties of a cloud service help to protect your data?

- How can strategies to scale and streamline operations also accrue to better protection?
- How can data scale be used to better protect your data?
- What is the provider relationship with your data?
- How can cloud-wide purview help protect you?

Cloud Security is Well Mis Understood

Cloud Security is Well Mis Understood

#RSAC

Maybe that will work...

"We have millions of users to protect, and our reputation is on the line, so of course we do a better job."

"Our budget is so big, we just keep scaling up our Security Operations, so of course we do a better job"

...but let's take a step back

"Reason from first principles rather than by analogy"

The problem with quotes from the Internet is that they aren't always accurate.

- Abraham Lincoln, 1864

Unique Properties of the Cloud

	Data Scale	Operations Scale	Cloud-Wide Purview	Data Sovereignty
Properties	Data is spread across hundreds of thousands of disks, machines, locations	Speed, Reliability, and Security all improve with automation. Machine homogeneity in code execution and communications	Signals that detect and act upon bad actors are service wide	The same company that hosts your content and provides value-add services must also honor your data sovereignty
Challenges	Breach risk is as large as data set	Accountability for security, availability, reliability squarely on service provider Stack is extremely agile	Reputation wise, customer breach = cloud service provider breach	Must find methods to prove it International variation

Cloud Security First Principles

The unique properties of the cloud introduces new security **first principles.**
Realize them via **engineered solutions**.

Cloud Operations Principles

1. Humans govern the service, code operates the service. Reduce human interaction with the system via automation.
2. When humans must be involved, JIT and JEA access only, gated by at least two decision makers. And don't touch the data.
3. Security must be engineered into operations fabric to take full advantage of scale, agility, and homogeneity.

Customer Protection Principles

4. Cloud-wide operational processes useful to individual customers should be made available.
5. Security learnings from one customer help all.
6. No customer can harm another as a result of both being in a cloud service.

Principle 1 and Principle 2:

Humans govern the service, code operates the service. Reduce human interaction with the system via automation.

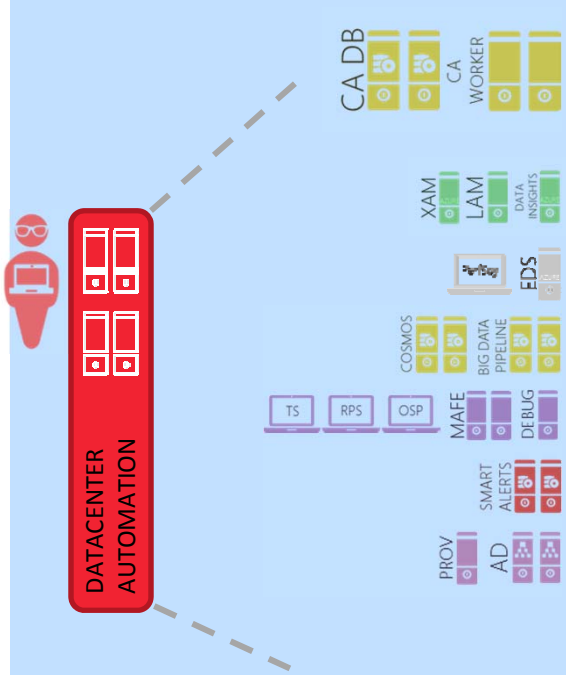
When humans must be involved, JIT and JEA access only, gated by at least two decision makers. And don't touch the data.

Approach

#RSAC

Automation	Reducing human interaction is as good for security as it is for scaling reliable operations.	
Remote Access Only, via Code	What if only explicit, hardened code, run remotely, could service machines? *Execution is in the context of the operator or workflow.*	
Enforce ID, Time and Scope	All Access is Just In Time and Just Enough *Multi-factor approval chain, with specific machine targets* *Scripts have a definitive execution scope and timeframe*	
Don't Touch The Data	Prove You Don't Touch The Data *Put an audited barrier between the cloud operator's interests – operations and value-add - and the customer's interests - data.*	

Office 365 Service Automation



Orchestration	Central Admin (CA), the change/task engine for the service
Deployment/Patching	Build, System orchestration (CA) + specialized system and server setup
Monitoring	eXternal Active Monitoring (XAM): outside in probes, Local Active Monitoring (LAM/MA): server probes and recovery, Data Insights (DI): System health assessment/analysis
Diagnostics, Perf	Extensible Diagnostics Service (EDS): perf counters, Watson (per server)
Data (Big, Streaming)	Cosmos, Data Pumpers/Schedulers, Data Insights streaming analysis
On-call Interfaces	Office Service Portal, Remote PowerShell admin access
Notification/Alerting	Smart Alerts (phone, email alerts), on-call scheduling, automated alerts
Provisioning/Directory	Service Account Forest Model (SAFM) via AD and tenant/user addition/updates via Provisioning Pipeline
Networking	Routers, Load Balancers, NATs
New Capacity Pipeline	Fully automated server/device/capacity deployment

Office 365 Service Automation

The “brain” operating our service is called

Central Admin

- Hardened code
- Safe, reliable, high throughput automation
- C# “workflows” or PowerShell script

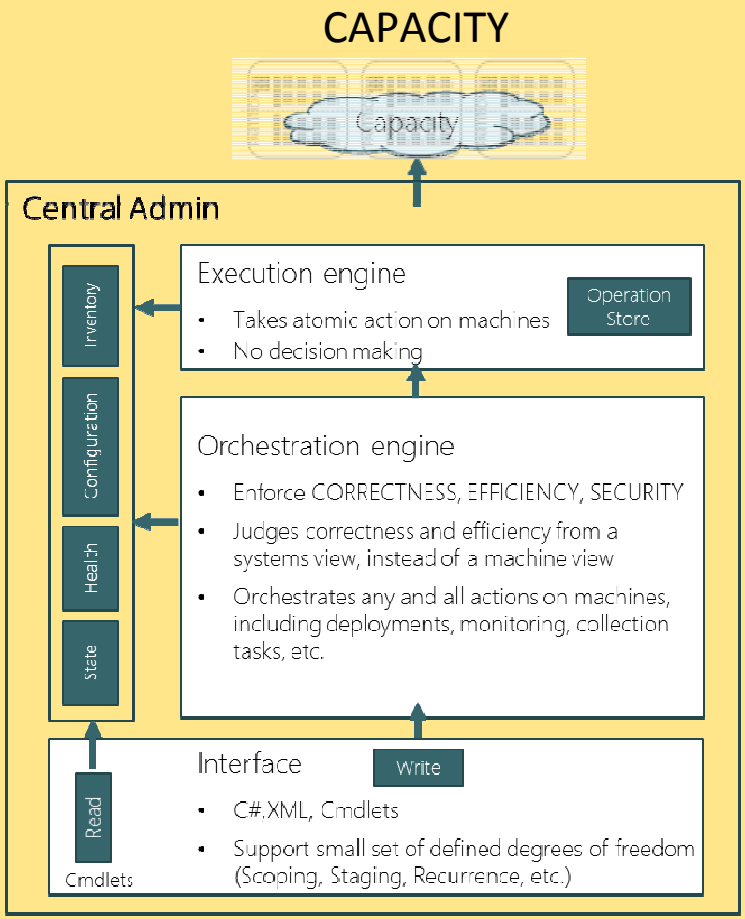
Runs check-in, build, and deployment tasks

Runs regular maintenance tasks

Runs monitoring and self-healing tasks

~200 million workflows handle day-to-day operations and failures.

Office 365



Remote Access Only, via Code

#RSAC

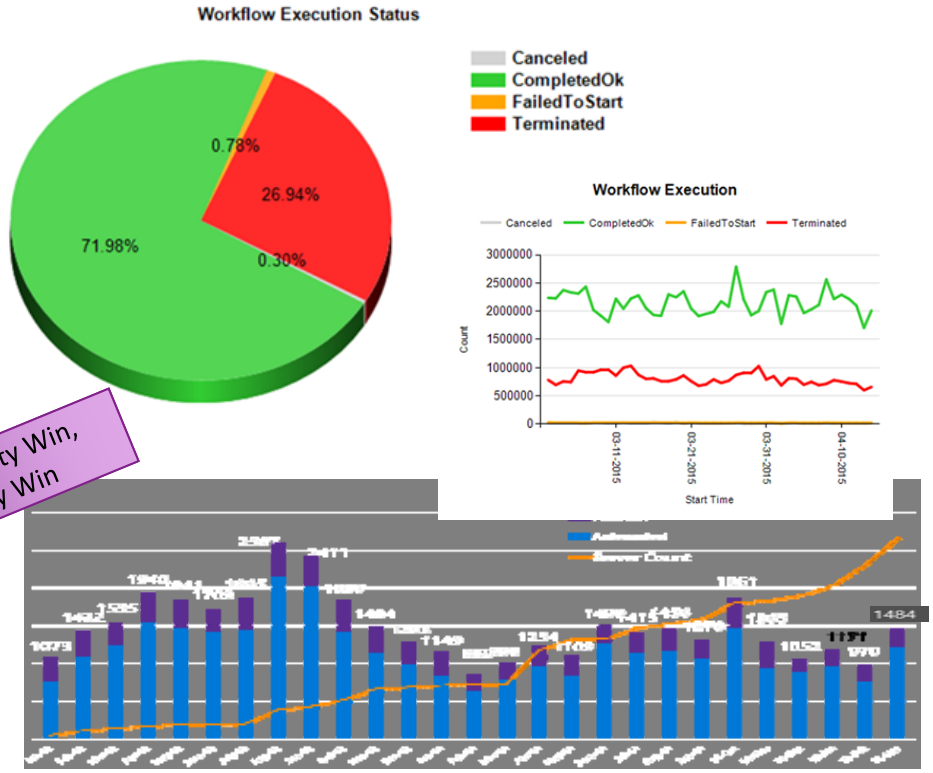
High order work is done in CA
e.g. rebalance a DAG, restart a service

but

EVERYTHING FAILS AT SCALE

- When troubleshooting, repair, recovery, or patching can't self-heal, engineering are paged
- Engineering intervention is limited to decision-making, code does the work

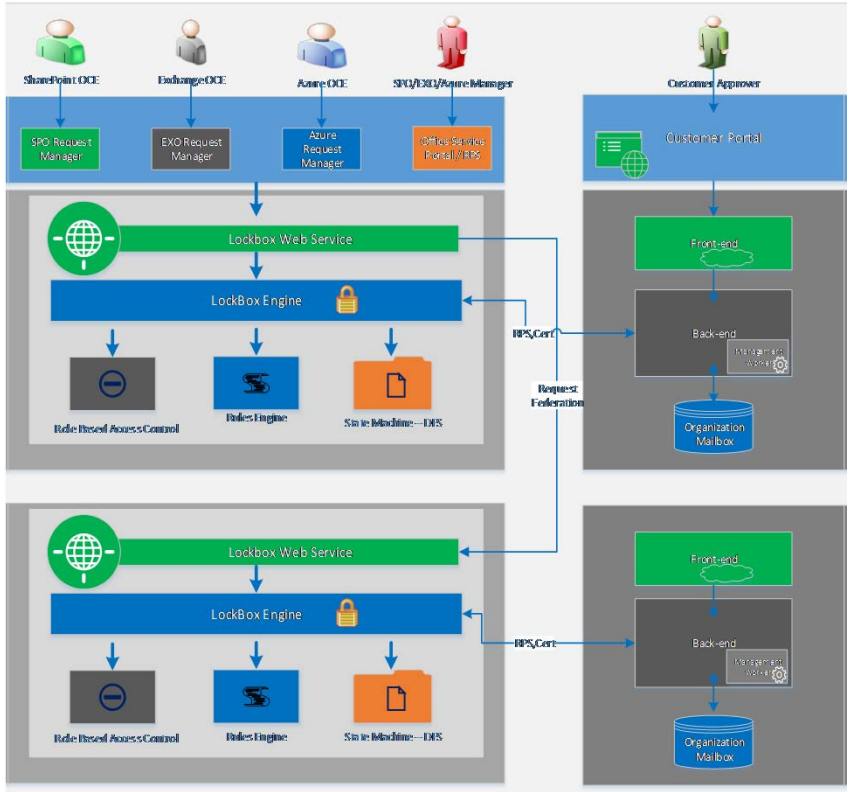
Serviceability Win,
Security Win



Office 365

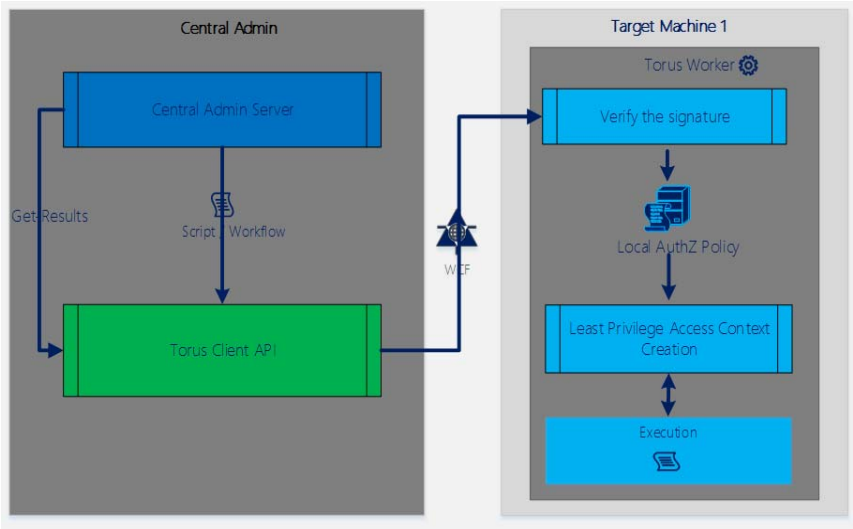
RSAConference2016

Enforce Time and Scope, Don't Touch the Data



Office 365 "Lockbox" 3 Factor Approval. (4 Factor with Customer Lockbox)

Claims-based, JIT and JEA sandboxed processes. No standing accounts, no standing access



Principle 3:

Security must be engineered into operations fabric
to take full advantage of scale, agility, and homogeneity.

Innovation Areas

#RSAC

Detections via Build-Time Intel

Use source code to auto-map execution and comms

Homogenous run-time environment knows what the machine should ever need to do or connect with, so detections can climb the stack.
SIEMs that depend on history hit limits in an agile and high-scale service.

Red Team Automation

Red Team creativity is critical to understanding risk

But even their function can benefit from automation. Response and Detections benefit as well.

Tighten Machine Communication & Execution

Evolve from "assume breach" to a protect posture

Eliminate interactive logon, local machine accounts, S2S elevation.

Hide Data In Scale

Distribute each organization's data, with anonymity

Protect logical access via obfuscation of Tenant-to-Mailbox mapping

Engineering Security Into Service Fabric

Office 365 Build and Deployment Process

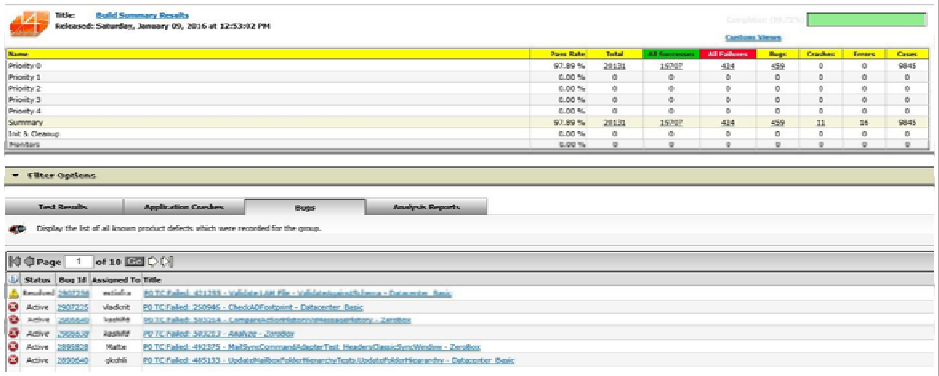
Access to code → Pre checkin → Official build → Official Test → Ring validations

Here, **map what's possible** to inform detection signals engine

Code is tested against realities of **current** environment

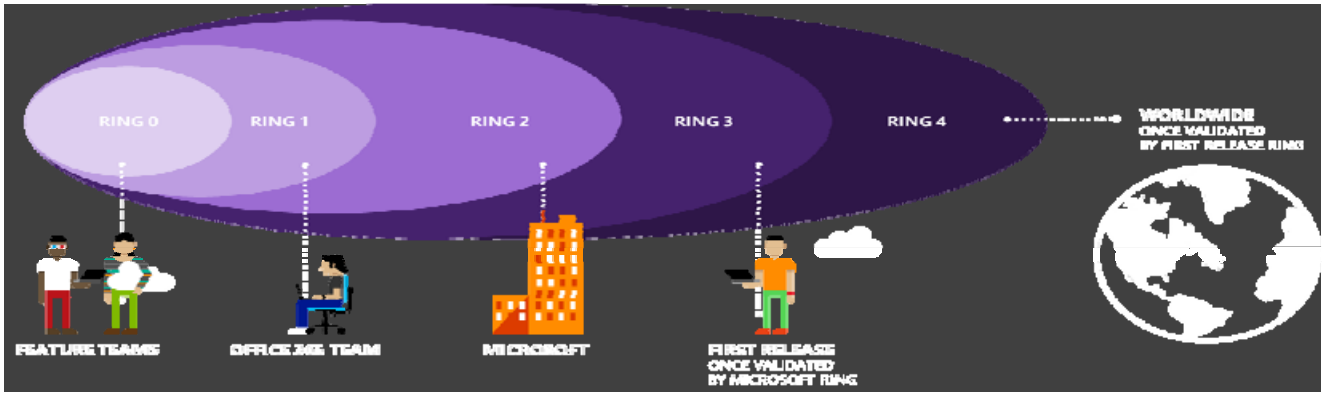
Official Test

- **Official test run all tests on entire build**
- **Test pass rate works as quality indicator of build to be deployed in rings**
- **Test pass automatically generates bugs to be fixed in build**



Engineering Security Into Service Fabric

Regular Build Deployment Train



Repair Box agent self-heals issues and vulnerabilities

REPAIR BOX

Specialized CA WF that scans and fixes variety of service issues

- Consistency checks (e.g. member of the right server group
- HW repair (automated detection, ticket opening, closing)
- NW repair (e.g. firewall ACL)
- “Base config” repair such as hyper-threading on/off
- Patching and vulnerability up-to-date checks

Emergency patching is rare, …and as critical to security as it is to stability

Emergency replacement of binaries

- CA controlled and staged with constant feedback
- Management approved and assisted

Engineering Security Into Service Fabric

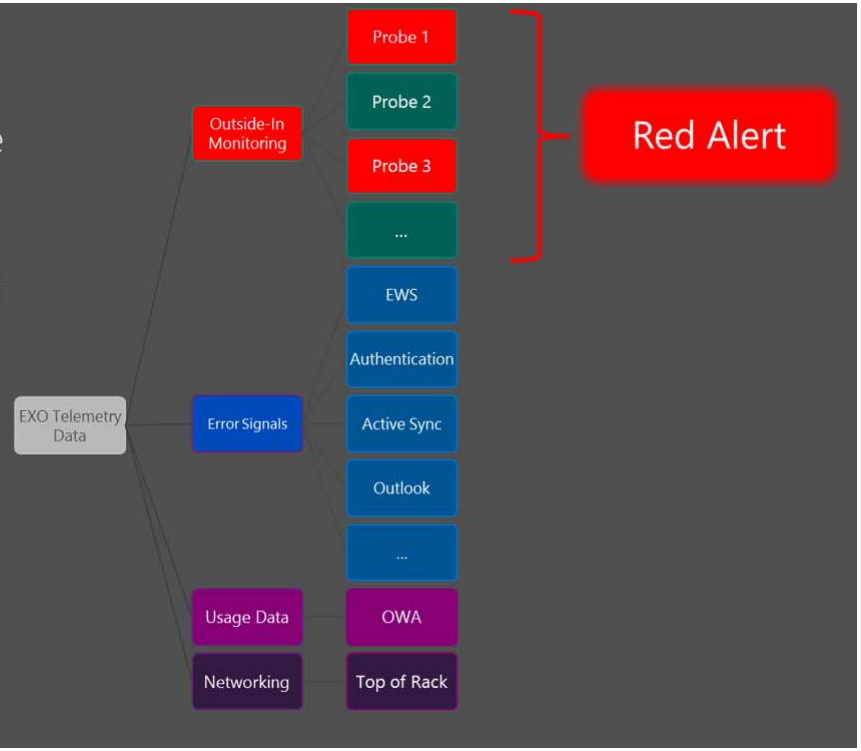
The Health Signals Pipeline needs a source of truth, a deviation confidence measure, and a notification pipeline. Sound familiar?

If something is happening across many entities/signals, then it must be true

Apply "baseline" from outside-in as a source of truth

If each signal has reasonability fidelity—you get **~100% accuracy**

We use this technique to build "Red Alerts"



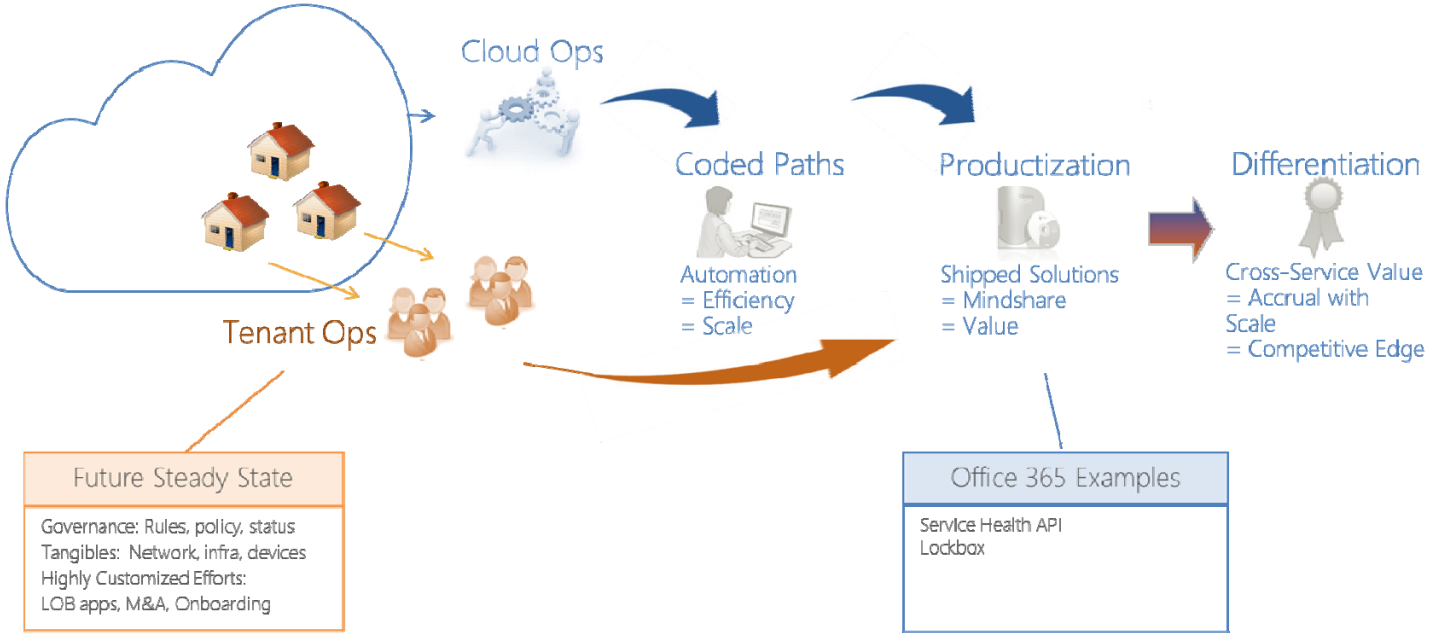
Customer Protection Principles (4-6):

Cloud-wide operational processes useful to individual customers are made available.

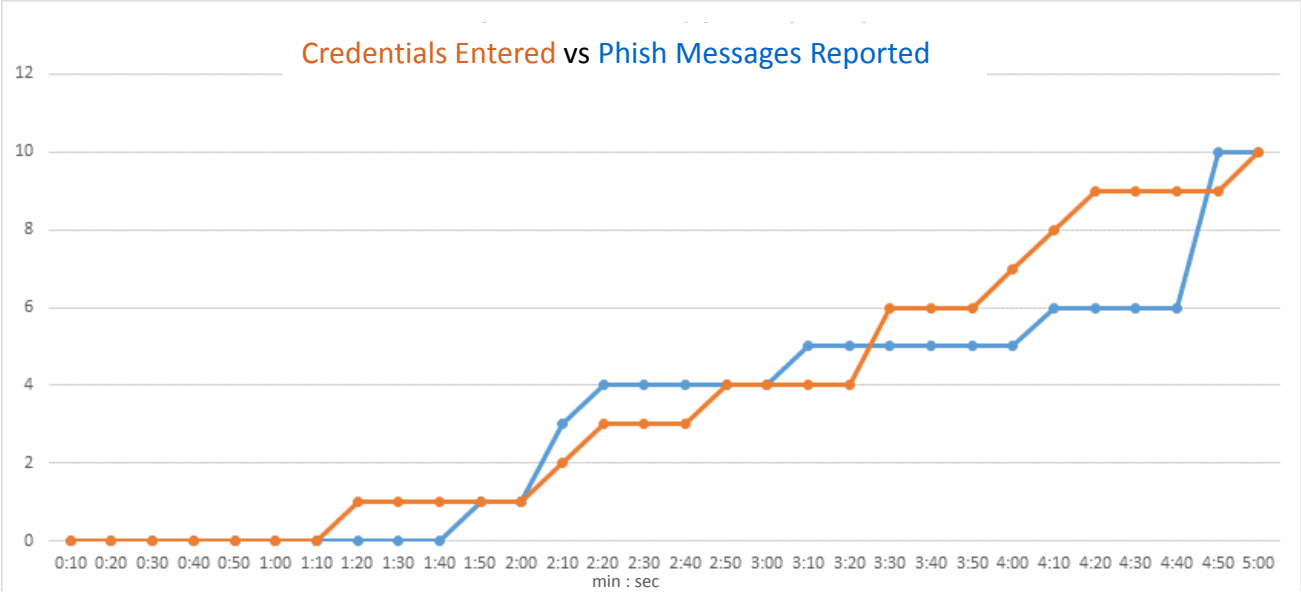
Security learnings from one customer help all.

No customer can harm another as a result of both being in the cloud service.

Cloud operations accrue customer value



One Security Learning Helps All



Phishing is an edge on the path of least resistance.
It's difficult to take action before it's too late.

One Security Learning Helps All

#RSAC

What if these are seen in multiple tenants

- From same IP?
- In a short timeframe?
- Clustered in same geo?
- Clustered within a particular industry?

What if multiple tenants

- Were forwarding to a single IP or email address?
- Were getting accessed from a single IP
- Got a message from an IP address that sent mail with a link, then OWA was accessed from that IP?

Suspicious Behaviors

Forwarding/Redirection/Journaling Rules leaving tenant

Broad or org-wide search for “password” or like

Export of data or exhaustive client-side downloading

Recognition of fake login pages in Phishing attack

Spike/anomaly in admin activity

New Admin is added or promoted

Security reduction activity (i.e. removal of MFA, MDM policies)

Data exposure admin activity (journaling rules, exposing SP libraries to external)

Anomalous activity or activity spike in external facing properties

Exhaustive web crawling or index building

Multiple OWA clients from same IP (anomalous, non-kiosk)

Delegates added to an elevated user

DEMO: Secure Score

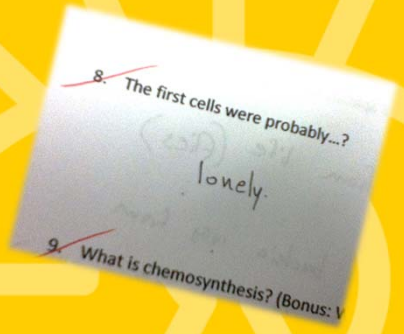
http:/aka.ms/O365securescore

Takeaways

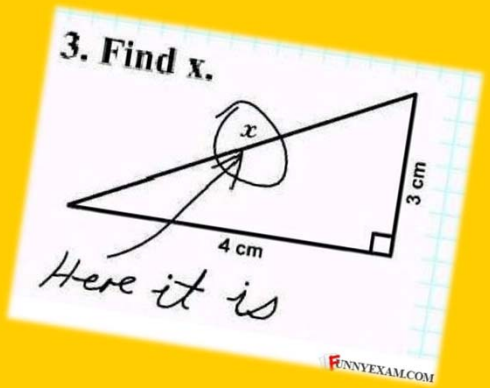
How can the unique properties of a cloud service help to protect your data?

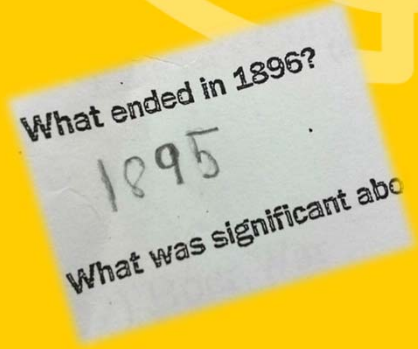
- How can strategies to scale and streamline operations also accrue to better protection?
- How can data scale be used to better protect your data?
- What is the provider relationship with your data?
- How can cloud-wide purview help protect you?


Where was the American Declaration of Independence
signed?
At the bottom.


8. The first cells were probably...?
lonely.
9. What is chemosynthesis? (Bonus:

Q&A


3. Find x.
x
3 cm
4 cm
Here it is
FUNNYEXAM.COM


What ended in 1896?
1895
What was significant abo