Fantastic cloud security mistakes and where to find them

Sarah Young

Agenda

- Whoami
- A changed world
- The current threat landscape
- Stuff you shouldn’t do
- Security capabilities you should know about and stuff you should be doing

whoami

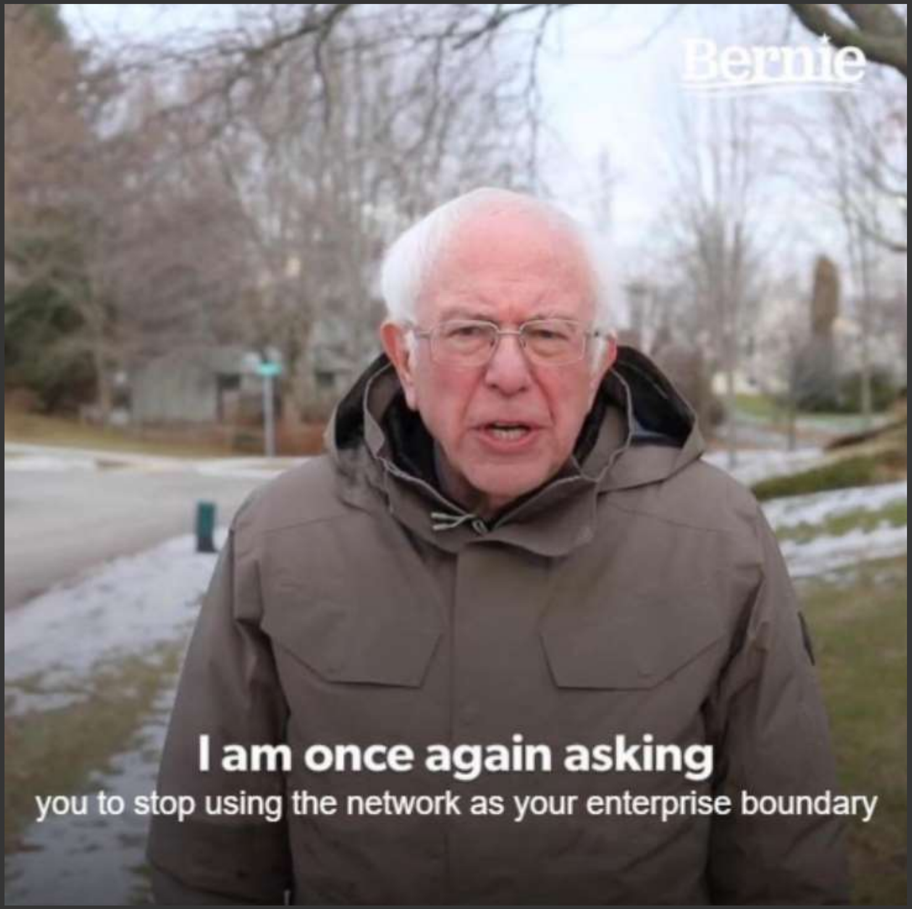
@_sarahyo
@sarahyo.com

whoami

- I'm a Senior Cloud Security Advocate @ Microsoft.
- Worked in security for the past 10+ years.
- I love talking about how we can secure all the things.
- Wrote some MS Press books.
- Co-host of the Azure Security Podcast.
- Definitely a crazy dog woman.

@_sarahyo
@sarahyo.com

A changed world



@_sarahyo
@sarahyo.com

A continuously changing world

Hybrid of Everything (On-Prem, multi-cloud, SaaS, IoT, OT, etc.)
Requires security to think and act holistically across the technical estate to keep up with attackers doing the same.

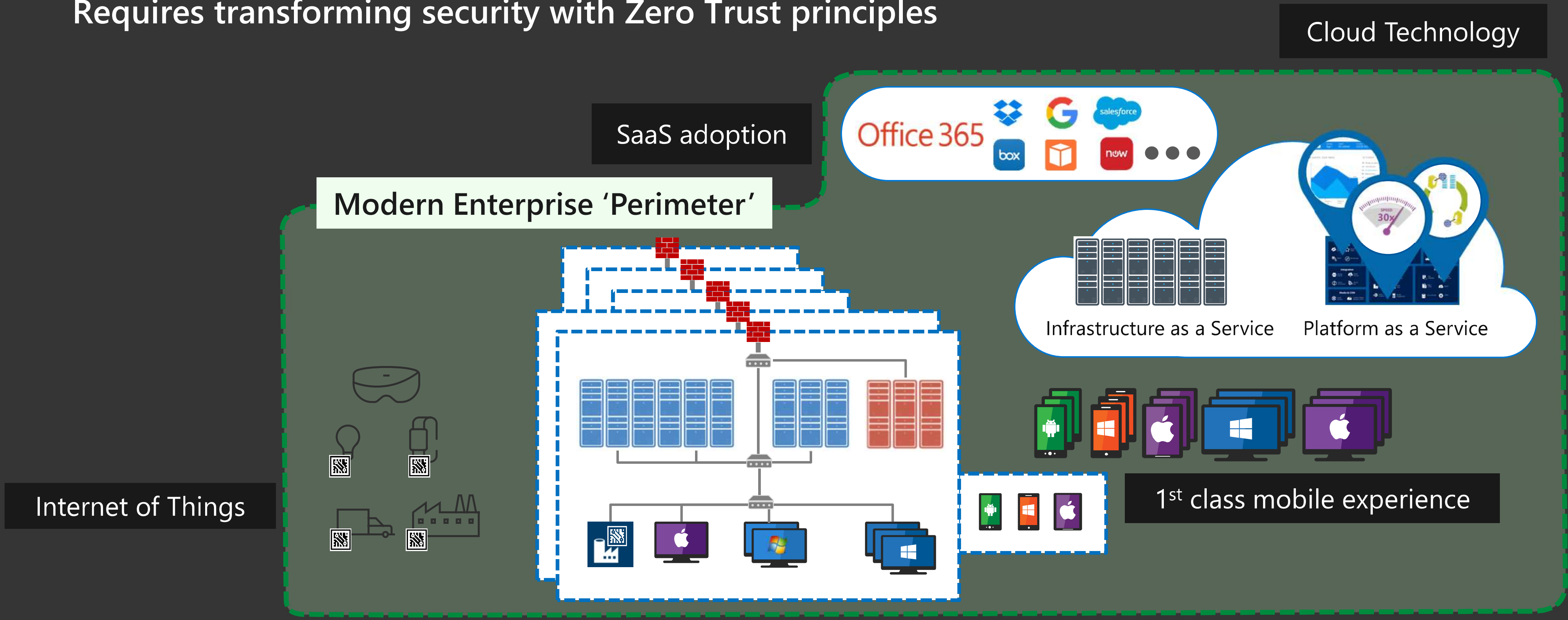
Changing Threat Landscape
Require adjusting security priorities to ensure top business risks are address first

Shared Responsibility Model
Requires changes to security mindsets, tooling, processes, and skillsets as responsibilities shift to cloud providers

Changing Processes and Architectures
Require updating security for new Cloud & Application Architectures, DevOps/DevSecOps processes, Infrastructure as Code, Citizen Developers, and more

Technical Estate becoming hybrid of everything

Requires transforming security with Zero Trust principles



Cloud Technology

SaaS adoption

Modern Enterprise 'Perimeter'

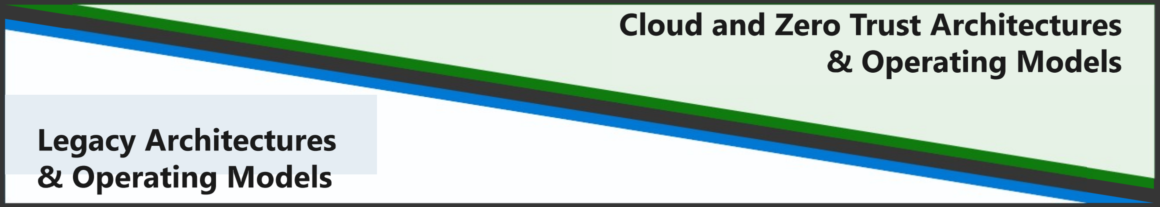
Internet of Things

Infrastructure as a Service

Platform as a Service

1st class mobile experience

This changed world has made roles change



🚫 "STOP THE PRESSES!" → CONTINUOUS VALIDATION 🔄

Security roles change with architectural/operational models

Project based Engagement	**Architecture** →	Continuous Engagement & Improvement
Network-only Tools and Expertise	**Network Security** →	Identity-Aware Network Security
Quality Check Before Release	**Development** →	Security SME in DevOps process
Manual Resource Administration	**Administration** →	Author & Govern Automation

The current threat landscape

@_sarahyo
@sarahyo.com

Attack services are inexpensive

Ransomware:
$66 upfront
Or
30% of the profit (affiliate model)

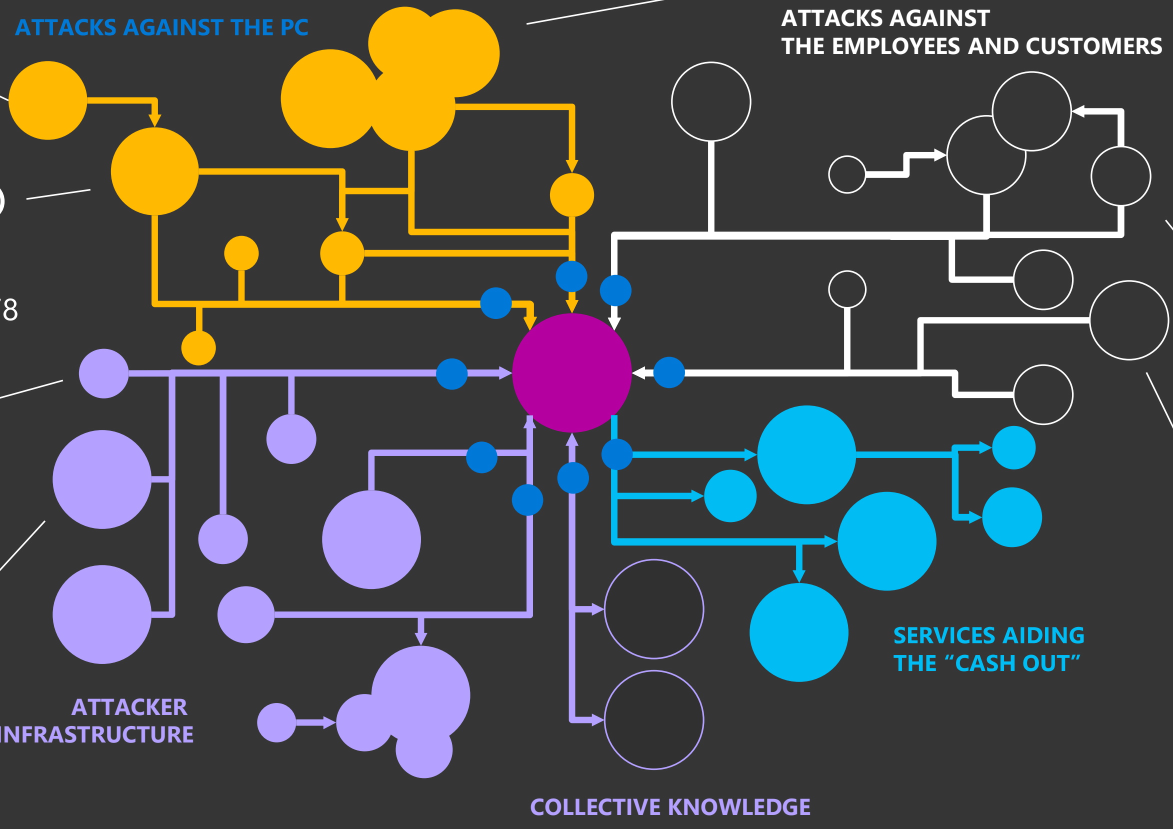
0days price range varies from $5,000 to $350,000

Loads (compromised device) average price ranges

- **PC** - $0.13 to $0.89
- **Mobile** - from $0.82 to $2.78

Denial of Service (DOS) average prices
day: $102.05
week: $327.00
month: $766.67

Proxy services (evade IP geolocation) prices vary
As low as $100 per week for 100,000 proxies.

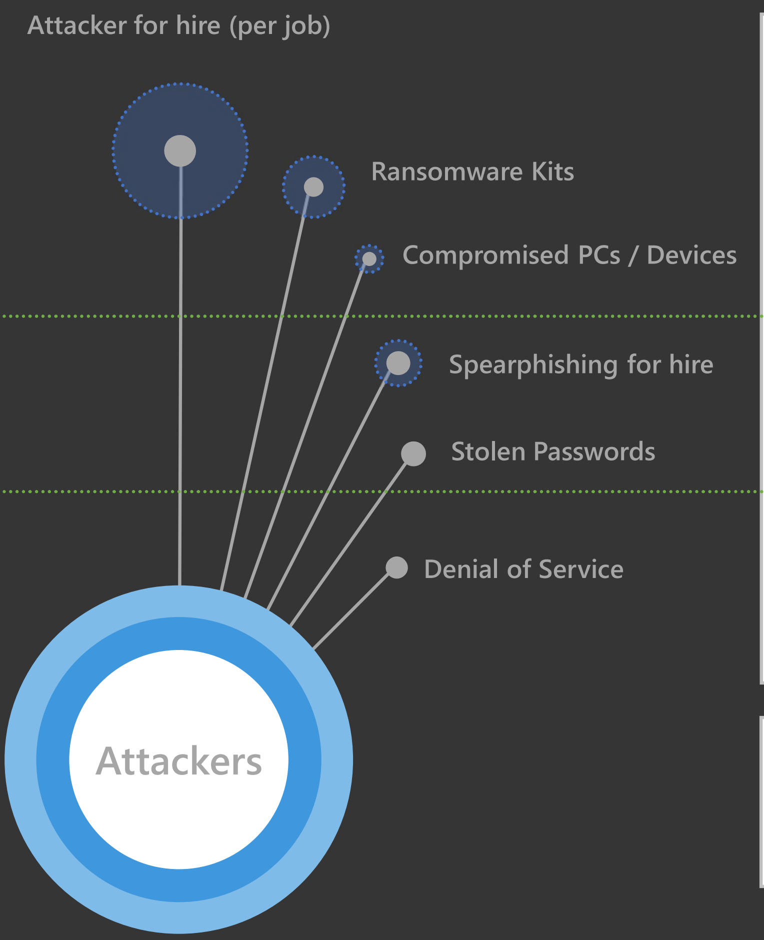

ATTACKS AGAINST THE PC
ATTACKS AGAINST THE EMPLOYEES AND CUSTOMERS
ATTACKER INFRASTRUCTURE
SERVICES AIDING THE "CASH OUT"
COLLECTIVE KNOWLEDGE

Spearphishing services range from $100 to $1,000 per successful account take over

Compromised accounts
As low as $150 for 400M.
Averages $0.97 per 1k.

@_sarahyo
@sarahyo.com

Security Capabilities and Guidance



Native Security Controls

and integration with existing security capabilities

Native Threat Detection (& SIEM)

Identity services, Windows, Linux, iOS, Android, SaaS apps + correlate with cloud native SIEM+SOAR+UEBA

Passwordless and Multi-factor Authentication (MFA)

Mitigate common and effective identity and password attacks with biometrics, hardware security, and threat intelligence

Native Firewall and Network Security

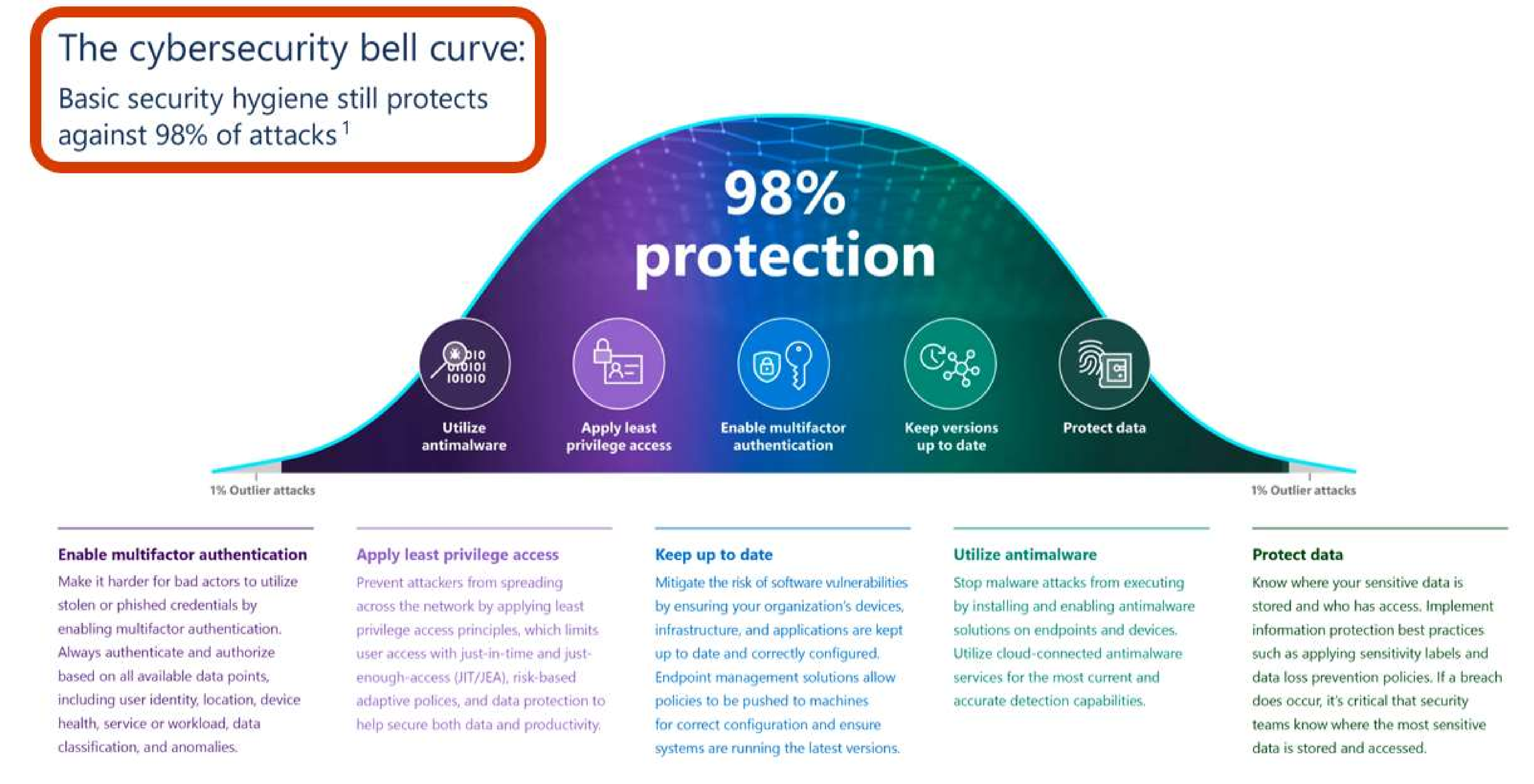
Protect business-critical assets with Firewall, DDoS protection, & integrated web application firewall (WAF)

Industry Collaboration

with customers, NIST, CIS, The Open Group, and others

Security Guidance

- Best practices
- Security Benchmarks
- Cloud provider architecture frameworks



The cybersecurity bell curve:

Basic security hygiene still protects against 98% of attacks[1]

98% protection

Utilize antimalware

Apply least privilege access

Enable multifactor authentication

Keep versions up to date

Protect data

1% Outlier attacks

1% Outlier attacks

Enable multifactor authentication

Make it harder for bad actors to utilize stolen or phished credentials by enabling multifactor authentication. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Apply least privilege access

Prevent attackers from spreading across the network by applying least privilege access principles, which limits user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Keep up to date

Mitigate the risk of software vulnerabilities by ensuring your organization's devices, infrastructure, and applications are kept up to date and correctly configured. Endpoint management solutions allow policies to be pushed to machines for correct configuration and ensure systems are running the latest versions.

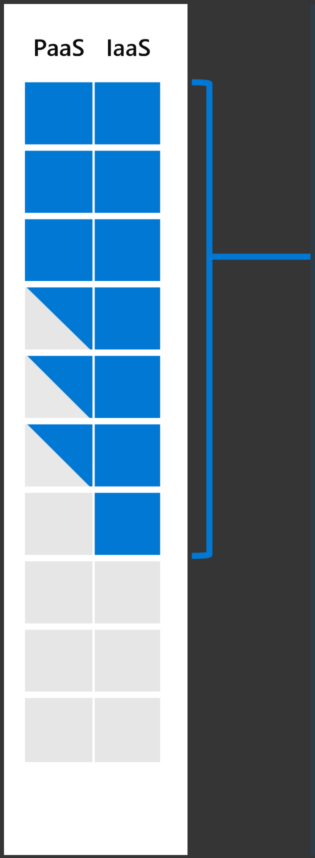
Utilize antimalware

Stop malware attacks from executing by installing and enabling antimalware solutions on endpoints and devices. Utilize cloud-connected antimalware services for the most current and accurate detection capabilities.

Protect data

Know where your sensitive data is stored and who has access. Implement information protection best practices such as applying sensitivity labels and data loss prevention policies. If a breach does occur, it's critical that security teams know where the most sensitive data is stored and accessed.

Multi-cloud threats are a mix of old & new…



EXISTING TECHNIQUES (AT COMPARABLE LEVELS)

EXPLOIT/ENTER	TRAVERSAL	MONETIZATION
SOCIAL ENGINEERING	CREDENTIAL THEFT & ABUSE (HASHES, SSH…)	RANSOMWARE/EXTORTION
PHISHING	SCAN & EXPLOIT	TARGETED DATA THEFT
GEO-FILTERING EVASION WITH PROXY		COMMODITY BOTNET/DDOS/ETC
● ● ●	● ● ●	● ● ●

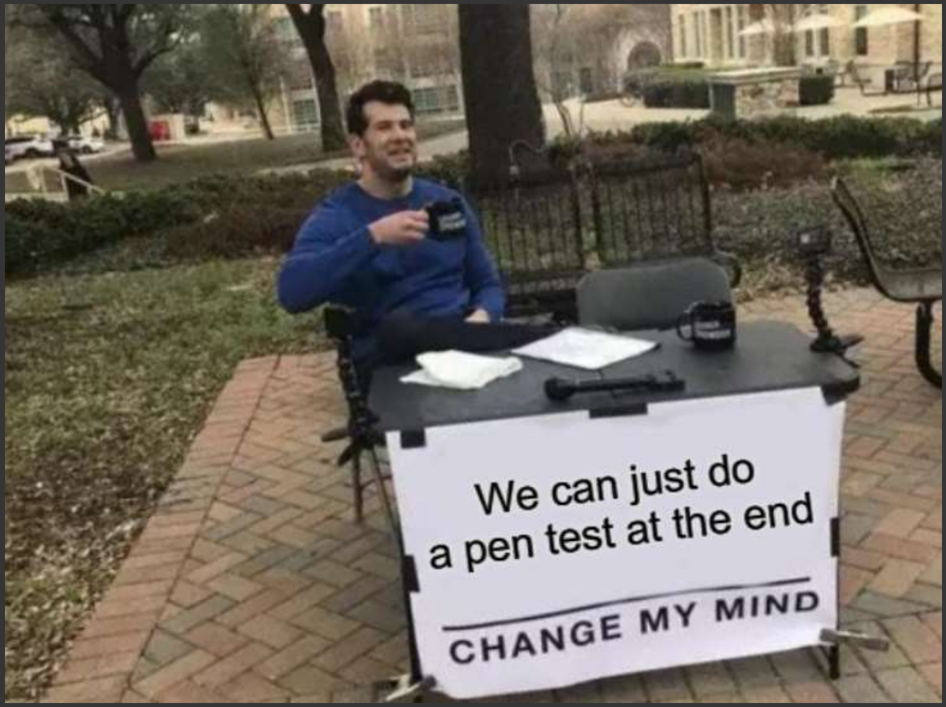
⚠ Massive & Growing Risk Factors

New Techniques (★) or Very High Usage (⇧)

- ★ ACQUIRE TENANT KEYS FROM GITHUB/ETC
- ★ PIVOT TO ON PREMISES FROM CLOUD
- ⇧ CRYPTOMINERS – (WEBSERVERS, VISITORS)
- ⇧ RDP/SSH PASSWORD SPRAY & BRUTE FORCE

@_sarahyo
@sarahyo.com

Stuff you shouldn't be doing



@_sarahyo
@sarahyo.com

Avoid anti-patterns

An anti-pattern is a common response to a recurring problem that is usually ineffective and risks being highly counterproductive.

Follow Best Practices

Best Practices are observed patterns that consistently and effectively improve processes across many organizations

Top Anti-patterns

- **Positioning security as an adversary to business and IT**
- **Using on-premises controls to secure cloud**
- **Trying to secure workloads after they are fully architected and/or deployed**
- **Security “owning” risks**

Stuff you should be doing

LEFT
EXIT 12
Zero Trust Experts
AI Experts
Security LinkedIn & Twitter

Identity

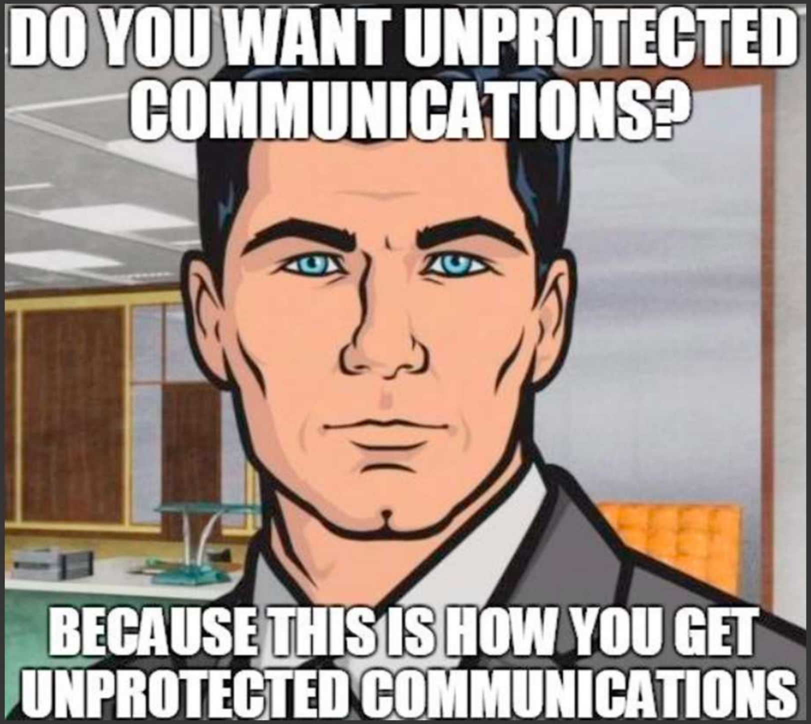
- Store your user identities in Azure AD – centralise your identity store.
- Use Conditional Access!
- Use multi-factor authentication which research shows protects against about 99% of attacks.
- Use Key Vault to store and protect certificates, keys and other secrets.
- You can use AAD managed identities to access Key Vault for improved security.
- Make sure client secrets/certificates have (relatively) short expiration lives.

SOMEONE FIGURED OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG.

@_sarahyo
@sarahyo.com

Connectivity

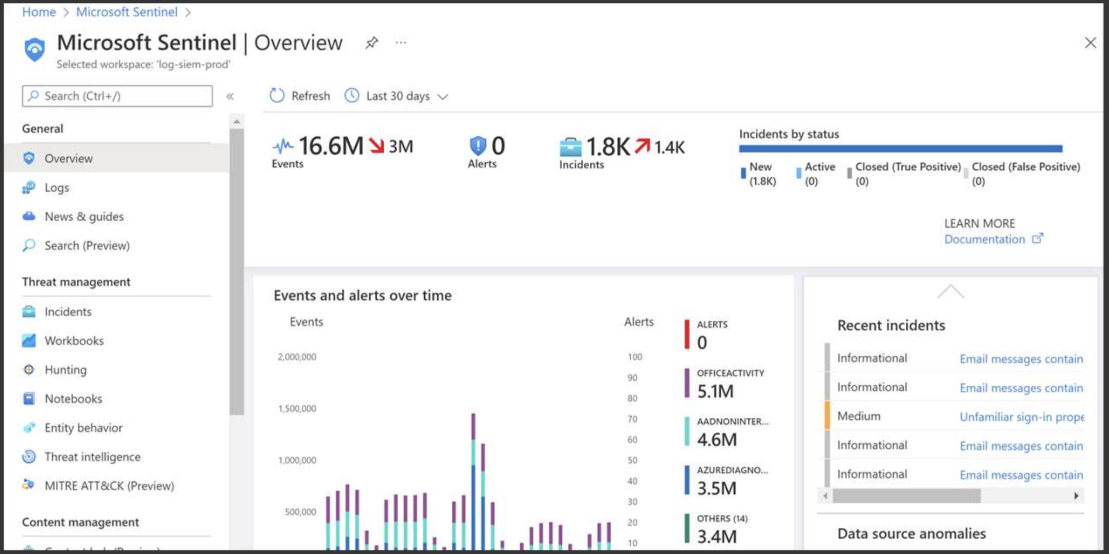
- Use a secure bastion/jump host.
- API management tooling – this is a proxy you put in front of APIs that adds features such as caching, throttling, and authentication or authorization.
- Load Balancer - you can use load balancers to increase the availability of applications (which is a security thing!)
- Encrypt yo' stuff.


DO YOU WANT UNPROTECTED COMMUNICATIONS?
BECAUSE THIS IS HOW YOU GET UNPROTECTED COMMUNICATIONS

@_sarahyo
@sarahyo.com

Logging and monitoring

- Turn on logging for everything in your environment e.g. UAL, audit logs, sign-in logs, mailbox auditing
- Collect logs into a central store.
- Ensure that you have someone reviewing and handling both your logs and alerts generated from your security tooling.
- Use out of the box monitoring capabilities.
- Automate as much as you can.



Selected workspace: 'log-siem-prod'

Informational	Email messages contain
Informational	Email messages contain
Medium	Unfamiliar sign-in prope
Informational	Email messages contain
Informational	Email messages contain

@_sarahyo
@sarahyo.com

Logging and monitoring cont.

- **Some key scenarios to monitor for:**
  - Attempts to sign in to disabled accounts
  - New access credential added to Application or Service Principal
  - Authentication Attempt from New Country
  - New Inbox-Rules created to forward to external domains
  - Inbox Rules with external mails
  - Multiple failed logon attempts
  - Files and Folders shared externally

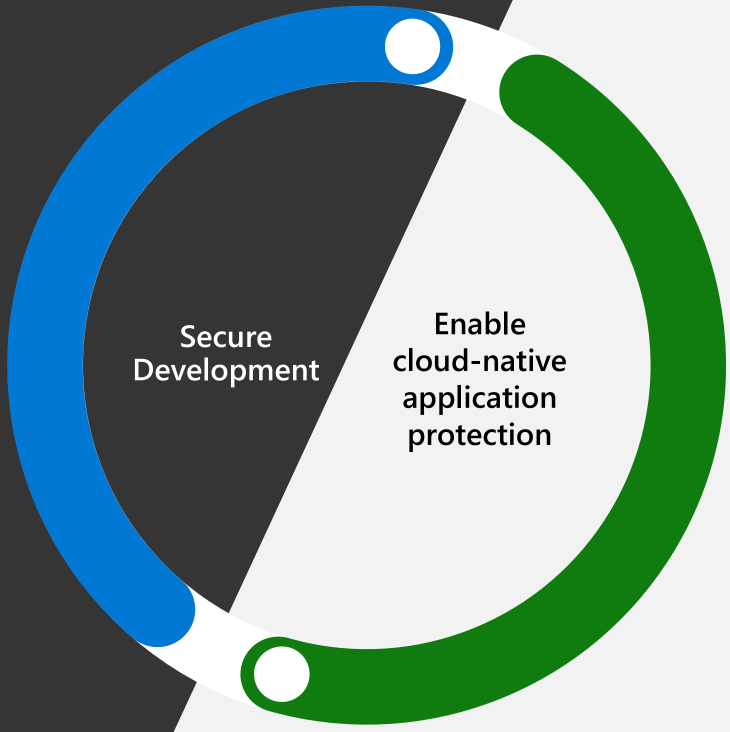
@_sarahyo
@sarahyo.com

Posture management

- CSPM tooling continually assesses your security posture and can track and identify vulnerabilities.
- CSPM tooling can also provide recommendations to harden your infrastructure.
- Some CSPMs can remediate vulnerabilities and misconfigurations.
- Microsoft’s CSPM tool is called Microsoft Defender for Cloud (the artist previously known as Azure Security Center).

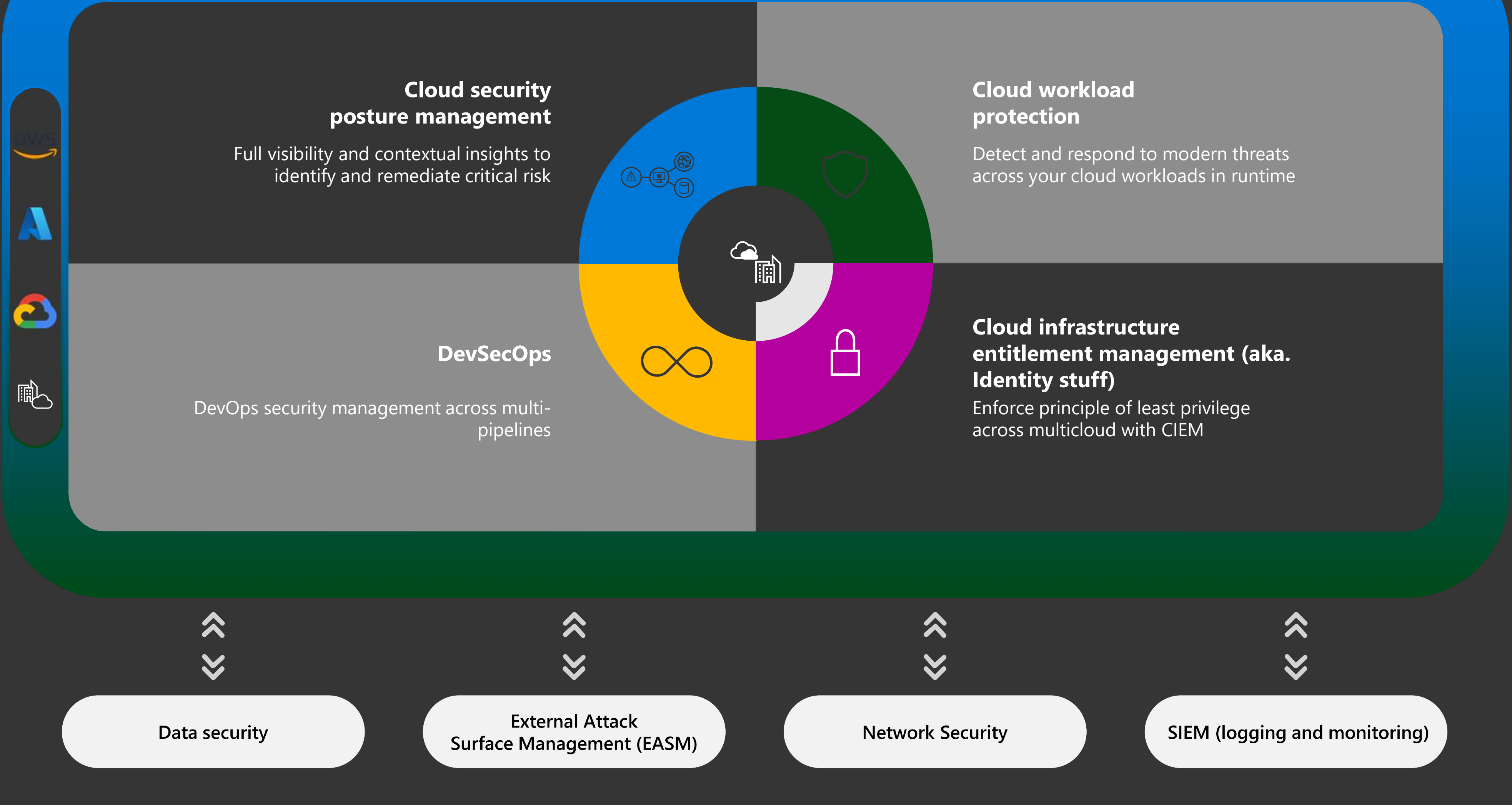
DevSecOps

- Code security
- Dependencies security
- Embedded secrets protection
- Developer code remediation



- Multi-pipeline DevOps security management
- Infrastructure-as-Code security
- Code to cloud contextualization
- Automated workflows

Security capabilites that you should have



Cloud security posture management

Full visibility and contextual insights to identify and remediate critical risk

Cloud workload protection

Detect and respond to modern threats across your cloud workloads in runtime

DevSecOps

DevOps security management across multi-pipelines

Cloud infrastructure entitlement management (aka. Identity stuff)

Enforce principle of least privilege across multicloud with CIEM

Data security

External Attack Surface Management (EASM)

Network Security

SIEM (logging and monitoring)

Thank you, OWASP NZ Day!

@_sarahyo
@sarahyo.com