RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands


SESSION ID: SPO-W09A

# Uncovering Infinity Stones in Cyber Security

*Powers & Abilities*

**Jordan Koh**

Cyber Security Adviser
Silverlake MasterSAM
@SMasterSAM

RSAConference2019
Asia Pacific & Japan

# What are our Powers and Abilities?

# What is Power?

- Outside-in : Granted to a person by someone
- Inside-out : Ability of individual to cultivate by themselves
- By choices someone makes, actions they take
- Real Power is **CLARITY**

# Do we have this clarity in the cyber world?

**14,717,618,286**
Since 2013

**3,353,172,708**
1st half of 2018

**6,204,729** **258,204** **4,303** **72**

# Is this the clarity we wish to have?

Clarity allows the security team to know which asset is the most critical, most vulnerable, and most accessible to attackers.

# New villains keep emerging

**63.59%**

**Breach by Identity Theft**

**Awareness**

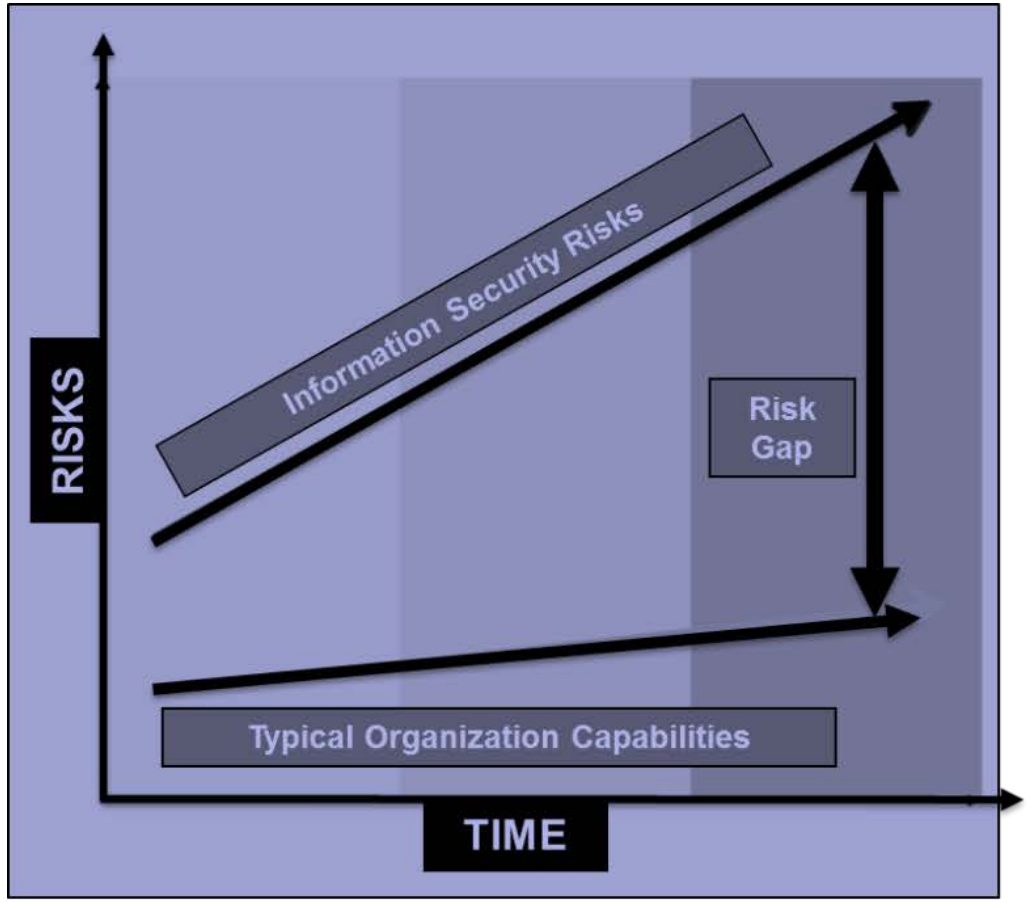
**Security incidents**

RSAConference2019
Asia Pacific & Japan

# Do we have this clarity in cyber world?

**there is no 100% security in the digital world**

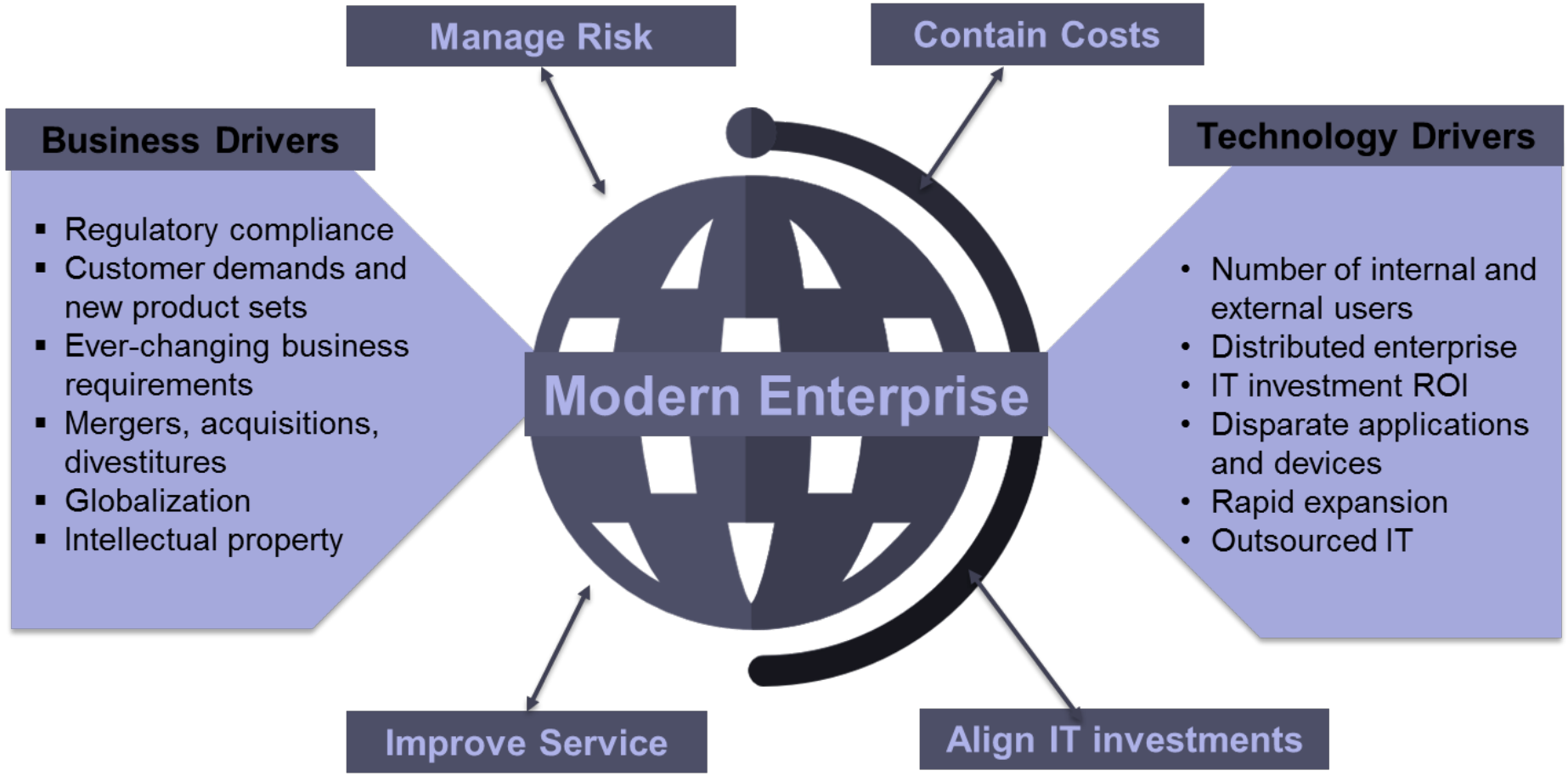
# Steady increase in Risk Gap



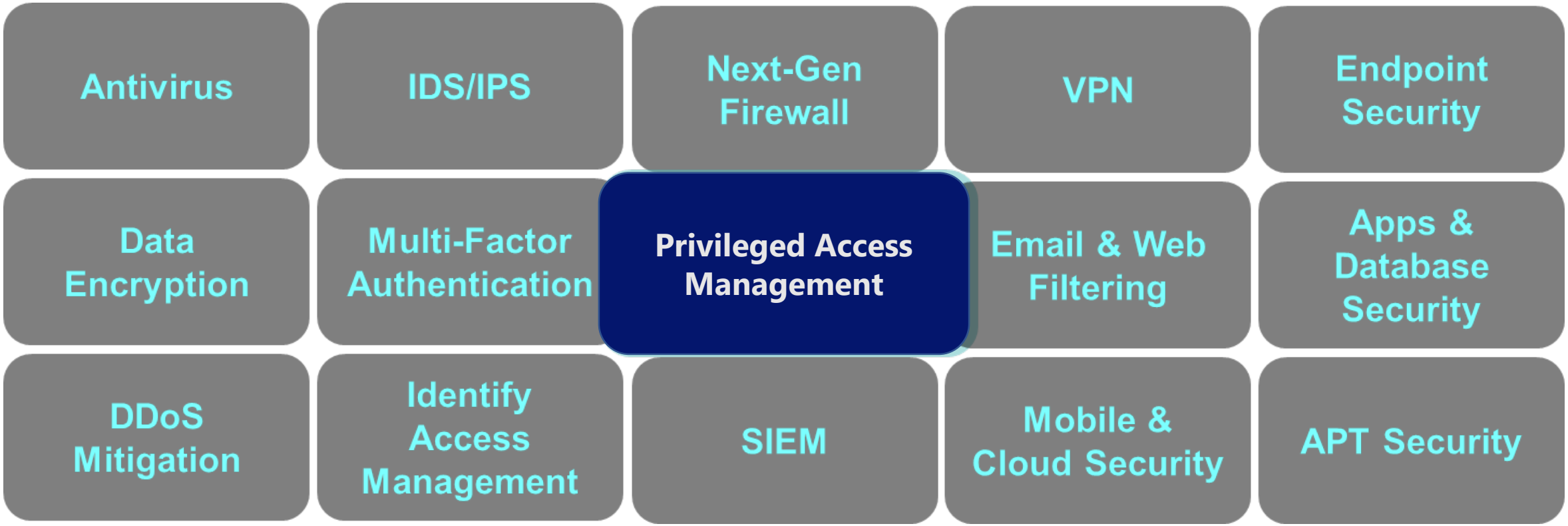

| Trends in the market |
| --- |
| Proliferation of data through the use of mobile devices |
| Excessive access rights and management of privileged accounts |
| Externalization and sharing of data with individuals, organizations, etc. |
| Move to cloud-based solutions (salesforce.com; Workday) |
| Advanced persistent threats and other advanced cyber attacks (hacking as a business; cyber espionage) |
| Attacks via social networks |
| Shortened product development lifecycles and rush to market |
| Difficult global economic environment |

Source : Deloitte, 2012: Think. Transform. Integrated Identity Management and its Impact on Governance, Audit, and Security

# A shift towards enabling technology to address the unknowns



# Security is getting complex



RSAConference2019
Asia Pacific & Japan

# PRIVILEGE ACCESS MANAGEMENT

## Infinity Stones

RSAConference2019
Asia Pacific & Japan

# Understand your powers

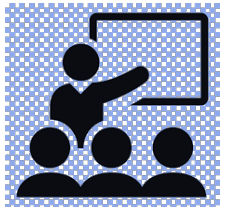
“Even with the most technologically advanced and capable cyber defence system in place, the **weakest** link will still be the **human** element”

# User Education

**Training should be continuous, incremental and hard-coded**

Cyber Security certifications

Well-conducted cyber response drill



End user Training

# User Education

## Where to begin?

- **Exposure, Exposure, more exposure**
- **Review Post breach investigation studies**
- **Participate in Security Events**
- **Networking**

“We discovered in our research that insider threats are not viewed as seriously as external threats, like a cyberattack.

But when companies had an insider threat, in general, they were much more costly than external incidents.

This was largely because the insider that is smart has the skills to hide the crime, for **months**, **sometimes**, **forever**”

- Dr. Larry Ponemon, SecureWorld Boston

# Auto Discovery

**Helps organisations to identify all available infrastructure assets**

# Auto Discovery

## Where to begin?

- Catalogue each resource in your IT environment, and update it every 3 months
- Perform a spot check on the inventory from time to time to ensure it is up to date
- From our experience, most customers have lists that only covers 80% of their resources

“Treat your password like toothbrush. Don’t let anybody else use it and get a new one every six months”

- Clifford Stoll

# Password Management

**Storing and managing passwords in an efficient manner to secure and prevent unauthorised access**


# Password Management

## Where to begin?

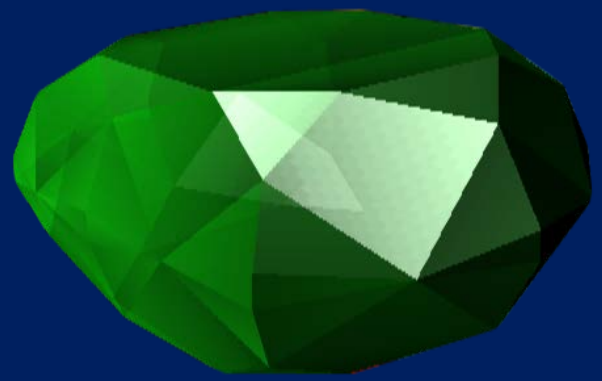
- **Enforce dual control policy**
- **Enforce scheduled password change – one can do this manually if they do not have a PAM product**

RSAConference2019
Asia Pacific & Japan

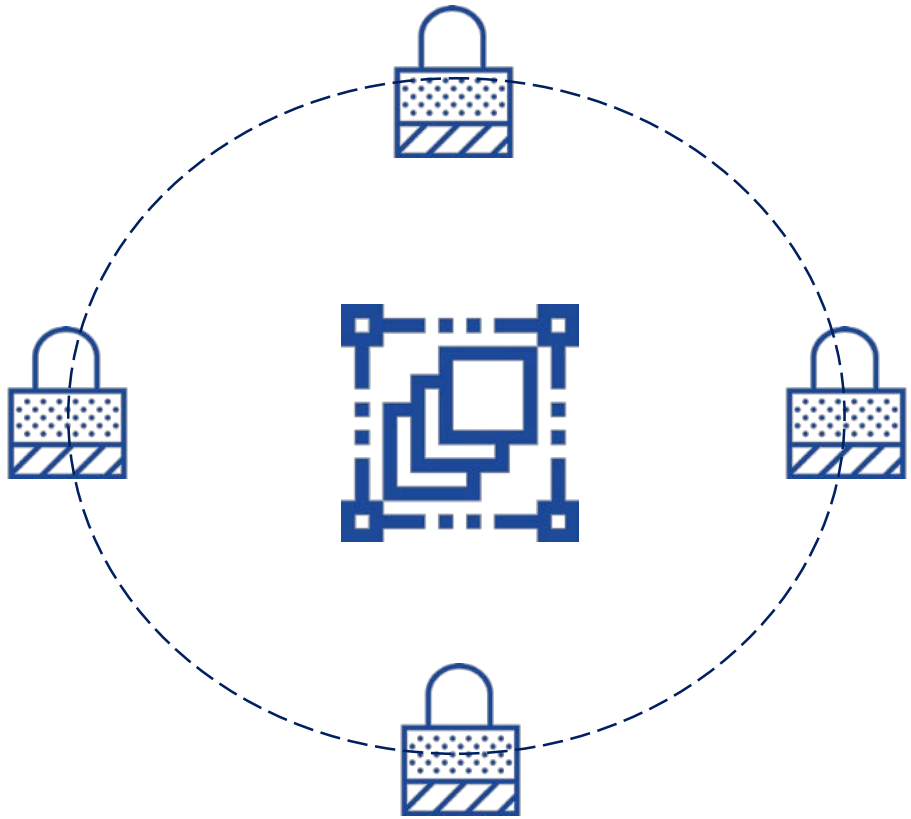
**“True cybersecurity is preparing for what is next, not what was last.”**

Neil Rerup, Cyber Security Expert

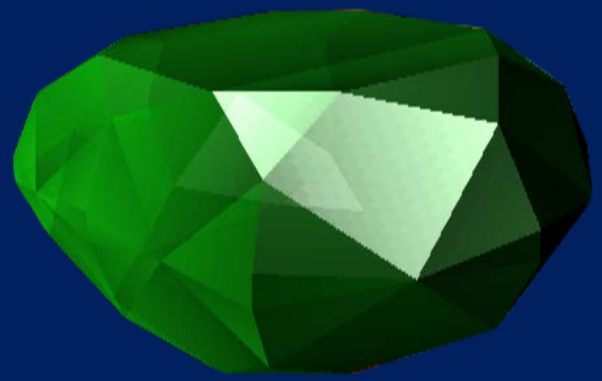
# Access Control



**Access control provides fine grained control over what a user can access**



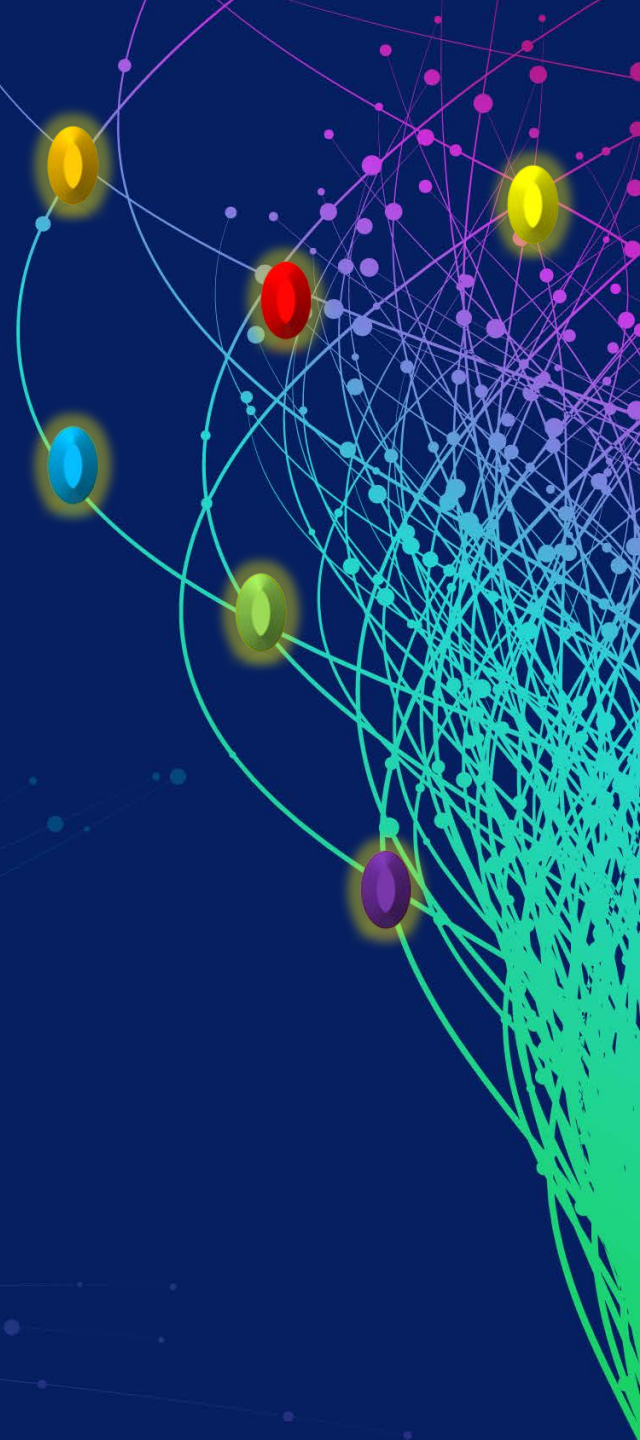
# Access Control



## Where to begin?

- Begin with your employees, team members, their resources
- Define clearly the access control each person should have on each resource
- Ensure this is done periodically
- As CIO/CISO one should have this information with him all the time

RSAConference2019
Asia Pacific & Japan

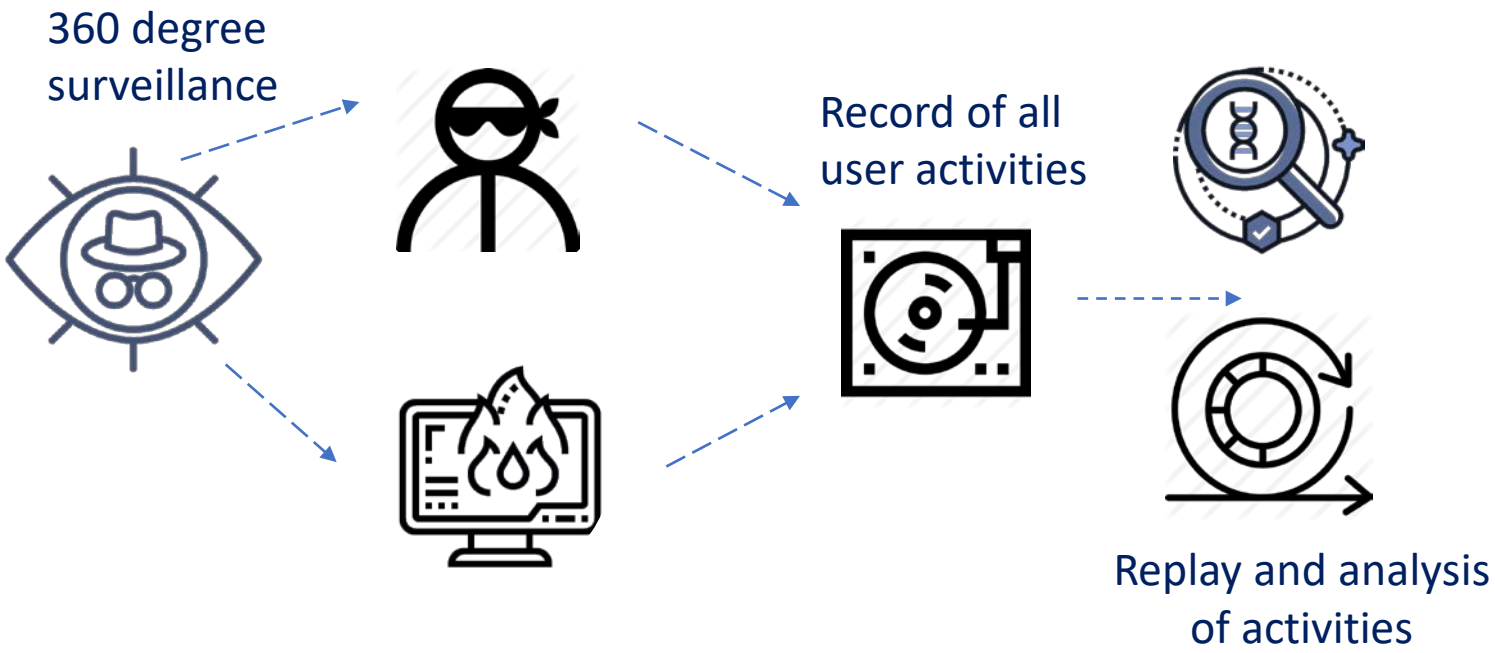


# “You can’t fight what you can’t see”

- Cyber Security Enthusiast

# Surveillance

## Monitoring and recording of user activities for audit and forensic

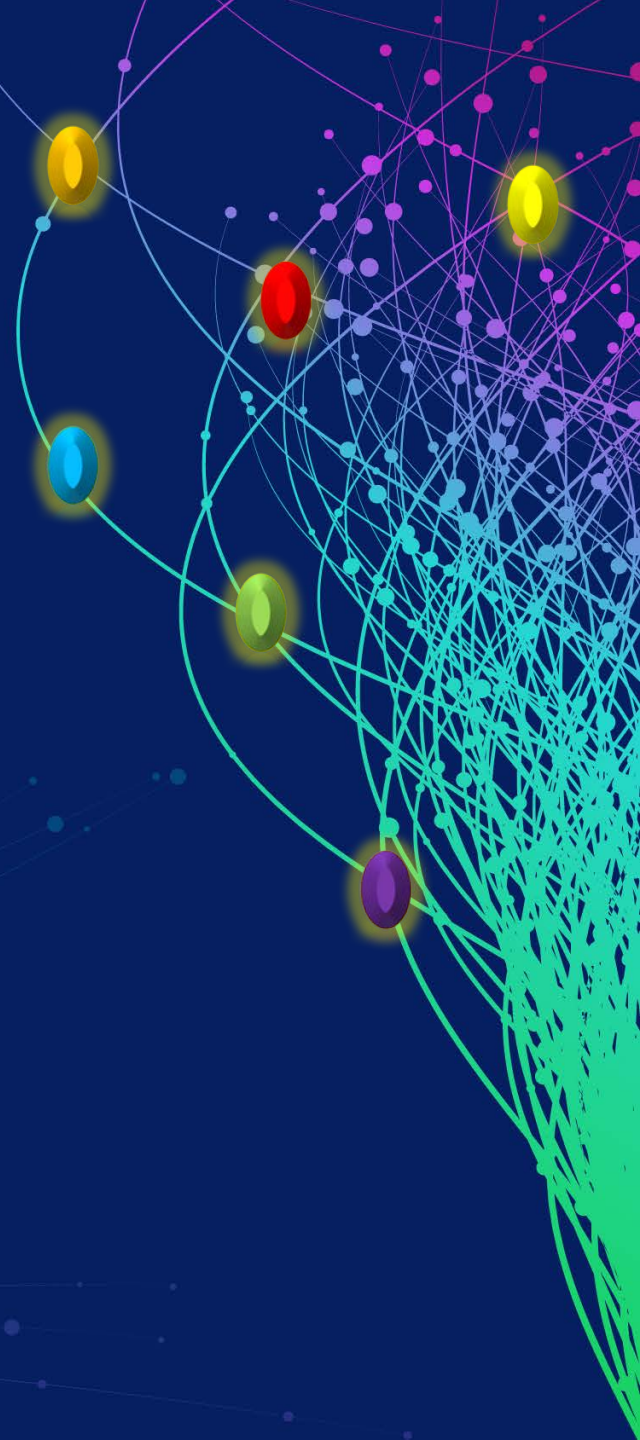


# Surveillance

## Where to begin?

- **Ensure you have adequate surveillance**
- **Could be in the form of CCTV, PAM software, or manual surveillance by having an internal staff to escort and monitor what the vendors do**

RSAConference2019
Asia Pacific & Japan



**“Cyber threats don’t happen in a vacuum. Nor should investigations”**

- Cyber Security Enthusiast

# Audit Compliance

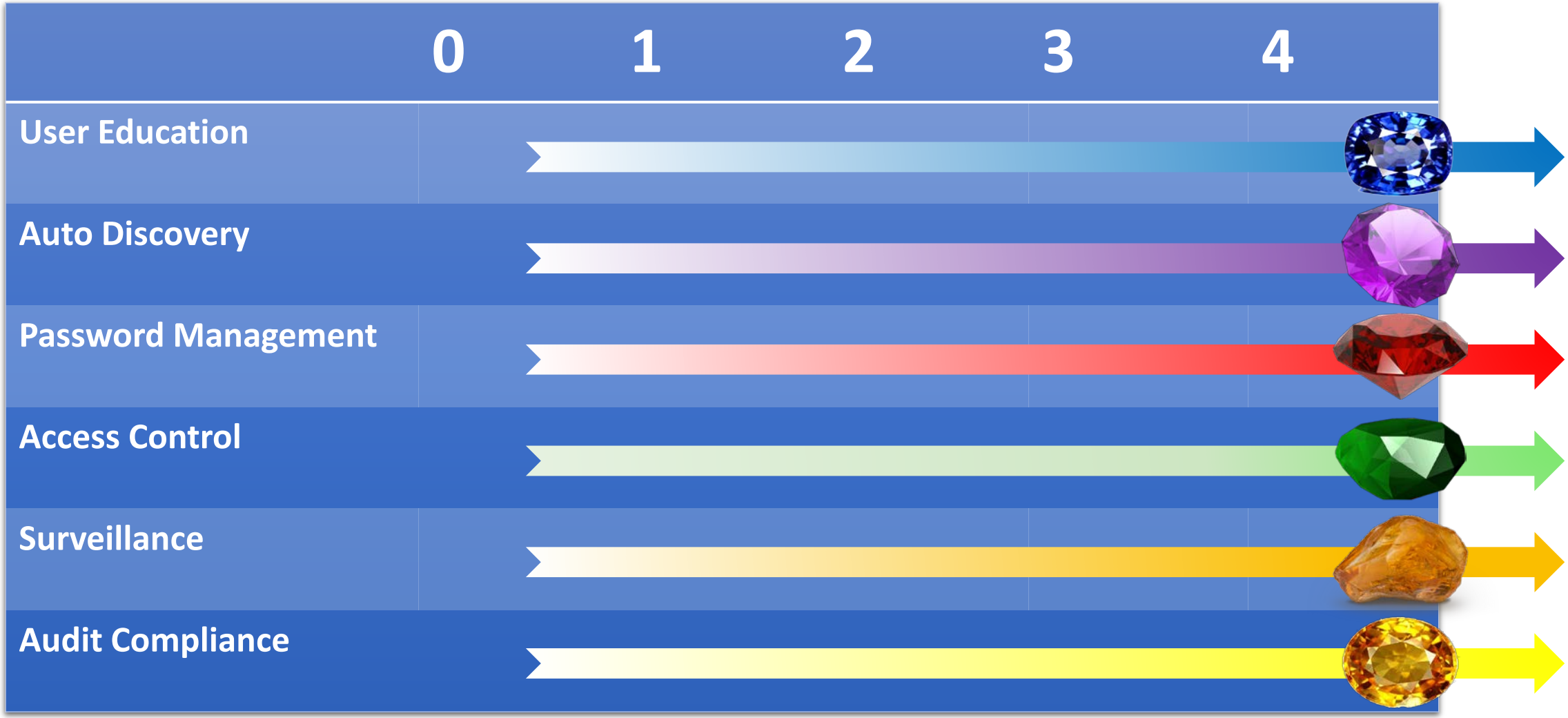
**Manual or systematic measurable technical assessment of a system of application**

# Audit Compliance

## Where to begin?

- **Set up internal teams to perform audit of all security related infrastructure**

# Make a **small** step in the journey



RSAConference2019
Asia Pacific & Japan

| | 1 | 3 | 6 |
|---|---|---|---|
| User Education | Read | Learn | Teach |
| Auto Discovery | Identify | Detect | Control |
| Password Management | List | Secure | Change |
| Access Control | Rights | Matrix | Refine |
| Surveillance | Record | Review | Alert |
| Audit Compliance | Study | Apply | Comply |

Cybersecurity is not the task of single department in an organisation.

It only requires a weak link to undermine all the investments and effort by every other person in the organisation.

RSAConference2019
Asia Pacific & Japan

"This is the fight of our lives. We are going to win. Whatever it takes"

Steve Rogers