Managing BYOD Networks

What is BYOD

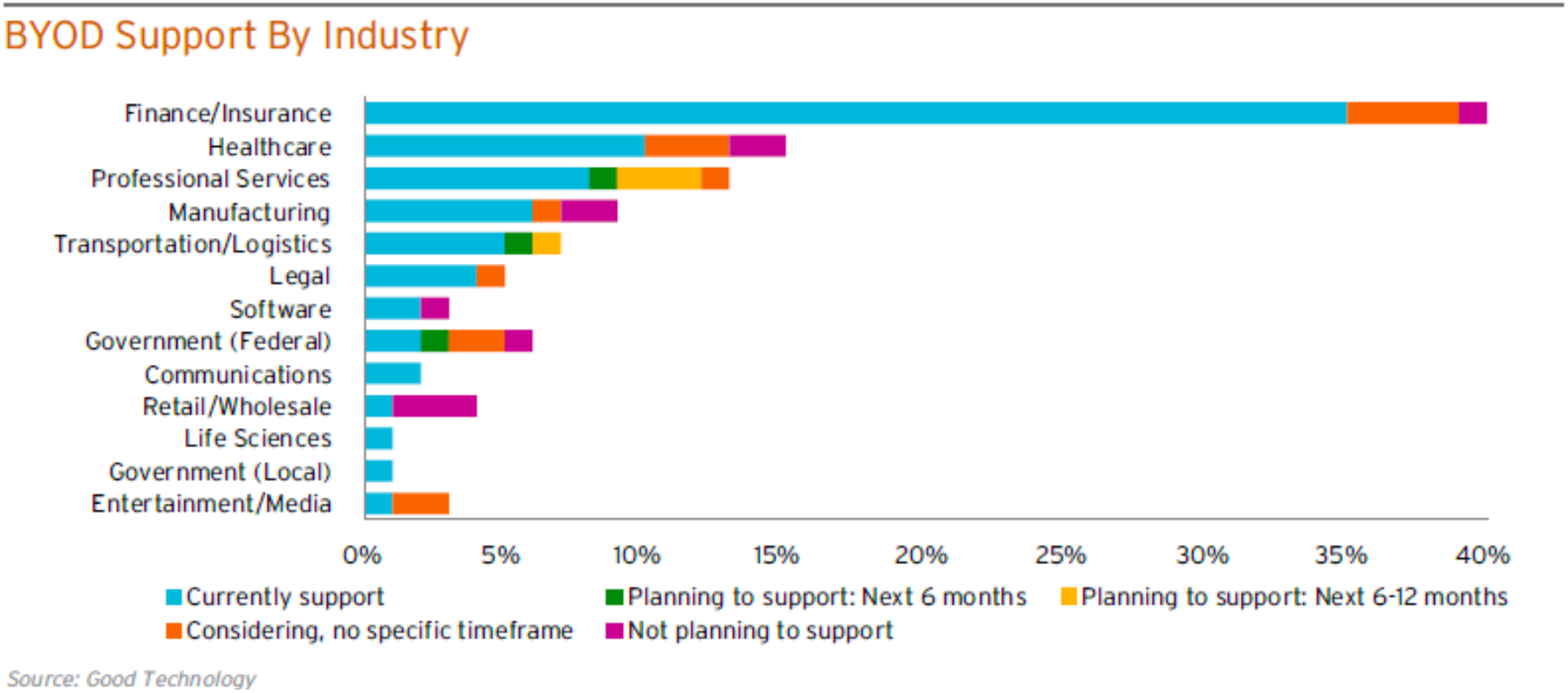
Bring Your Own Device

Are you allowing a Rogue ?

Why BYOD

- Increased productivity and employee satisfaction
  - Employees can respond to work requests outside work hours
  - Employees report higher satisfaction with flexible working hours
  - The traditional work place has morphed – airports, coffee shops
- Penetration of IT into homes
  - Emails, social networking, digital entertainment, net-banking
  - Highly capable laptops, tablets and smartphones found in many homes
- Employees do not wish to carry multiple devices
  - Personal IT devices are more capable than the corporate device
- Attracting, retaining and supporting new talent
  - Employees seek work environments that foster freedom on choice of tools and technologies
- Lower IT procurement, support costs
  - Employees procure, maintain and upgrade their own devices

Who is adopting BYOD



Source: Good Technology

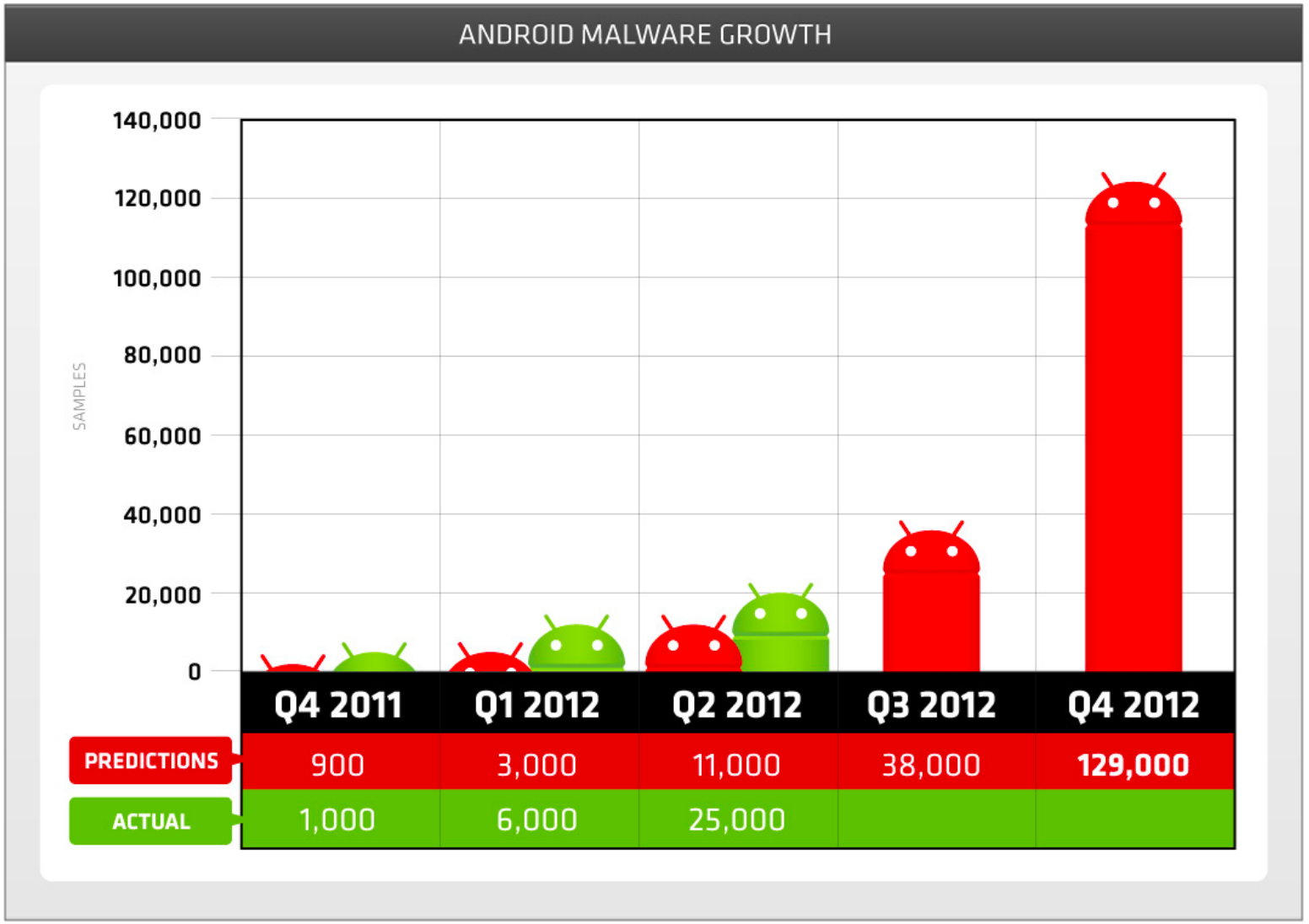
Universities are pioneers of BYOD

Out of necessity

Risks of BYOD

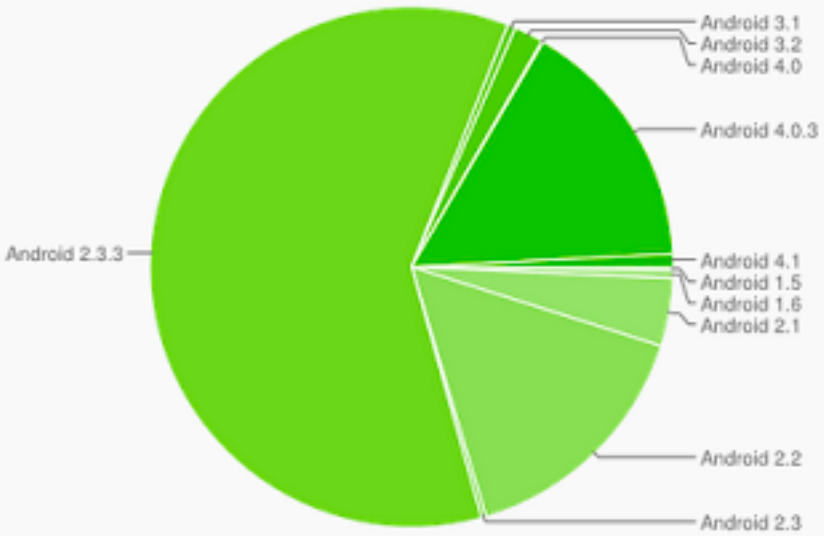
- Corporate data loss
  - Legal and Financial consequences of inappropriate use of data
  - Staying compliant and preventing privacy breaches – regulatory challenge
  - Intellectual Property loss – e.g. the iPhone 4 was lost even before launch
- Application Security
  - Freeware or Malware or Spyware
  - Greater than 80% Android and IOS Apps access sensitive information such as location, calendars, address books. Many share information with service providers, app developers and possibly 3rd parties.
- Device security
  - Stolen/lost devices can get back into the network
  - In a survey greater than 40% of personal device users did not have device unlock passcodes
- Support costs may escalate
  - Device variety and heterogeneity can be overwhelming
  - Absence of suitable infrastructure can be human resource intensive

Growth of Android Malware



Outdated Versions of Android

Version	Codename	API Level	Distribution
1.5	Cupcake	3	0.2%
1.6	Donut	4	0.5%
2.1	Eclair	7	4.2%
2.2	Froyo	8	15.5%
2.3 - 2.3.2	Gingerbread	9	0.3%
2.3.3 - 2.3.7		10	60.3%
3.1	Honeycomb	12	0.5%
3.2		13	1.8%
4.0 - 4.0.2	Ice Cream Sandwich	14	0.1%
4.0.3 - 4.0.4		15	15.8%
4.1	Jelly Bean	16	0.8%



BYOD Administration

Plan for BYOD Adoption

- Accept the inevitable – plan proactively.
  - Plan for a phased roll out. Begin with a smaller a target user segment and limited device type and limited application support. Expand coverage in phases.
- Define a BYOD strategy with a governance plan and an acceptable use policy that users must sign up to.
  - Specify security requirements and practices based on employee roles and devices types
  - Explain user liabilities and responsibilities
  - Address employee privacy concerns
  - Develop plans for violations
- Deploy a BYOD Authorization and a Network Access Control as a first line of defense
- Deploy security and management tools to monitor and manage BYOD threats

Solution Architecture for BYOD

Registration

Self Help Portals

KYC procedures

Reduce Risk

Provision configuration, monitoring agents

Device registration using digital certificate

Continuously Assess

Authentication

Enforce Compliance

Regulate Access

Attribute based access control

Device, Location, Time, User Role based

Monitor

Deploy Data Mining, Analytics

Track User activity, Traffic

Self Help Registration Portal

- User friendly secure device registration, provisioning portal
  - Potential to reduce IT support costs
  - Redirect unregistered devices to self help portal
  - Enable user to register device with a browser
    - Provisioning wizard to guide user through the process
    - Process may include checkpoints for administrator intervention/authorization
  - Deploy device specific supplicant for security posture check and monitoring
    - Cater to heterogeneous device and OS variety
  - Provision digital certificates chained to organization Root CA

- De-provisioning, De-registration
  - Device loss or theft
  - Employee self help page for device management
  - Revoke all Digital Certificates issued to the user/device
  - Blacklist Access

Certificate Infrastructure

- Maintain a Root Certificate Authority (CA)
  - Organization MUST only trust client certificates that can be traced back to a Root CA controlled by the organization.
  - An intermediate CA chained to the Root must issue final certificates
- Certificate Attributes
  - Must include Device specific information – e.g. MAC address
  - Must have low life time – recommend 6 months
- Certificate Revocation check should be enforced
  - CRL should be “always available”
- Scalable to maintain high volume of certificate issue/renew/revocation activity

Central Authentication

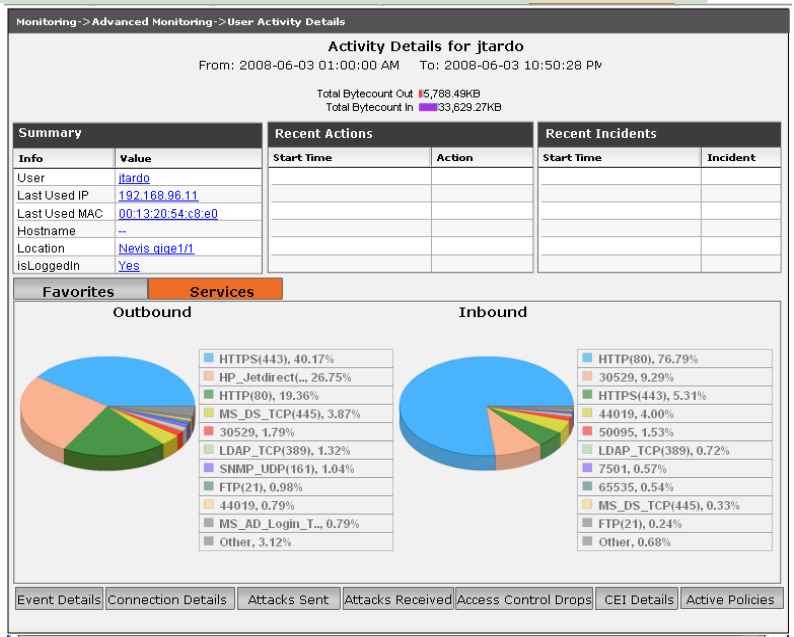
- Maintain Enterprise wide User and Device Identity
- Maintain User/Device groups and manage memberships
- Scalable to address organization growth
  - Headcount
  - Geographical spread – low latency, replicated
  - Authentication Rates – Monday morning flood
- Support digital certificate based identity verification

Network Access Control

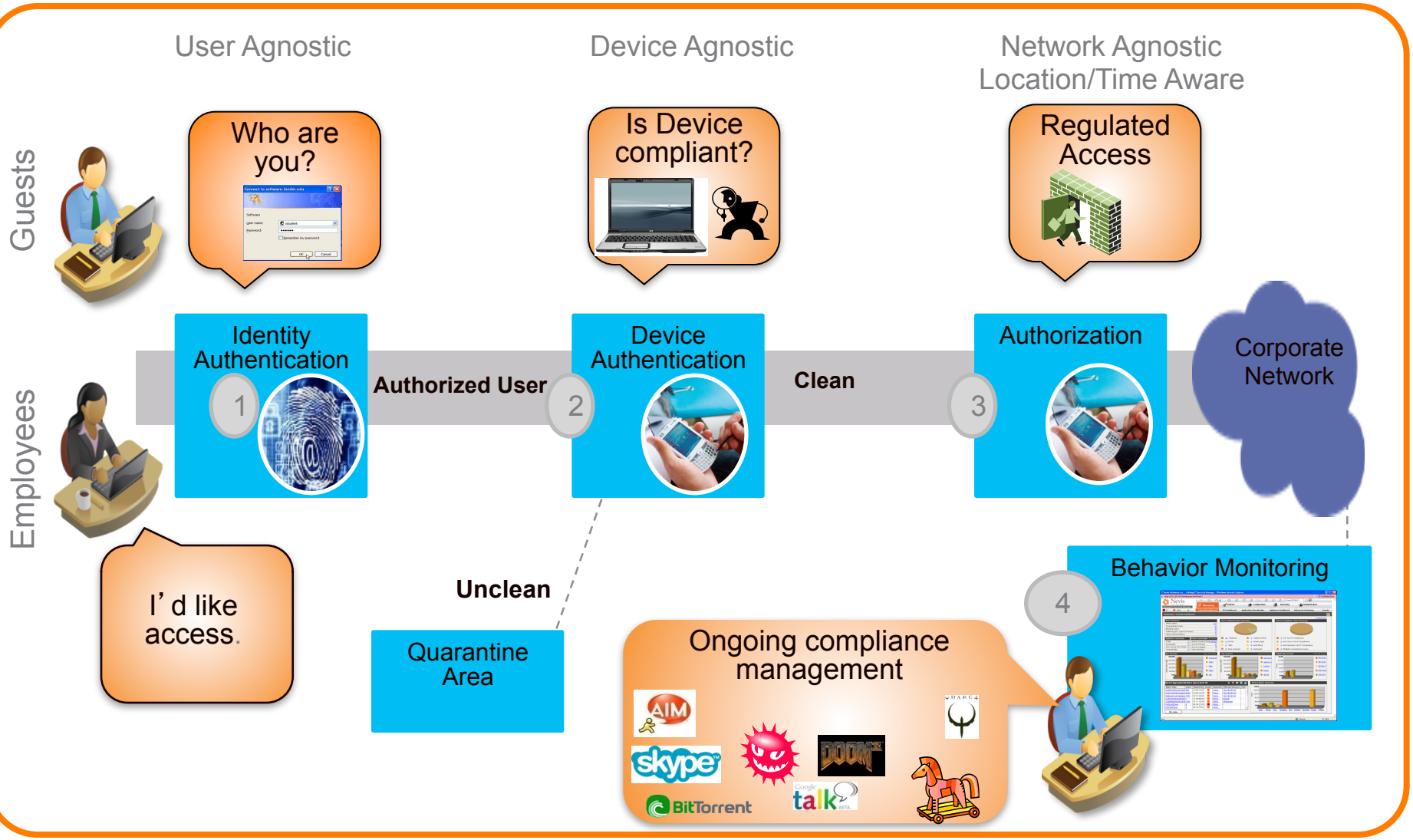
- User and Device ID established via digital certificates and central authentication server
- Registered Devices
  - Typically employee owned and employee registered via self help portal
  - Granted partial or full access based on Device category and Employee group membership in Central Authentication server
- Whitelist
  - Corporate owned and provisioned device list manually administered
  - Access control pre-determined by administrator – mostly Full Access
- Blacklisted devices denied access, can be reinstated
- Posture checks by supplicant
  - Ensure passcodes for device “unlock” are implemented
  - Verify OS/Application versions, verify “permitted/disallowed applications”
  - Disable Cameras and other accessories when “plugged into network”
  - Check for “Jail break” devices

Monitor and Log User/Device Traffic

- LAN based IPS
  - Malware injection points are now spread throughout the network – no longer a single perimeter gateway problem
  - Signature based
  - Anomaly based
- Deploy data mining and Analytics
  - Provision flow logging
    - Get visibility
    - E.g. Netflow/S-Flow
  - Provision user and device network access logging
  - Archive logs
    - Plan for storage scale
  - Deploy correlation tools to simplify log analysis and shorten incident response times



BYOD Network Process



Thanks

Q&A