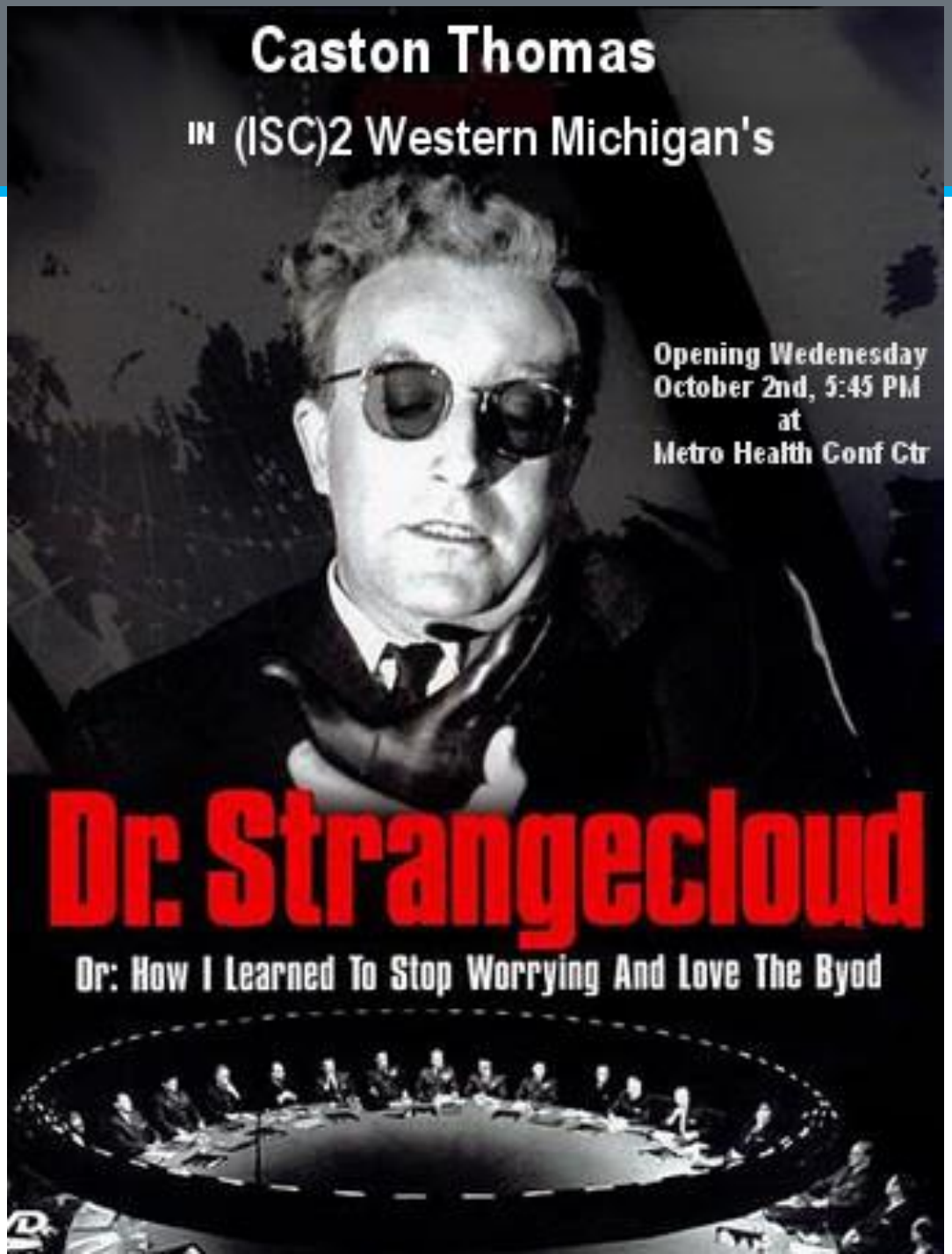

Caston Thomas
IN (ISC)2 Western Michigan's
Opening Wedenesday
October 2nd, 5:45 PM
at
Metro Health Conf Ctr
Dr. Strangecloud
Or: How I Learned To Stop Worrying And Love The Byod

The BYOD Phenomenon

"68% of devices used by information workers to access business applications are ones they own themselves, including laptops, smartphones, and tablets."

"IT organizations underestimate the number of personal mobile devices on their network by 50%."

"By 2020, 70% of '4 Pillar Solution' buyers will have the LOB as their buyer."

4 Pillars = mobile, cloud, big data, social media

[1]IDC Research, The Mobility Game Changer, June 2013

What is BYOD?

Option 1:

BYoD refers to employees using their own devices – to access the corporate network or corporate cloud based applications

Option 2:

BYoD is a change in how we move the cost of computing from corporate owned devices to personally owned devices.

Option 3:

BYoD is the fundamental change in how we view ownership of, not just devices, but also data, applications, & network. It changes how we approach our company's security, culture, & responsibility.

Fight or Embrace?

"The rise of "BYoD" is the single most radical shift in the economics of client computing for business since PCs invaded the workplace." **- Gartner[1]**

"The rise of "BYoD" is the single most radical cultural shift in the corporate workplace since the typewriter."

- Caston Thomas

[1] Gartner "Bring Your Own Device: New Opportunities, New Challenges", August 16, 2012


20 Critical Security Controls
for Effective Cyber Defense
1 Inventory of Authorized and Unauthorized Devices
2 Inventory of Authorized and Unauthorized Software
3 Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers
4 Continuous Vulnerability Assessment and Remediation
5 Malware Defenses
6 Application Software Security
7 Wireless Device Control
8 Data Recovery Capability
9 Security Skills Assessment and Appropriate Training to Fill Gaps
10 Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11 Limitation and Control of Network Ports, Protocols, and Services
12 Controlled Use of Administrative Privileges
13 Boundary Defense
14 Maintenance, Monitoring, and Analysis of Security Audit Logs
15 Controlled Access Based on the Need to Know
16 Account Monitoring and Control
17 Data Loss Prevention
18 Incident Response Management
19 Secure Network Engineering
20 Penetration Tests and Red Team Exercises

SANS Critical Controls

Critical Security Control	NAC Capability	Advice for Automation
1 Inventory of Authorized and Unauthorized Devices	NAC can obtain the identity, device, network and authorization attributes of systems connecting to (and connected on) the network. NAC responses to detected devices include the capability to classify, assess, alert, report, segment, enforce and mitigate.	Use NAC to identify and classify what's requesting access to network resources; then focus on devices that you haven't authorized to determine if they are wanted or unwanted. NAC policy can block or reassign unknown devices to a segmented LAN for further investigation. NAC can generate tickets and report on such events.
2 Inventory of Authorized and Unauthorized Software	By inspecting a device and comparing its configuration against policy (on access request, post-access or at polling intervals), NAC can fingerprint installed and running software and assess if the system configuration adheres to policy.	Use NAC to maintain and enforce a blacklist or whitelist of approved software versions. Provide automated response based on policy in the event of unapproved application use, such as a noncorporate IM or P2P tool. NAC can generate tickets and reports on such events.
3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	By virtue of identifying and enforcing OS patches and host-based protection before a device connects to network resources, NAC reduces the attack surface by closing vulnerabilities attackers look to exploit.	Define policies for what is an acceptable configuration based on device type and usage. Maintain secure configurations through NAC-initiated scans as devices attempt access. Automatically execute remediation if the device is out of compliance. Integrate MDM device-level controls (device, application, data) with NAC network-based controls to secure BYOD/CYOD devices.
4 Continuous Vulnerability Assessment and Remediation	NAC can identify and remediate or block suspicious and vulnerable nodes. NAC can be leveraged to initiate an immediate vulnerability assessment (VA) scan on new network devices.	Tune NAC enforcement policies based on device, user, resource request and configuration or host-based protection violation scenarios. Integrate NAC with vulnerability assessment tools to trigger vulnerability scans of new devices attaching to the network and to isolate and remediate vulnerable systems.
5 Malware Defenses	NAC complements host-based protection to ensure malware defense is installed, active and up-to-date when requesting network access. Some NAC platforms offer post-network admission behavior analysis to respond to suspicious or malicious behavior. For example, it can check the state of active antivirus or DLP software on the device. If the software is out of date or absent, NAC can automatically isolate the device from the network until it is brought into compliance.	As above, dictate policy for when NAC discovers host-based protection issues or suspicious behavior; integrate NAC events with other reporting systems such as SIEM. Use NAC as a first-line "circuit breaker" defense to stop zero-day malware propagation.
7 Wireless Device Control	NAC works with WAPs and wireless networks to enable guest management and role-based device authentication with or without relying on an 802.1X-managed supplicant on the device. NAC can identify and isolate rogue WAPs and provides network-based enrollment, on-access profile checks and network-based enforcement, which fortifies MDM-based device, user, data and application controls. NAC enforcement also supports WLAN reassignment.	Leverage NAC-related features with wireless network and MDM platforms in place in your organization. Through integration with MDM suites, automatically enforce controls on devices across the network that would be enforceable only by MDM across the cellular network. (An increasing number of MDM vendors offer NAC integration capability.)
8 Data Recovery Capability	Host-based backup protection software cannot always ensure that it is installed, running and up-to-date. NAC endpoint security policy can provide a complementary control to ensure such protection is active.	Configure NAC to automatically verify installation and run state of host-based backup and encryption software.

SANS Critical Controls

Critical Security Control	NAC Capability	Advice for Automation
11 Limitation and Control of Network Ports, Protocols, and Services	Role-based access control (RBAC) enforcement explicitly allows only trusted network traffic using valid protocols to cross through ports and services that are approved as per policy. NAC complements endpoint protection to ensure that host-based firewalls and filtering tools are installed and running.	Enable NAC to restrict network traffic to known devices and valid profiles based on device, configuration and role. Use NAC to identify and eliminate unapproved protocols, ports and services on devices requesting access and post-admission to the network. Enforcement can range from alerting to limiting or blocking access.
13 Boundary Defense	NAC can identify users and devices connecting remotely, such as devices gaining access via VPN and that are in need of configuration, patching or software update.	Enable pre-admission NAC monitoring and defenses to take action on out-of-spec devices. Isolate, report and remediate automatically. Integrate NAC as much as possible with other event correlation sources, including firewalls, SIEM systems and VPNs.
14 Maintenance, Monitoring, and Analysis of Audit Logs	NAC can verify, activate and update logging applications, services and settings on endpoints. Beyond NAC events being sent to logging systems, NAC can also send endpoint configuration details to SIEM platforms.	Configure NAC to integrate with the current logging or SIEM platform. Enable NAC profile check to verify and remediate endpoint logging. Determine if and where SIEM can leverage NAC endpoint mitigation capabilities.
15 Controlled Access Based on the Need to Know	NAC can fortify and enforce role-based access control leveraging directory services and VLAN network segmentation. NAC can also assure the installation and use of host-based DLP tools.	Phase in NAC enforcement controls and enforce the use of DLP client software. Integrate NAC with DLP tools as they become active to include the status of these DLP tools during endpoint scans.
17 Data Loss Prevention	NAC can assure the installation and use of host-based DLP security on the endpoint.	Phase in NAC enforcement controls and enforce the use of DLP client software and the use of storage peripherals.

The Risks of BYOD

- Data loss
  - Lost phone or laptop
  - Unauthorized access
  - Compromised systems
- APT/Malware
  - Threats in the network
- Compliance
  - Rogue infrastructure
  - Unauthorized apps (e.g., dropbox)
  - Unauthorized data (e.g., drug interaction)

For more depth, see:

Gartner,"Strategic Road Map for Network Access Control",
Lawrence Orans and John Pescatore,11 October 2011

Gartner Recommendations

"No matter what BYOD strategy is selected, the ability to detect when unmanaged devices are in use for business purposes will be required — and that requires **NAC**."

Gartner, "NAC Strategies for Supporting BYOD Environments", 22 December 2011, Lawrence Orans and John Pescatore

What Are Your BYOD Solution Options?

SOLUTION	CHARACTERISTICS

What Are Your BYOD Solution Options?

SOLUTION	CHARACTERISTICS
Manage all personal devices (MDM)	• Good security at the device level • Often ignores Win/Mac/Linux • Separate management console • Minimal network protection

What Are Your BYOD Solution Options?

SOLUTION	CHARACTERISTICS
Manage all personal devices (MDM)	• Good security at the device level • Ignores Windows and Macs • Separate management console • No network protection
Restrict the data (VDI)	• Strong information protection • Poor user experience • Not for the road warrior

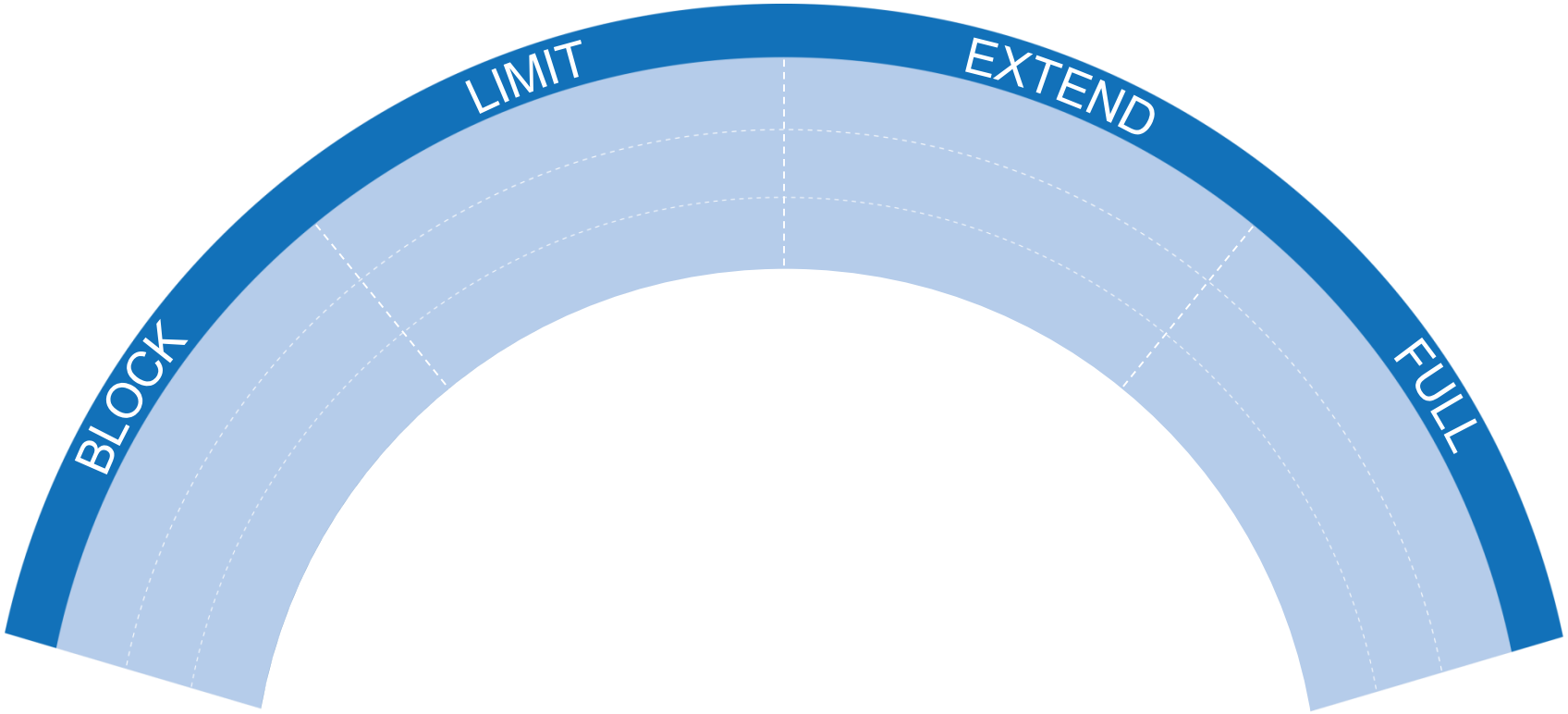
What Are Your BYOD Solution Options?

SOLUTION	CHARACTERISTICS
Manage all personal devices (MDM)	• Good security at the device level • Ignores Windows and Macs • Separate management console • No network protection
Restrict the data (VDI)	• Strong data protection • Poor user experience • Not for the road warrior
Control apps (MAM, MAW)	• Leading edge approach • Often used with other controls

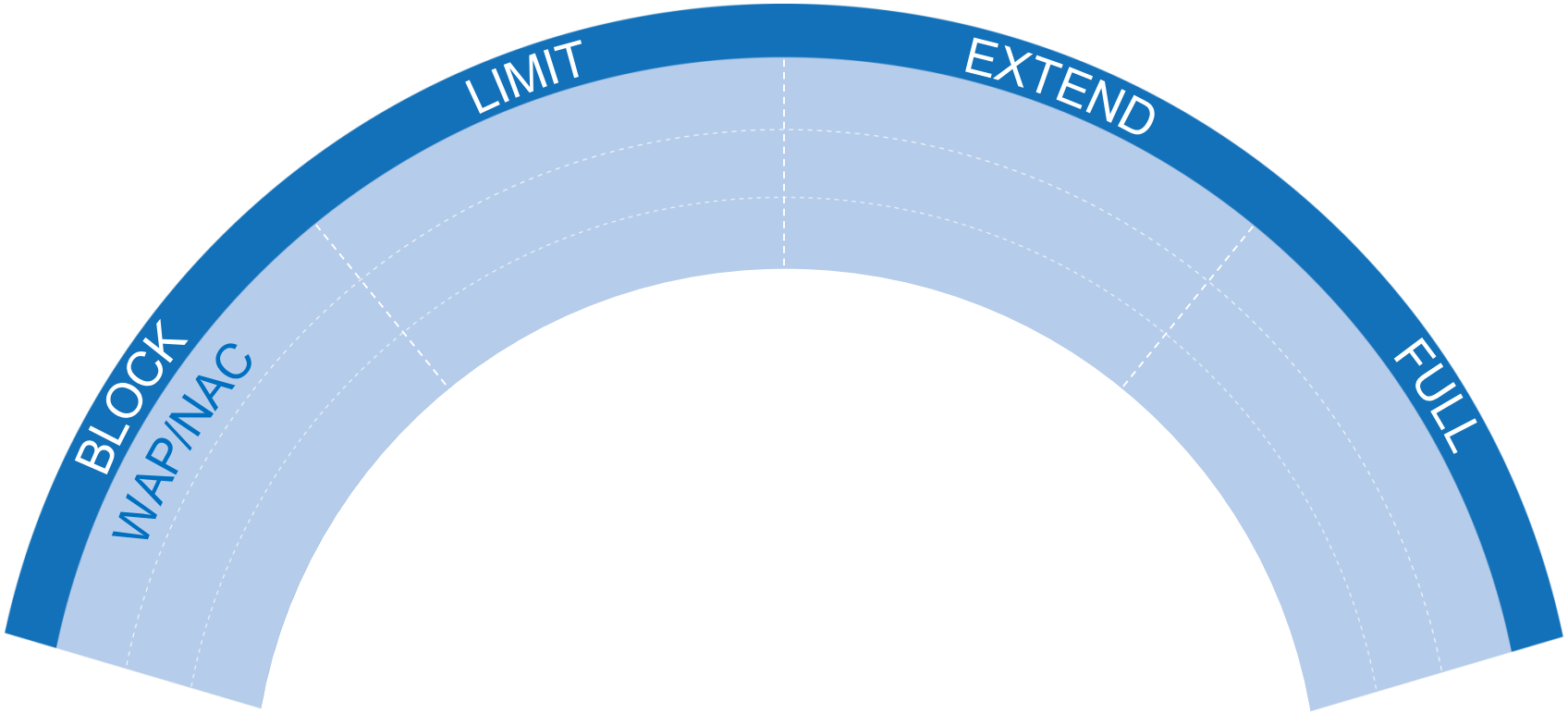
What Are Your BYOD Solution Options?

SOLUTION	CHARACTERISTICS
Control devices (MDM)	• Good security at the device level • Ignores Windows and Macs • Separate management console • No network protection
Control data (VDI)	• Strong data protection • Poor user experience • Not for the road warrior
Control apps (MAM, MAW)	• Leading edge approach • Must be used with other controls
Control the network (NAC)	• Simple, fast, 100% coverage • Protects data on the network, not on the device

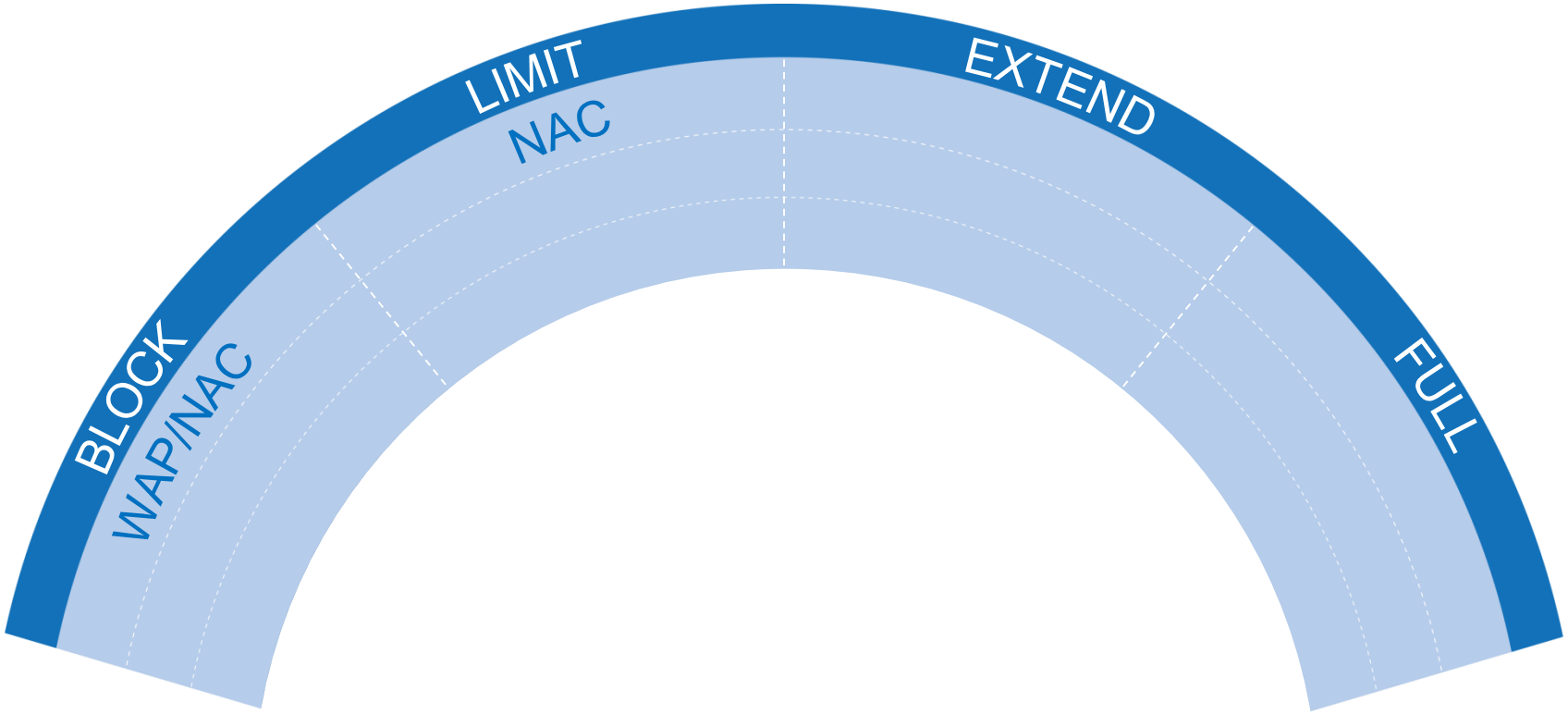
Multiple Security Choices



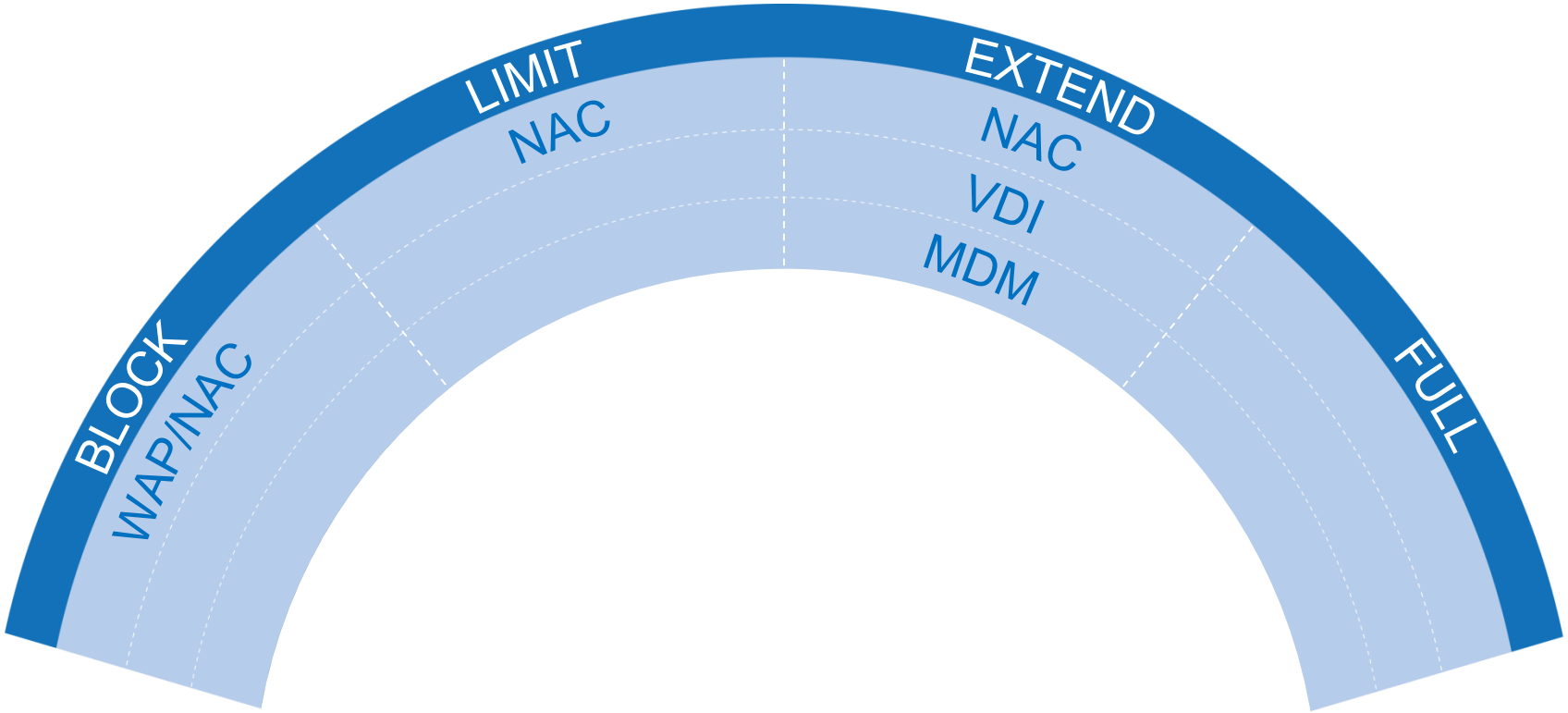
Multiple Security Choices



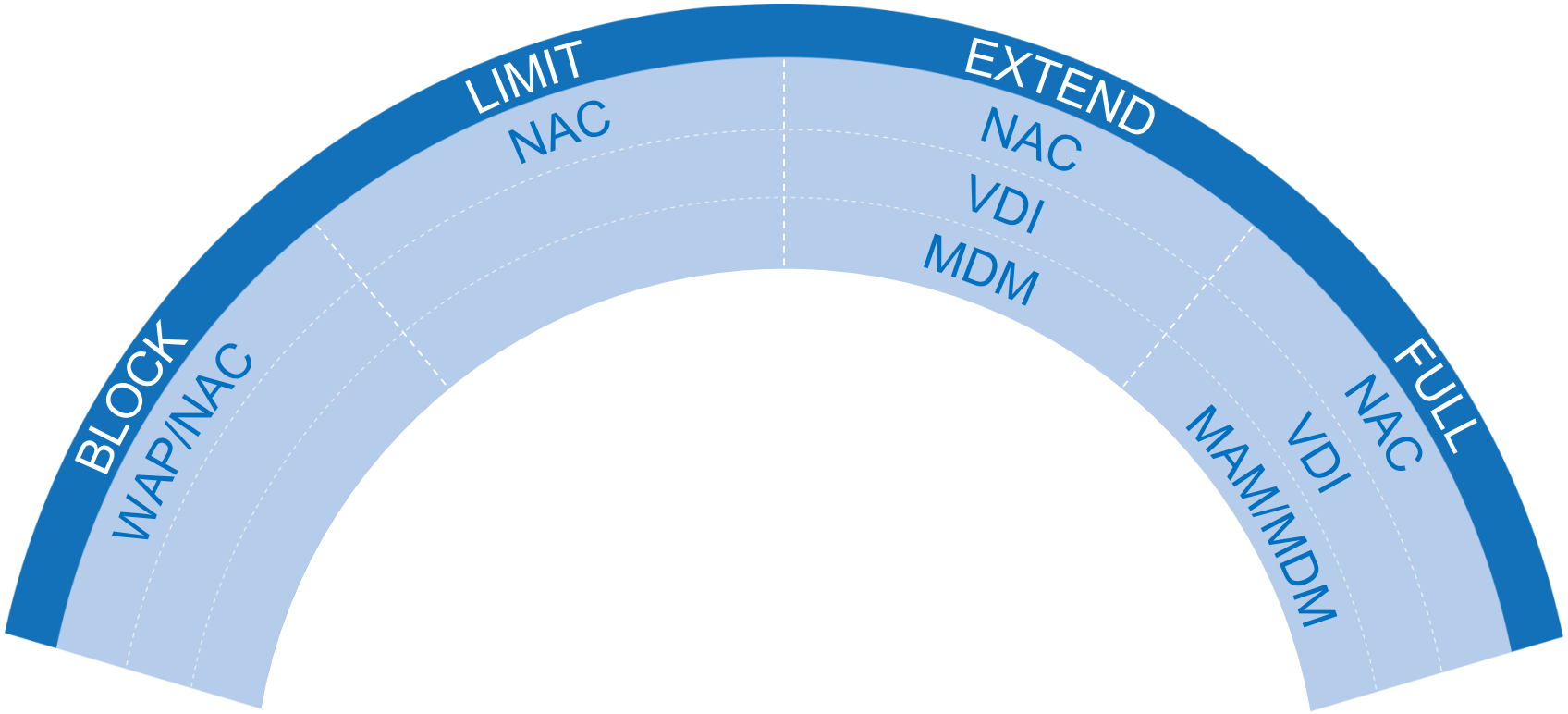
Multiple Security Choices



Multiple Security Choices



Multiple Security Choices



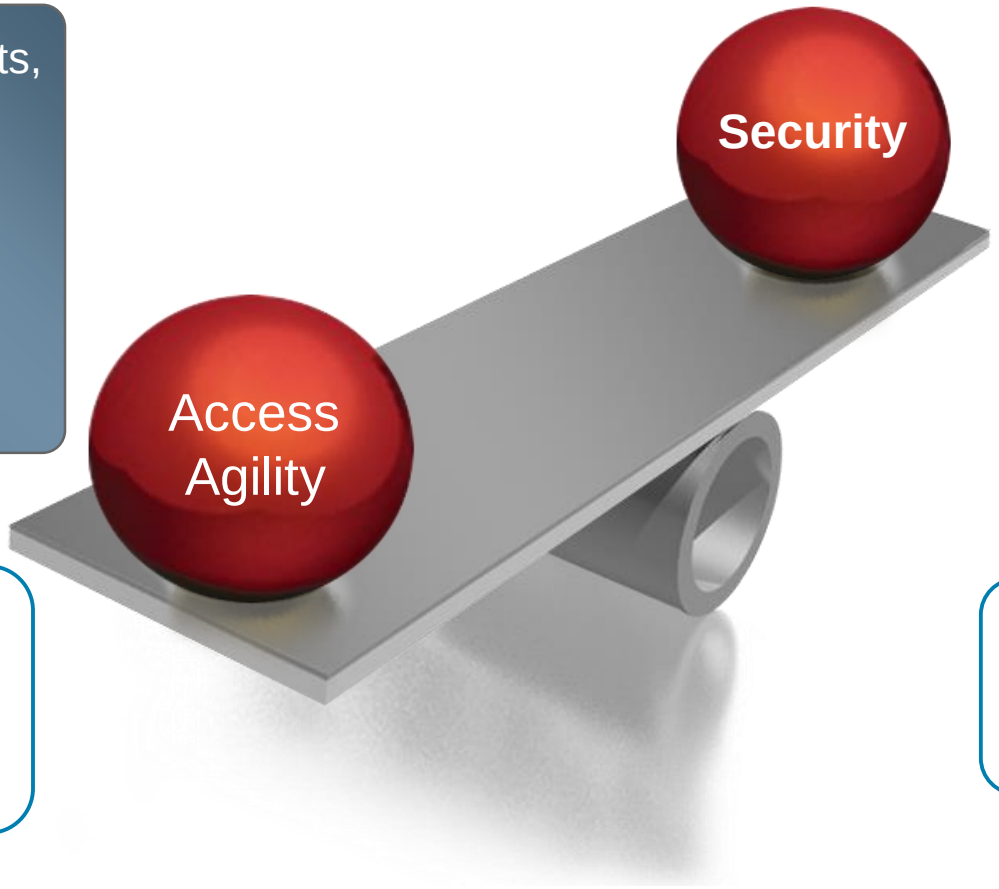
“Points of Integration”

- Universal visibility
- Universal access policy
- Universal reporting
- Automated enrollment
- On-access assessment
- Block malicious activity

The Enterprise Challenge: Balance Access Agility With Security

- Employees, Guests, Contractors
- Personal devices
- Wireless, wired, VPN, mobile

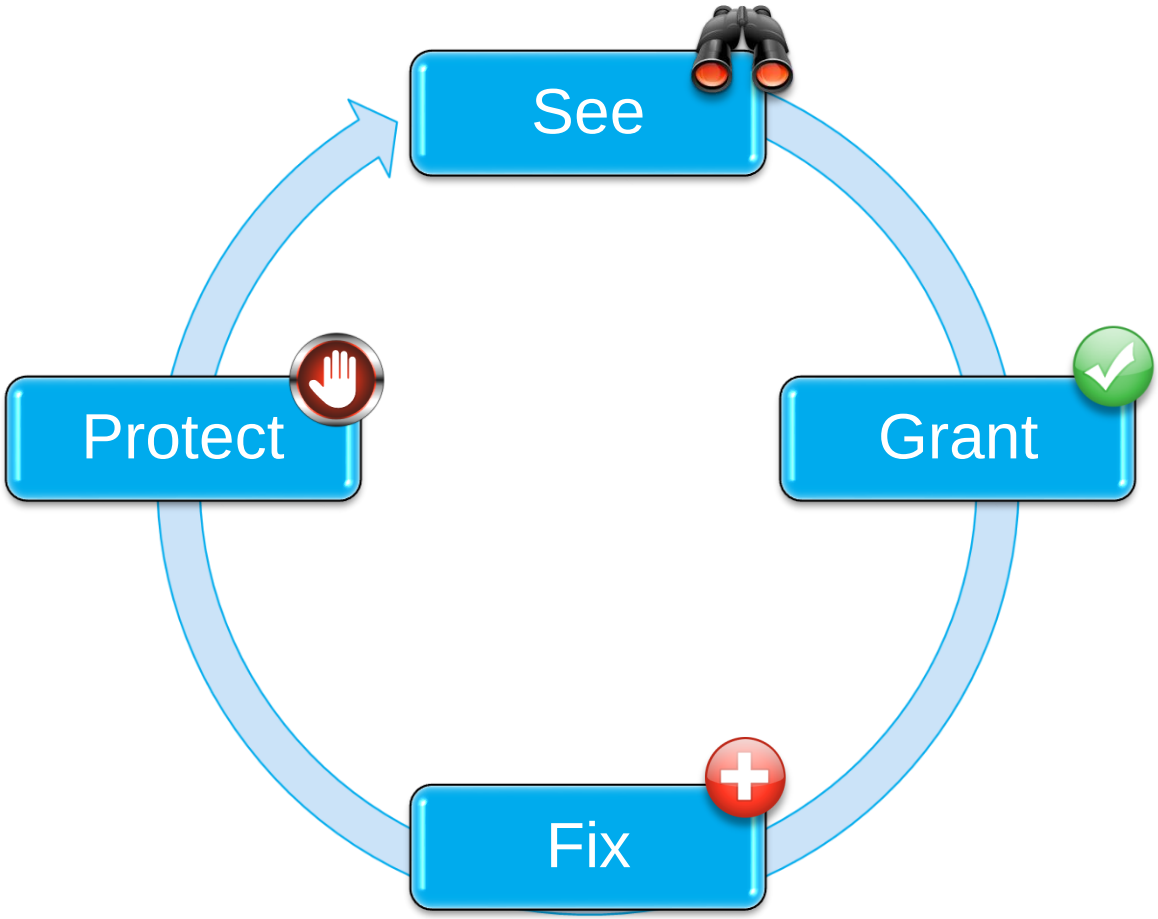
Requires real-time, comprehensive visibility



- Data loss
- Zero-day attacks and malware
- Endpoint integrity
- Regulations and compliance

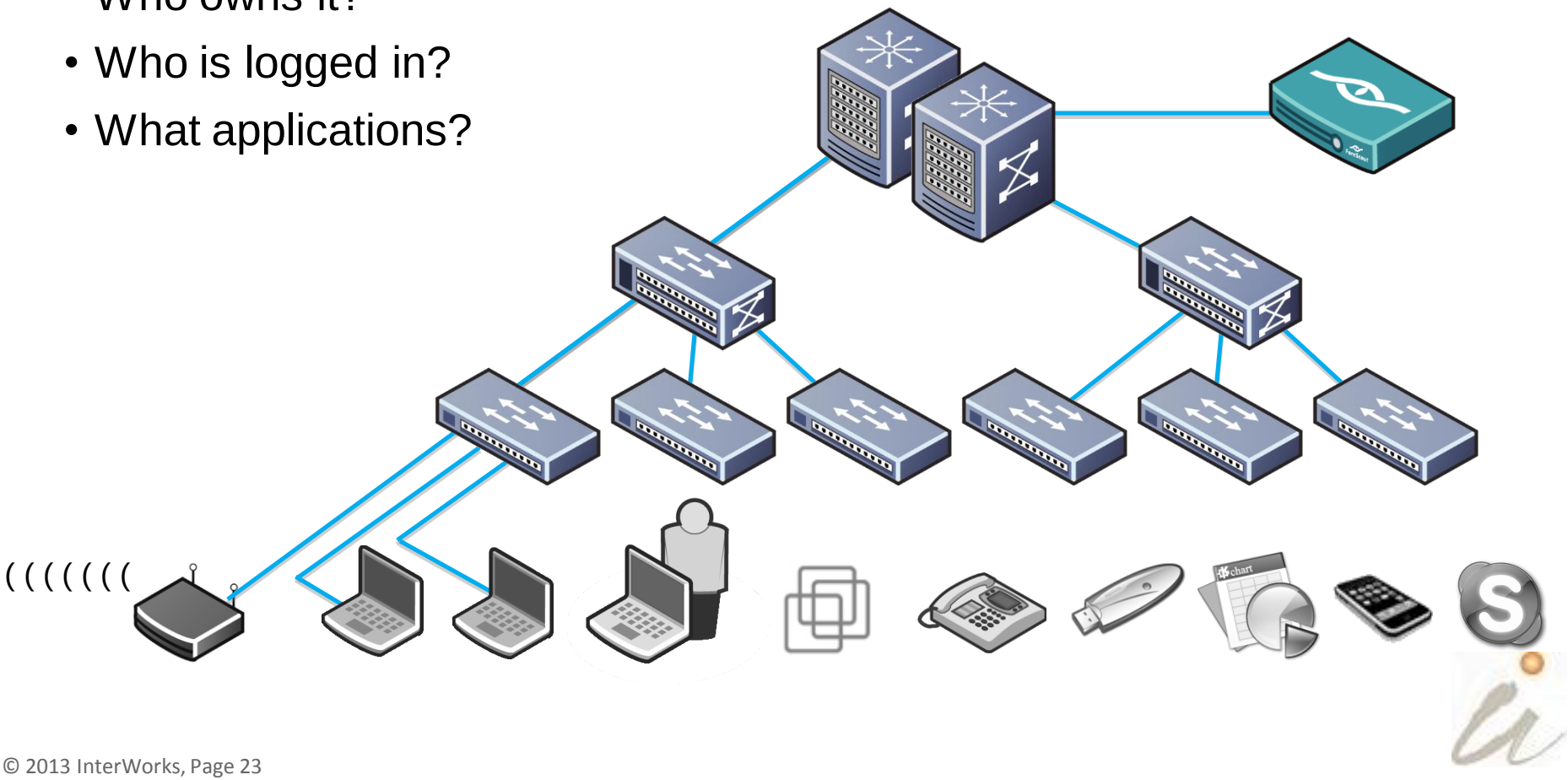
Requires real-time, automated controls

End-To-End Security Automation

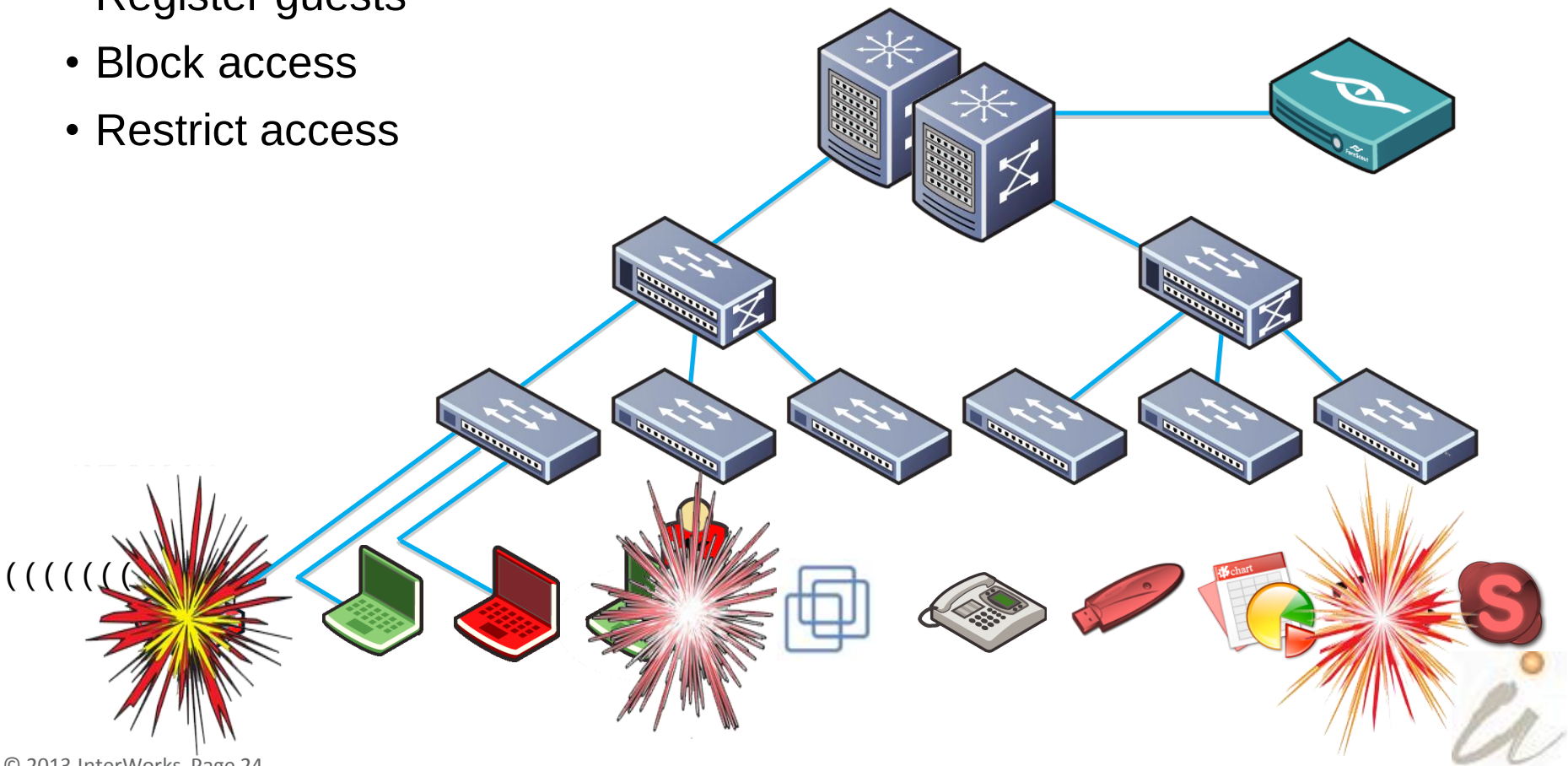


See Grant Fix Protect

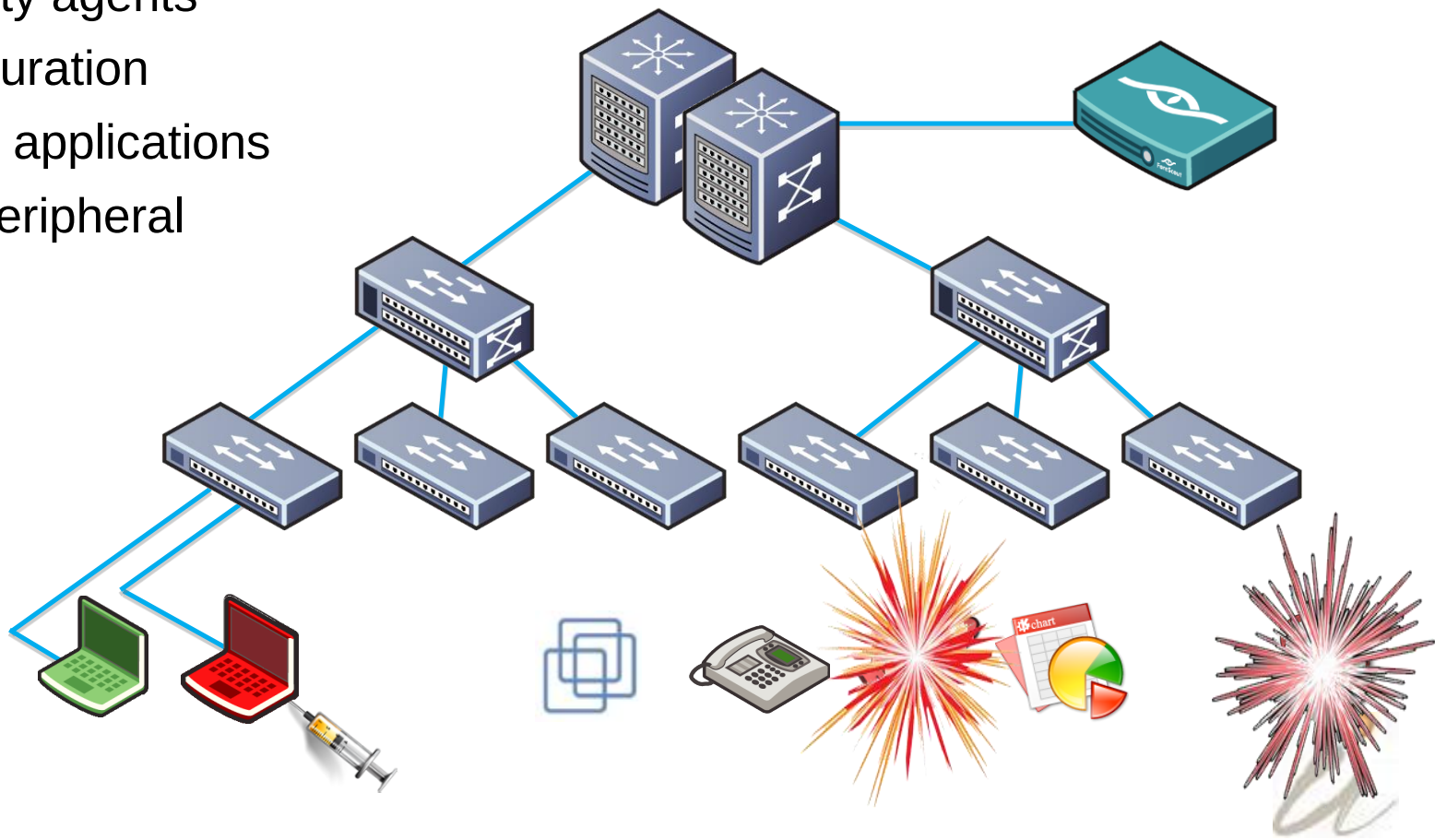
- What type of device?
- Who owns it?
- Who is logged in?
- What applications?



- Grant access
- Register guests
- Block access
- Restrict access

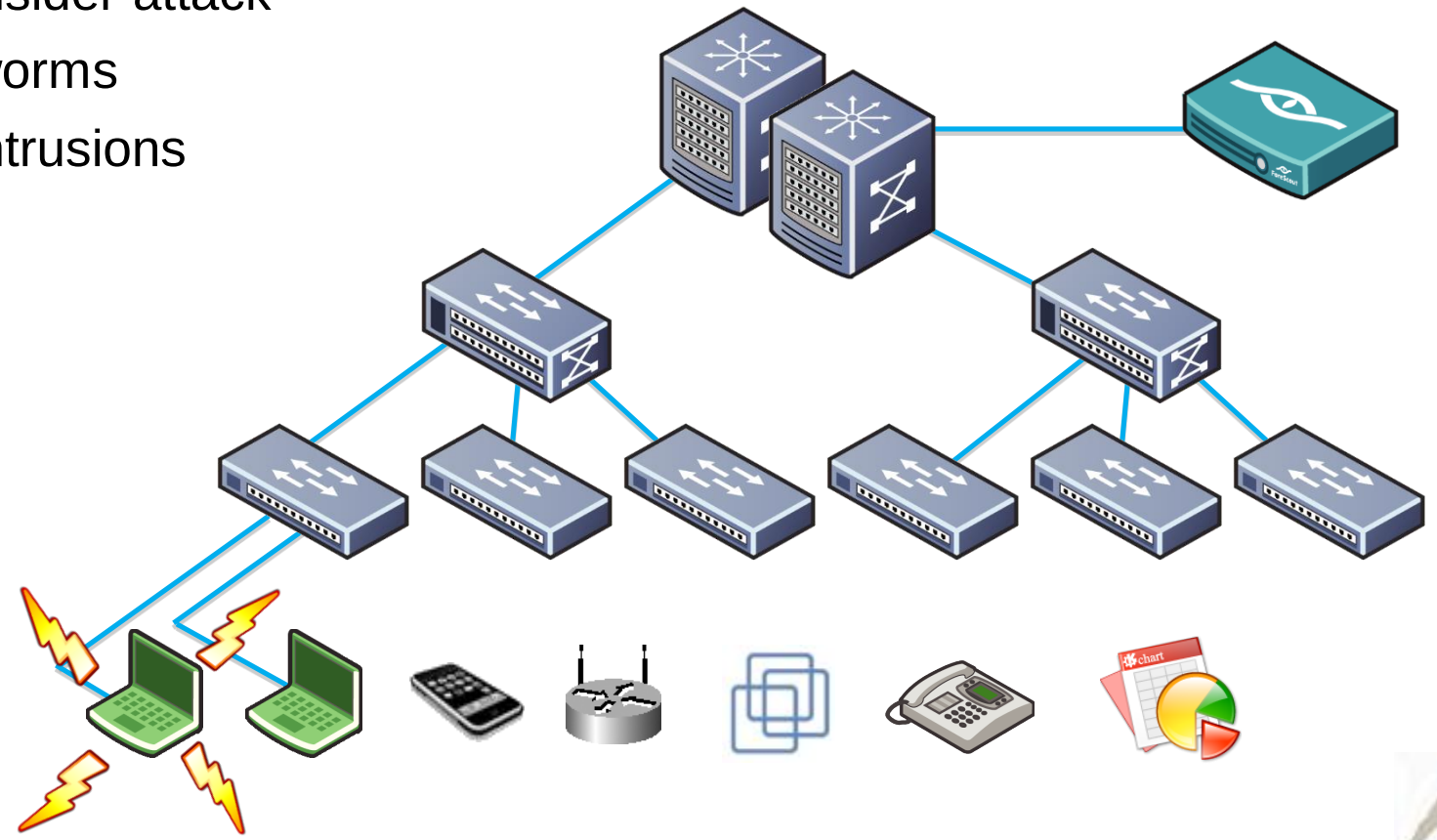


- Remediate OS
- Fix security agents
- Fix configuration
- Start/stop applications
- Disable peripheral



See Grant Fix **Protect**

- Detect unexpected behavior
- Block insider attack
- Block worms
- Block intrusions



See Grant Fix **Protect**

ALERT & REMEDIATE	RESTRICT ACCESS	MOVE & DISABLE
Open trouble ticket	Deploy a Virtual Firewall around an infected or non-compliant device	Reassign device from production VLAN to quarantine VLAN
Send email notification	Reassign the device into a VLAN with restricted access	Block access with 802.1X
SNMP Traps	Update access lists (ACLs) on switches, firewalls and routers to restrict access	Alter login credentials to block access
Syslog	Automatically move device to a pre-configured guest network	Block access with device authentication
HTTP browser hijack		Turn off switch port (802.1X or SNMP)
Auditable end-user acknowledgement		Terminate unauthorized applications
Self-remediation		Disable peripheral device
Integrate with SMS, WSUS, SCCM, Lumension, BigFix		

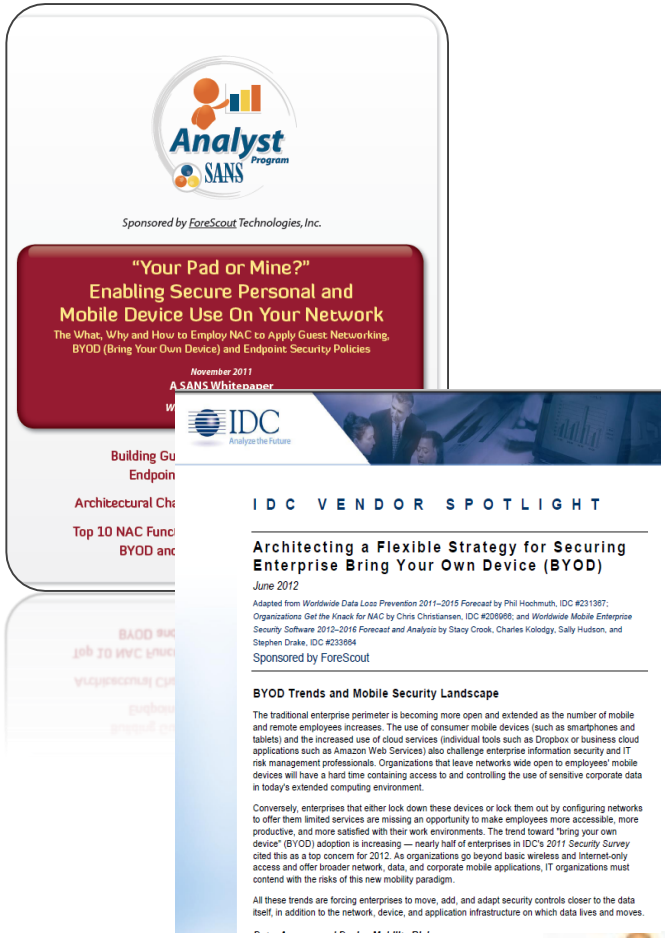
Mobile Security Remediation

- A variety of actions are available to manage, remediate and restrict mobile devices
- Multiple actions can be stacked together to provide even more control

Whitepapers

SANS Report: *"Your Pad or Mine: Enabling Secure Personal and Mobile Device Use on Your Network*"

IDC Report: "*Architecting a Flexible Strategy for Securing Enterprise Bring Your Own Device (BYOD)*"



10 Steps to BYOD Implementation

1. Form a committee
   - Multiple IT departments
   - Users across departments

10 Steps to BYOD Implementation

1. Form a committee
2. Gather data
   - Devices in use?
   - Ownership of devices?
   - Applications in use?
   - Entry paths?

10 Steps to BYOD Implementation

1. Form a committee
2. Gather data
3. Identify use cases
   - Which applications?
   - Which users? Role?
   - Offline use?
   - Sensitivity of data?

10 Steps to BYOD Implementation

1. Form a committee
2. Gather data
3. Identify use cases
4. Create an economic model
   - Device costs (capital)
   - Data connectivity costs (expense)
   - Employee stipends (expense)
   - Software license costs (capital)
   - Employee productivity gains
   - Infrastructure costs (security, bandwidth, data protection)

10 Steps to BYOD Implementation

1. Form a committee
2. Gather data
3. Identify use cases
4. Create an economic model
5. Formulate policies
   - Which devices will you support?
   - Which corporate applications?
   - Which users?
   - How will data be secured?
   - Acceptable use?
   - What if the device is lost or stolen?
   - How will the endpoint be updated?

10 Steps to BYOD Implementation

1. Form a committee
2. Gather data
3. Identify use cases
4. Create an economic model
5. Formulate policies
6. Decide how to protect your network
   - Manual or automated ?
   - Types of compliance checks?
   - Multiple wireless networks or one network?

10 Steps to BYOD Implementation

1. Form a committee
2. Gather data
3. Identify use cases
4. Create an economic model
5. Formulate policies
6. Decide how to protect your network
7. Decide how to protect data
   - Containerization on the mobile device?
   - Hosted Virtual Desktop?

10 Steps to BYOD Implementation

1. Form a committee
2. Gather data
3. Identify use cases
4. Create an economic model
5. Formulate policies
6. Decide how to protect your network
7. Decide how to protect data
8. Build a project plan
   - Remote device management?
   - Cloud storage?
   - Wipe devices when employees are terminated?

10 Steps to BYOD Implementation

1. Form a committee
2. Gather data
3. Identify use cases
4. Create an economic model
5. Formulate policies
6. Decide how to protect your network
7. Decide how to protect data
8. Build a project plan
9. Evaluate solutions
   - Ease of implementation?
   - Cost?
   - Security?
   - Usability?

10 Steps to BYOD Implementation

1. Form a committee
2. Gather data
3. Identify use cases
4. Create an economic model
5. Formulate policies
6. Decide how to protect your network
7. Decide how to protect data
8. Build a project plan
9. Evaluate solutions
10. Implement solutions
    - Phased approach
    - Monitor, then pilot, then full deployment

10 Steps to BYOD Implementation

1. Form a committee
2. Gather data
3. Identify use cases
4. Create an economic model
5. Formulate policies
6. Decide how to protect your network
7. Decide how to protect data
8. Build a project plan
9. Evaluate solutions
10. Implement solutions

10 Steps to BYOD Implementation

1. Form a committee
2. Gather data
3. Identify use cases
4. Create an economic model
5. Formulate policies
6. Decide how to protect your network
7. Decide how to protect data
8. Build a project plan
9. Evaluate solutions
10. Implement solutions