Cisco 思科演示云dCloud系列培训

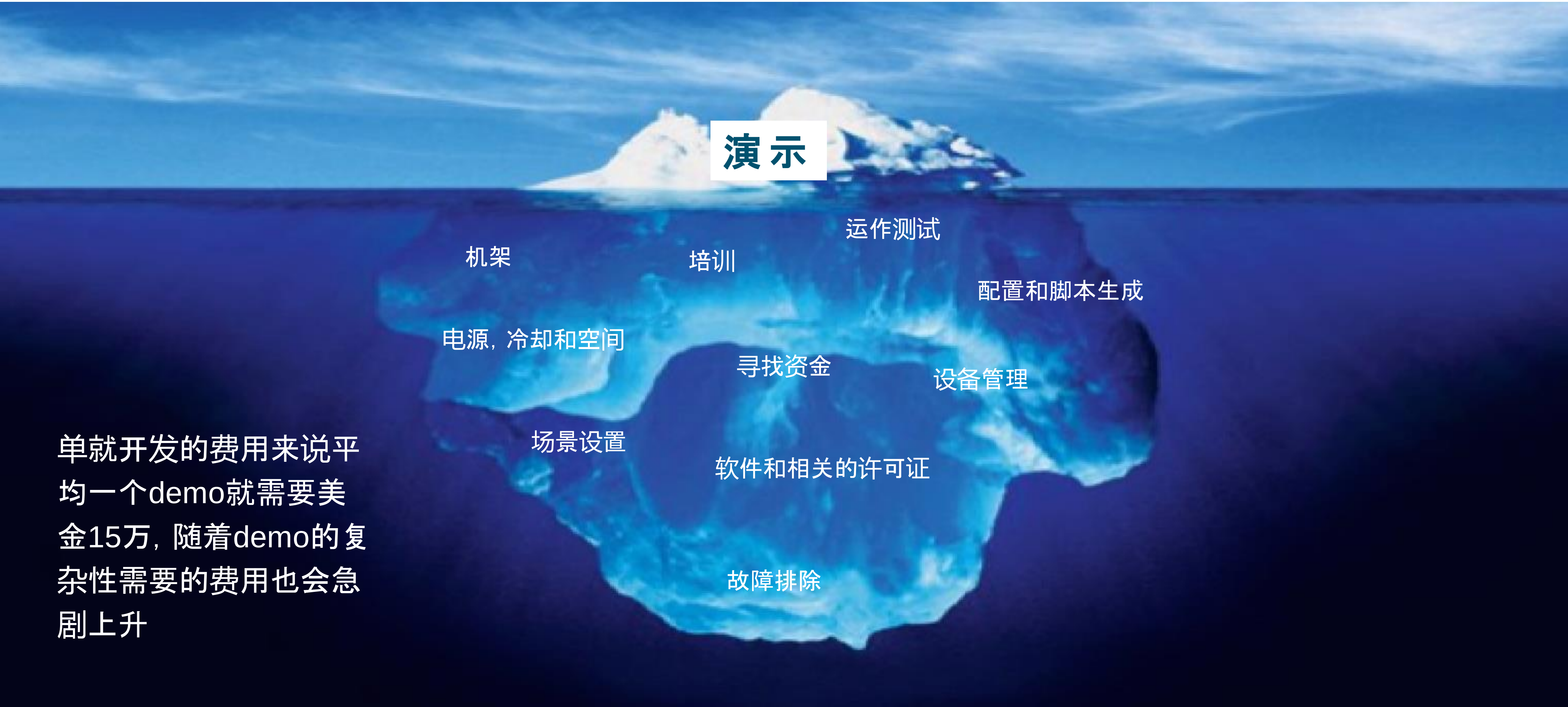
如何使用dCloud 来做Cisco Rapid Threat Containment v1的演示

- 您是否有这样的感触：在日常工作中，我们常常为搭建一套演示环境而奔走操劳；在客户拜访过程中，因缺少简单便捷的演 示方式，而无法将思科的语音、视频、BYOD等解决方案更好的展示在客户面前。今天，思科演示云dCloud可以祝您一臂之 力，帮您解决以上困扰!

dCloud – 思科的演示云

思科演示云将其产品解决方案架构的软件和硬件虚拟化，让思科与合作伙伴的销售团队在任何地方，任何时间都可以做产品演示.

创建一个演示背后所需要的资源



单就开发的费用来说平均一个demo就需要美金15万，随着demo的复杂性需要的费用也会急剧上升

Cisco 思科演示云dCloud

体验思科

使用方式

- 客户
- 合作伙伴
- 思科员工
- 通过全球的4个数据中心

立即可用

- 预先配置
- 已测试
- 完整的脚本和视频

按需所用

- 定制化+保存
- 共享
- 协作

可信赖

- 每个思科架构
- 每年使用量超过16万
- 24x5 技术支持

销售助力

- 自主学习
- 演示
- 体验

dCloud Platform

- 云
- 协作
- 数据中心
- 企业网
- 万物互联
- 安全
- 分析和自动化
- 服务提供商

dCloud 满足你的要求

http://dcloud.cisco.com

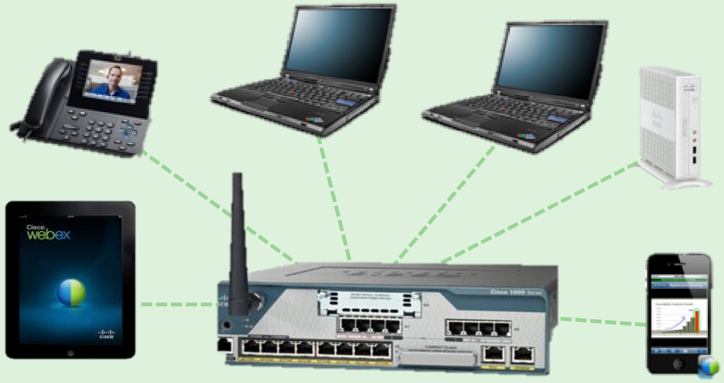
As Easy As…

- 思科员工和合作伙伴
- 完整脚本
- 定制化，本地化，共享
- 可选的终端 (BYOD)
- 可使用你自己的设备

dCloud
Data Centers

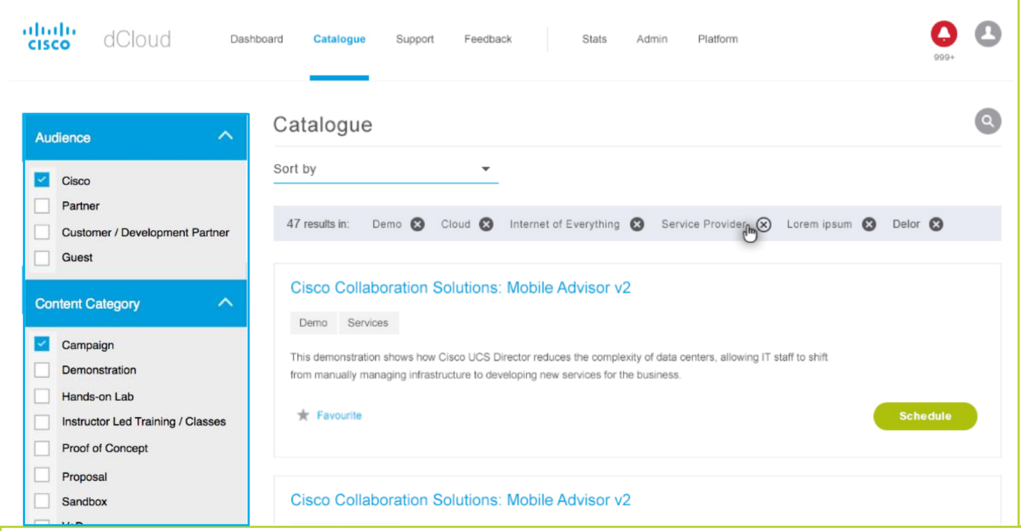
AMERICAS
EMEAR
APJ
GC

As Complete As…



- Virtual desktops
- Local clients on laptops
- Room based configuration
- 可添加你本地的服务器
- 多种使用案例

Cisco dCloud v2 UI – dCloud 有了一个全新的改变



Catalogue

☑ Cisco
□ Partner
□ Customer / Development Partner
□ Guest

☑ Campaign
□ Demonstration
□ Hands-on Lab
□ Instructor Led Training / Classes
□ Proof of Concept
□ Proposal
□ Sandbox

47 results in: Demo ☒ Cloud ☒ Internet of Everything ☒ Service Provider ☒ Lorem ipsum ☒ Delor ☒

Cisco Collaboration Solutions: Mobile Advisor v2

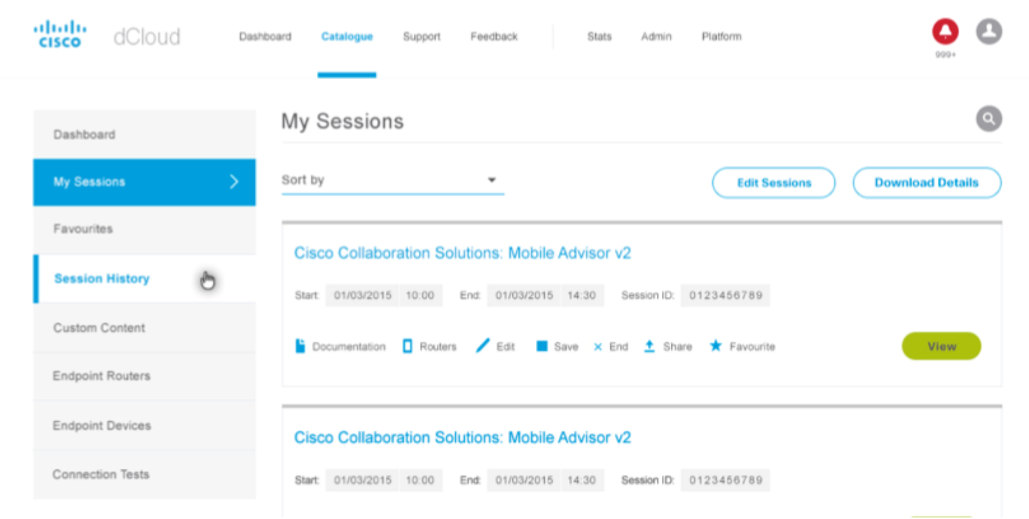
Demo Services

This demonstration shows how Cisco UCS Director reduces the complexity of data centers, allowing IT staff to shift from manually managing infrastructure to developing new services for the business.

Cisco Collaboration Solutions: Mobile Advisor v2

- 新的dCloud界面是为台式机，平板电脑和智能电话专门设计的
- **Cisco Atlantic** approved 设计
- 基于**API**，为今后的延展提供了可能性
- 使用现有的 **dCloud production 架构**

- Cisco.com **Single Sign On 单点登录**
- 动态的索引目录 – 删选**filter,** 排序**sort and** 搜索**search**
- 可收藏Favorites, 90-day 使用历史记录, 共享/移除共享
- **手机版dCloud 应用**正在开发中



My Sessions

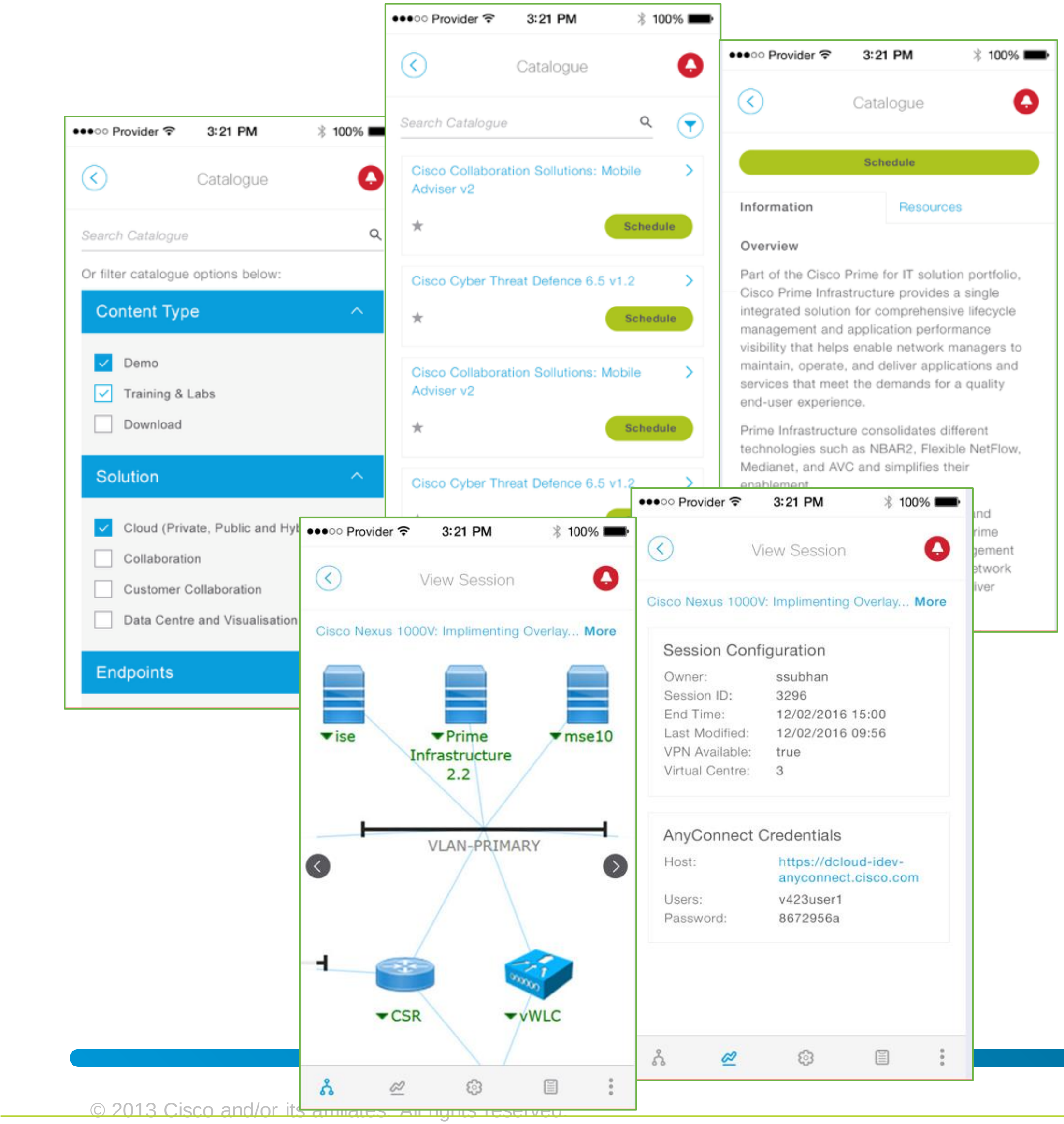
Cisco Collaboration Solutions: Mobile Advisor v2

Start: 01/03/2015 10:00 End: 01/03/2015 14:30 Session ID: 0123456789

Cisco Collaboration Solutions: Mobile Advisor v2

Start: 01/03/2015 10:00 End: 01/03/2015 14:30 Session ID: 0123456789

Cisco dCloud v2 – 手机版应用



●●●○○ Provider 3:21 PM 100%

Catalogue

Search Catalogue

Or filter catalogue options below:

Content Type

☑ Demo

☑ Training & Labs

□ Download

Solution

☑ Cloud (Private, Public and Hyb

□ Collaboration

□ Customer Collaboration

□ Data Centre and Visualisation

Endpoints

●●●○○ Provider 3:21 PM 100%

Catalogue

Search Catalogue

Cisco Collaboration Solutions: Mobile Adviser v2 — Schedule

Cisco Cyber Threat Defence 6.5 v1.2 — Schedule

Cisco Collaboration Solutions: Mobile Adviser v2 — Schedule

Cisco Cyber Threat Defence 6.5 v1.2

●●●○○ Provider 3:21 PM 100%

Catalogue

Schedule

Information | Resources

Overview

Part of the Cisco Prime for IT solution portfolio, Cisco Prime Infrastructure provides a single integrated solution for comprehensive lifecycle management and application performance visibility that helps enable network managers to maintain, operate, and deliver applications and services that meet the demands for a quality end-user experience.

Prime Infrastructure consolidates different technologies such as NBAR2, Flexible NetFlow, Medianet, and AVC and simplifies their enablement

●●●○○ Provider 3:21 PM 100%

View Session

Cisco Nexus 1000V: Implimenting Overlay... More

●●●○○ Provider 3:21 PM 100%

View Session

Cisco Nexus 1000V: Implimenting Overlay... More

Session Configuration

Owner:	ssubhan
Session ID:	3296
End Time:	12/02/2016 15:00
Last Modified:	12/02/2016 09:56
VPN Available:	true
Virtual Centre:	3

AnyConnect Credentials

Host:	https://dcloud-idev-anyconnect.cisco.com
Users:	v423user1
Password:	8672956a

- 在手机上可使用dCloud的所有功能
- 专为智能电话和平板电脑设计
- Cisco Atlantic approved 设计
- IOS and Android安卓应用
- Desktop app also designed for browsing on any mobile device

Cisco Rapid Threat Containment v1的演示

- **现在就让我们和思科安全架构的专家Yiwei一起开始吧：**
  - 转去dcloud.cisco.com
  - 使用CCO帐户SSO登陆
  - 选择大中华区GC数据中心
  - 马上就跟随Yiwei开始Rapid Threat Containment演示的学习吧，你可以随时提问题

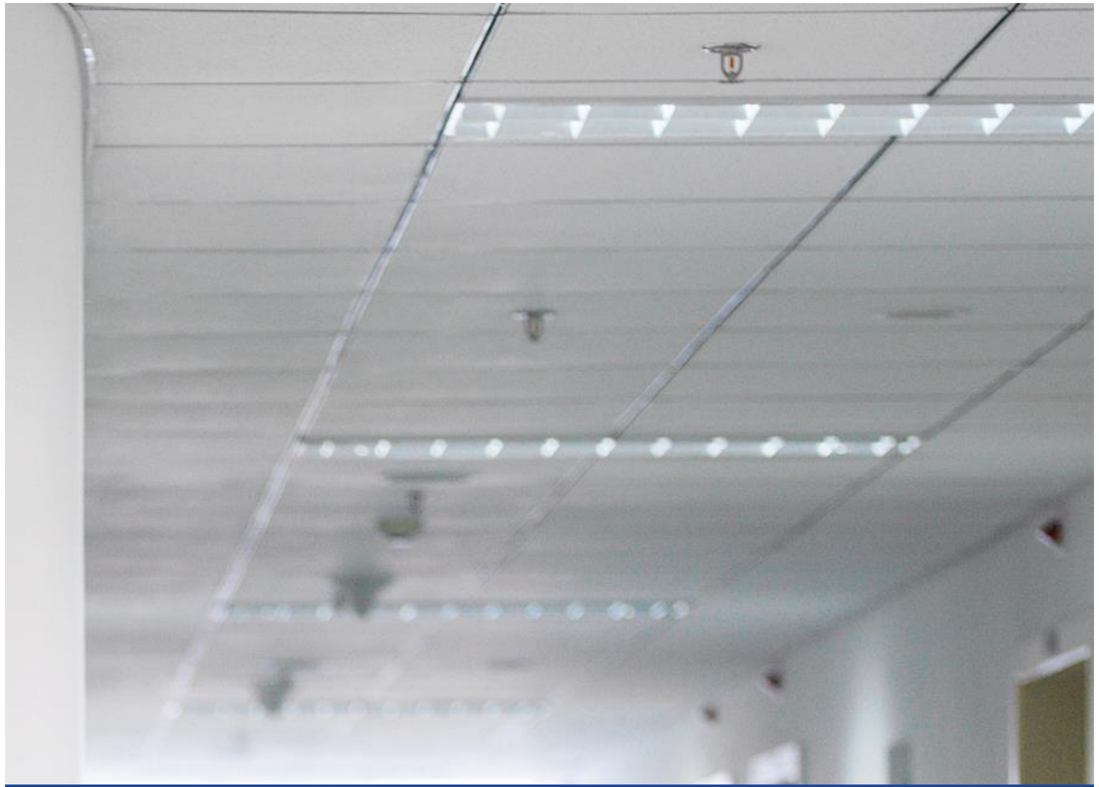
Cisco Rapid Threat Containment

Get Answers Faster, Stop Threats Faster, Protect Data Faster

Yiwei Zhou
Global Virtual Engineer

2017.3

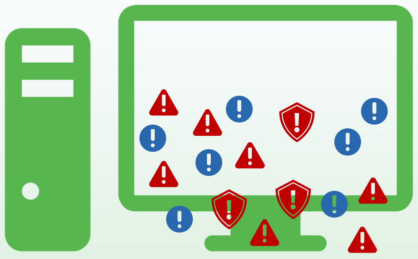
Fire Is a Threat

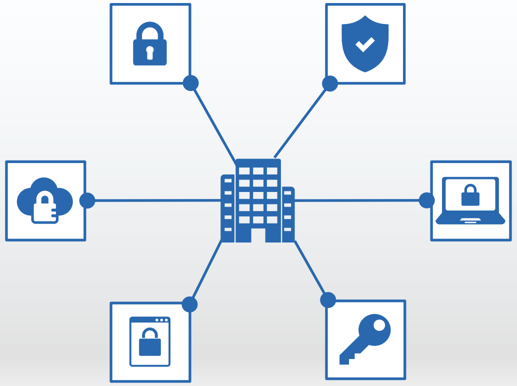


Sprinklers Sense and Enforce

Malware and Ransomware Are Threats

Average cost per data breach: $3.8 million





Speed

17,000 alerts received on average per week

Stealth

Current industry average detection time: 200 days

Sophistication

Security teams investigate just 4 percent of warnings

Companies Have Best-in-Class Defenses

Security Threat Defenses

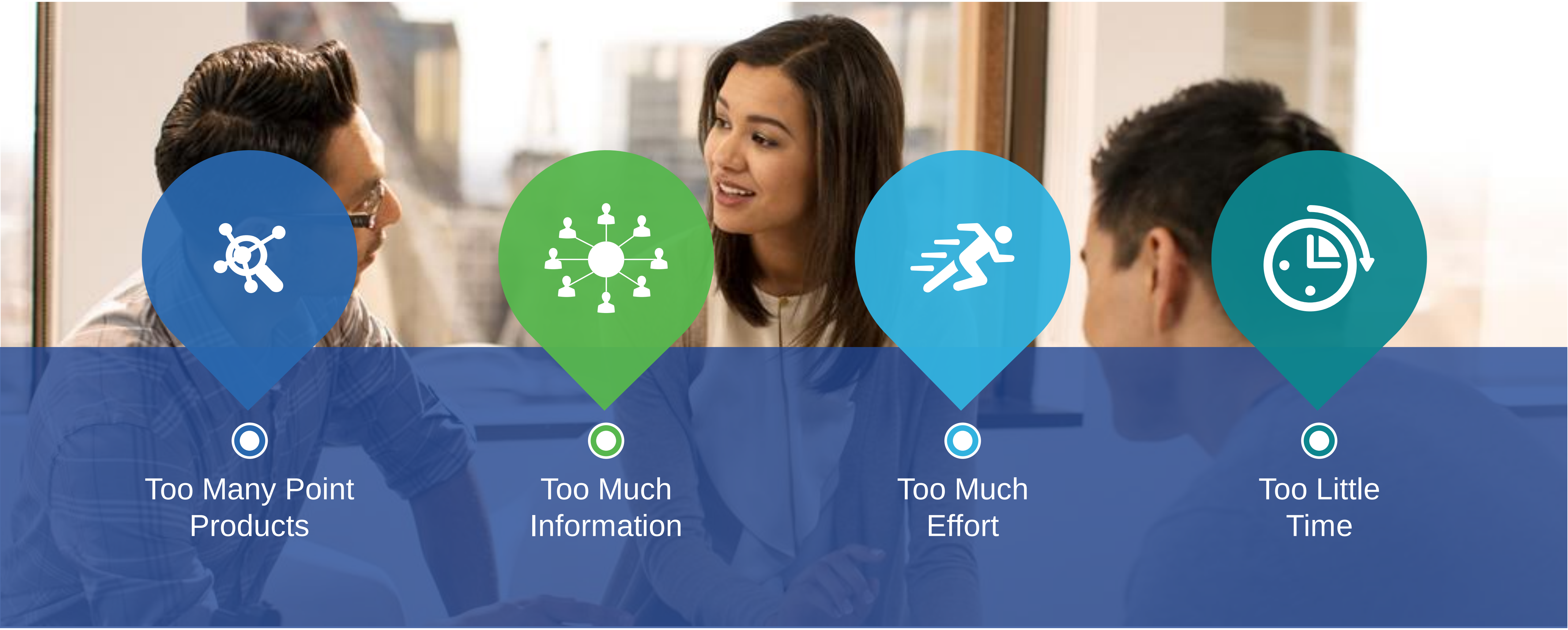
- Firewall
- Data loss prevention
- Authentication
- Encryption/privacy/data protection
- Email/messaging security
- Web security
- Endpoint protection/anti-malware
- Access control/authorization
- Identity administration/user provisioning
- Intrusion prevention/detection
- Mobility security
- Secured wireless
- Vulnerability scanning
- VPN
- Security information and event management
- Distributed-denial-of-service (DDOS) protection
- Penetration testing
- Patching and configuration
- Network forensics
- Endpoint forensics

Processes to Analyze Compromised Systems

- Firewall log
- System log analysis
- Network flow analysis
- Malware of file regression analysis
- Registry analysis
- Full packet capture analysis
- Correlate event/log analysis
- Disk forensics
- Indications of compromise (IOC) detection
- Memory forensics
- External incident response analysis

Having 40 to 60+ unrelated security solutions is common

But They Don't Work Together



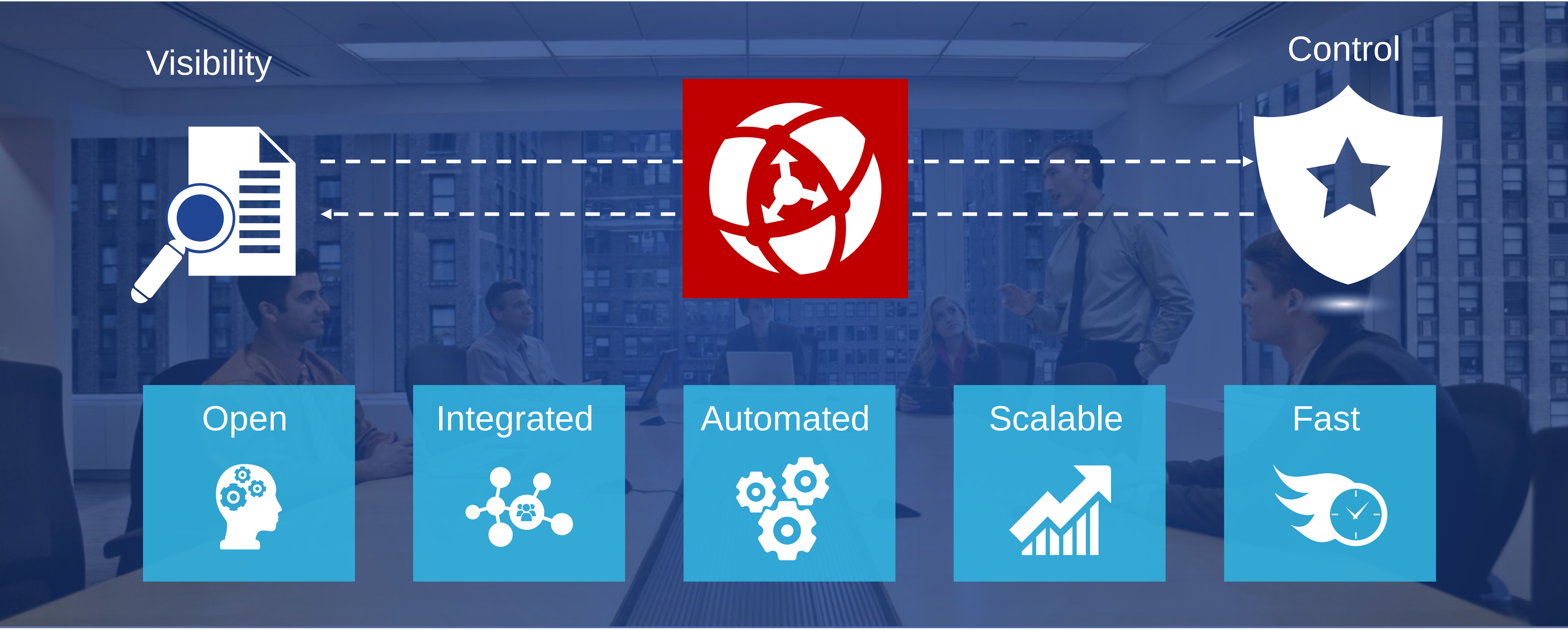
- Too Many Point Products
- Too Much Information
- Too Much Effort
- Too Little Time

This Impedes Getting Answers and Taking Action

Visibility

Control

Rapid Threat Containment
Get Answers Faster and Stop Attacks Faster



Visibility

Control

Open

Integrated

Automated

Scalable

Fast

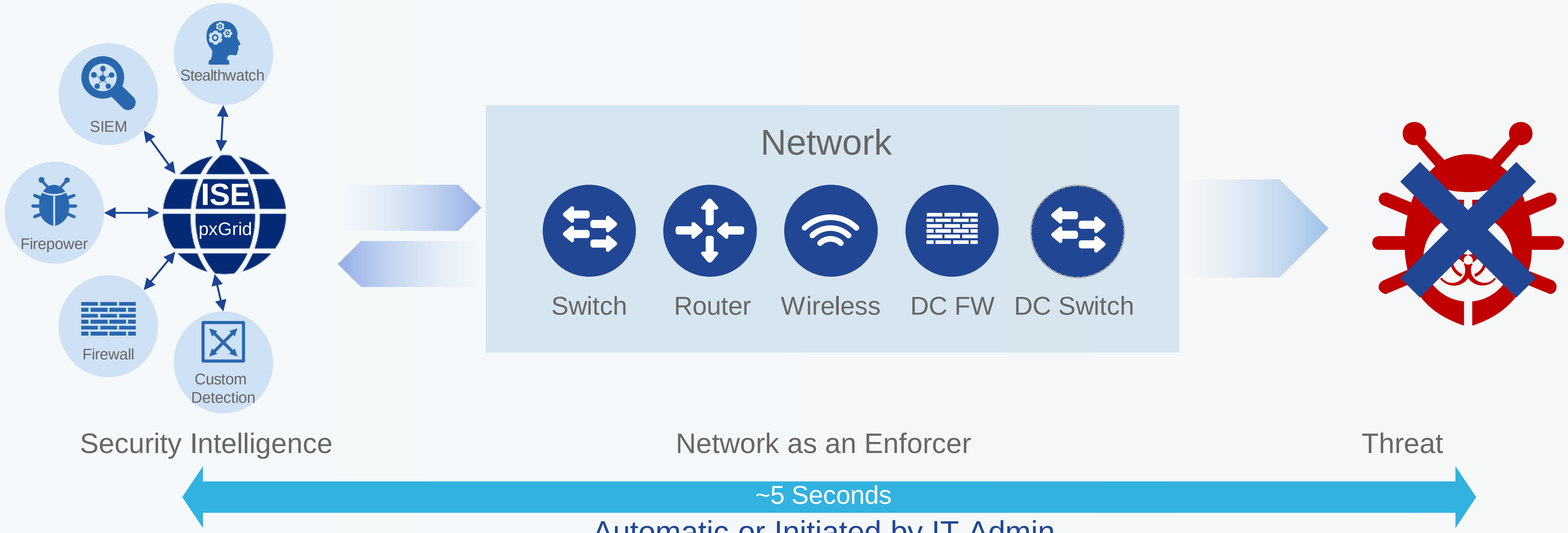
Operation

Rapid Threat Containment in Action

Get Answers Faster
Use Cisco® Platform Exchange Grid (pxGrid) partner technologies to find threats faster

Stop Attacks Faster
Use the network to contain attacks manually or automatically

Protect Critical Data Faster
Dynamically restrict access permissions or remove a device as its threat score worsens



Security Intelligence

Network as an Enforcer

Threat

~5 Seconds

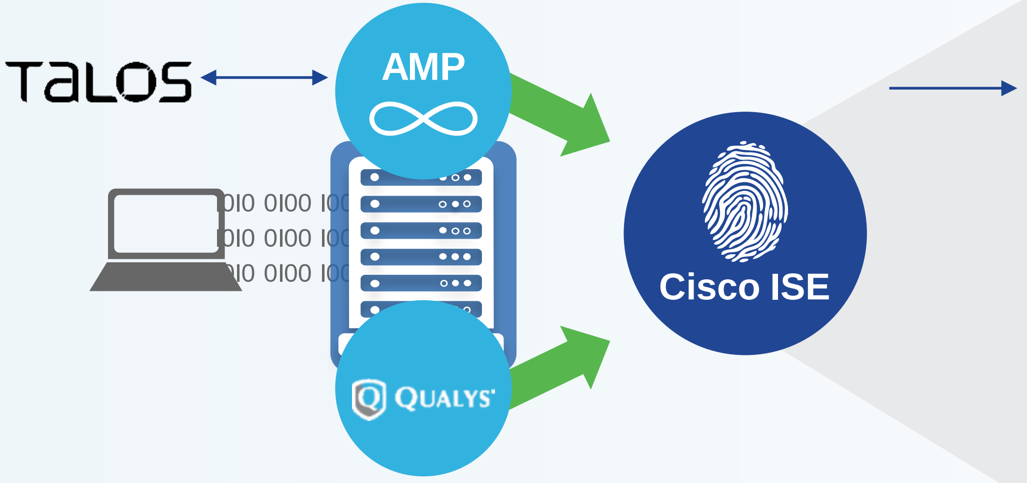
Automatic or Initiated by IT Admin

Rapid Threat Containment Now Offering Threat-Centric NAC

- Protect critical data faster
- Access privileges dynamically change with **threat** or **vulnerability** score
- Ratings based on open, structured expressions

STIX: Structured **Threat** Information Expression

Insignificant



CVSS: Common **Vulnerability** Scoring System

Access Policy

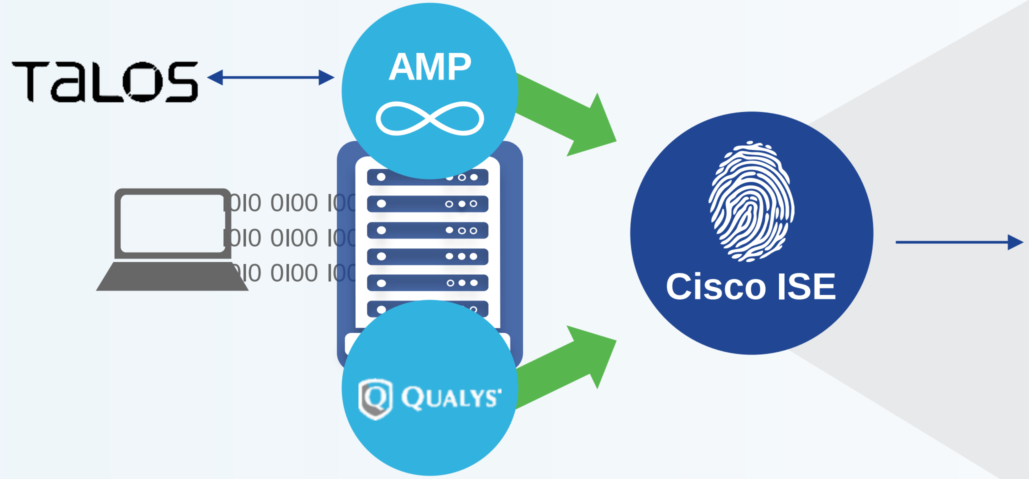
Source \ Destination	Worker	Guest	Finance	E-mail	Internet	Remediation
Worker	✓	−	✓	✓	✓	−
Guest	−	−	−	−	✓	−
Risk L1	✓	−	−	✓	✓	−
Risk L2	✓	−	−	−	✓	−
Risk L3	−	−	−	−	✓	−
Risk L4	−	−	−	−	−	✓

Rapid Threat Containment Now Offering Threat-Centric NAC

- Protect critical data faster
- Access privileges dynamically change with **threat** or **vulnerability** score
- Ratings based on open, structured expressions

STIX: Structured **Threat** Information Expression

Distracting



CVSS: Common **Vulnerability** Scoring System

Access Policy

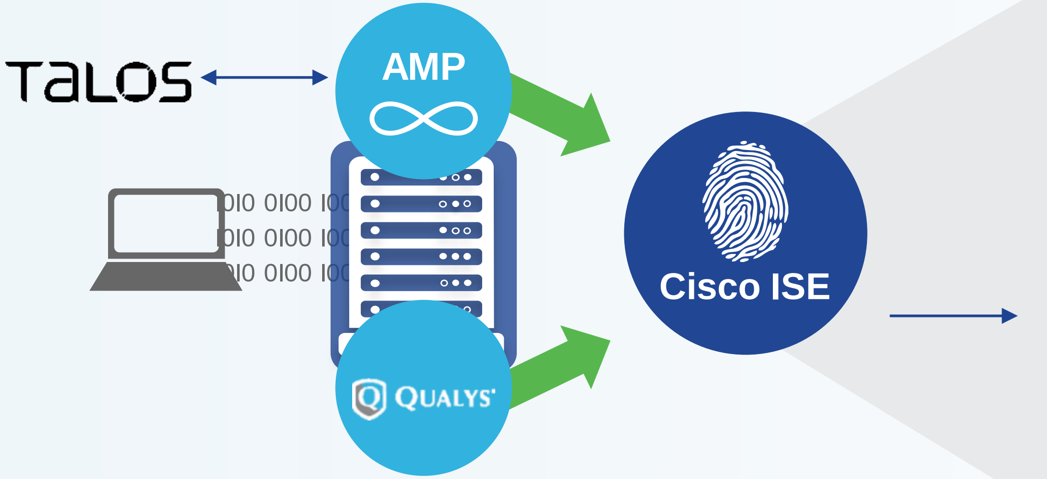
Source \ Destination	Worker	Guest	Finance	E-mail	Internet	Remediation
Worker	✓	−	✓	✓	✓	−
Guest	−	−	−	−	✓	−
Risk L1	✓	−	−	✓	✓	−
Risk L2	✓	−	−	−	✓	−
Risk L3	−	−	−	−	✓	−
Risk L4	−	−	−	−	−	✓

Rapid Threat Containment Now Offering Threat-Centric NAC

- Protect critical data faster
- Access privileges dynamically change with **threat** or **vulnerability** score
- Ratings based on open, structured expressions

Painful

STIX: Structured **Threat** Information Expression



CVSS: Common **Vulnerability** Scoring System

Access Policy

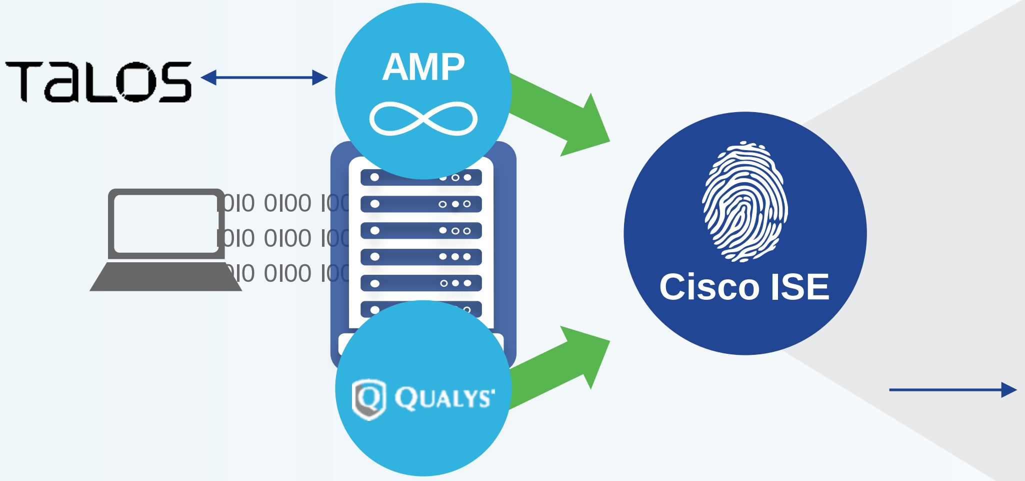
Destination	Worker	Guest	Finance	E-mail	Internet	Remediation
Source						
Worker	✓	–	✓	✓	✓	–
Guest	–	–	–	–	✓	–
Risk L1	✓	–	–	✓	✓	–
Risk L2	✓	–	–	–	✓	–
Risk L3	–	–	–	–	✓	–
Risk L4	–	–	–	–	–	✓

Rapid Threat Containment Now Offering Threat-Centric NAC

- Protect critical data faster
- Access privileges dynamically change with **threat** or **vulnerability** score
- Ratings based on open, structured expressions

STIX: Structured **Threat** Information Expression

Damaging



CVSS: Common **Vulnerability** Scoring System

Access Policy

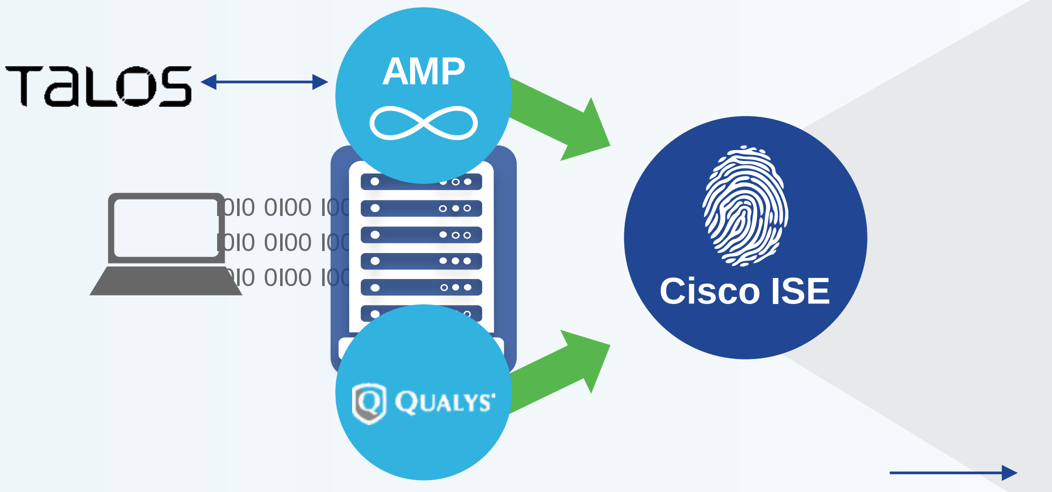
Source \ Destination	Worker	Guest	Finance	E-mail	Internet	Remediation
Worker	✓	−	✓	✓	✓	−
Guest	−	−	−	−	✓	−
Risk L1	✓	−	−	✓	✓	−
Risk L2	✓	−	−	−	✓	−
Risk L3	−	−	−	−	✓	−
Risk L4	−	−	−	−	−	✓

Rapid Threat Containment Now Offering Threat-Centric NAC

- Protect critical data faster
- Access privileges dynamically change with **threat** or **vulnerability** score
- Ratings based on open, structured expressions

STIX: Structured **Threat** Information Expression

Convicted



CVSS: Common **Vulnerability** Scoring System

Access Policy

	Destination					
Source	Worker	Guest	Finance	E-mail	Internet	Remediation
Worker	✓	−	✓	✓	✓	−
Guest	−	−	−	−	✓	−
Risk L1	✓	−	−	✓	✓	−
Risk L2	✓	−	−	−	✓	−
Risk L3	−	−	−	−	✓	−
Risk L4	−	−	−	−	−	✓

Parts

Cisco Identity Services Engine (ISE) pxGrid

Open* **Sharing** to Get Answers Faster; **Control** to Stop Threats

Any-any sharing

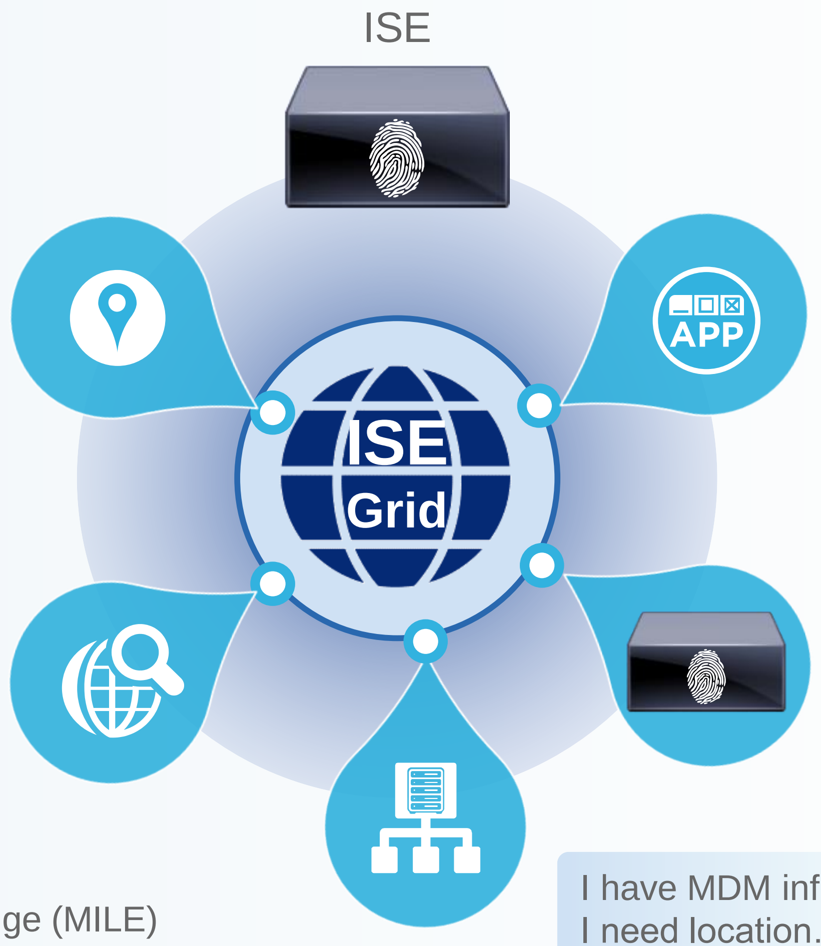
- Publish
- Subscribe

ISE sharing

- Identity context

ISE network control

- Adaptive network control



I have location!
I need app
and identity…

I have application info!
I need location and
device type

I have sec events!
I need identity
and device…

I have identity and
device!
I need geo-location
and MDM…

I have MDM info!
I need location…

* IETF Standards Track: Managed Incident Lightweight Exchange (MILE)

Intelligence Sharing between Cisco and Technology Partners

New Partners for ISE 2.1 Release (June 14, 2016)

Cisco use cases

Management

Cisco Firepower™ Management Center

Analysis

Cisco® Stealthwatch

Behavior

Cisco Advanced Malware Protection (AMP)

Partner use cases

Threat-Centric NAC

QUALYS®

Cloud Access Security Broker

netskope

User Entity Behavior Analytics

niara™

Rapid Threat Containment and Threat Defense

REDSHIFT NETWORKS

Attivo

inteliment®

FORTSCALE

TRAPX

ThreatTrack™ Security

LemonFish TECHNOLOGIES

Identity Access Management

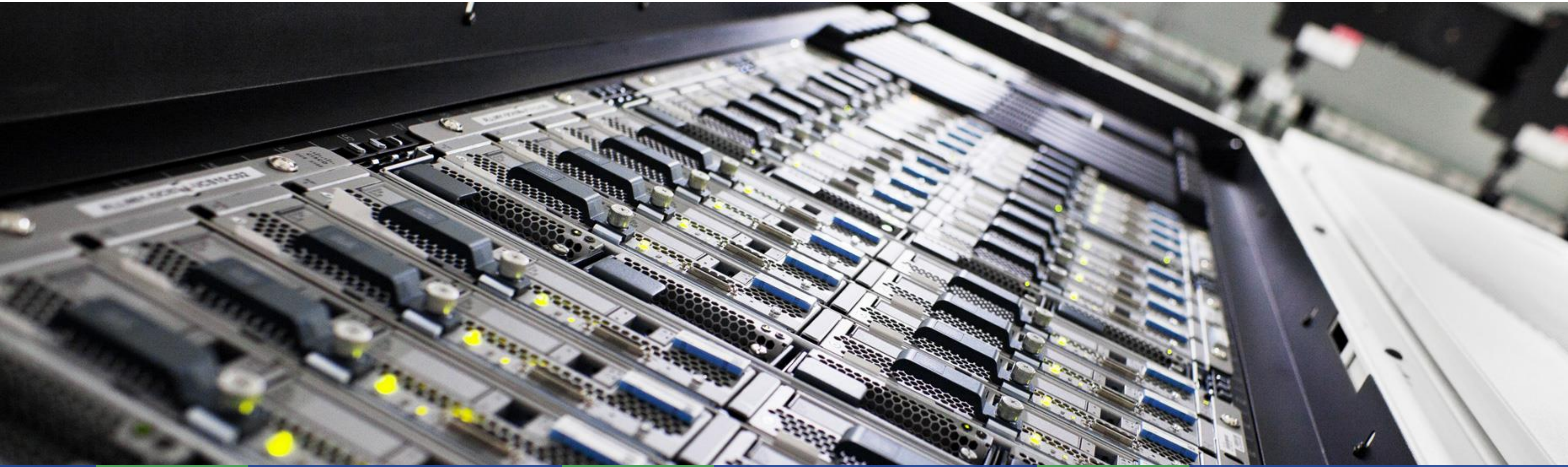
Situational

Network Visibility

Lumeta®

CISCO

Cisco Identity Services Engine



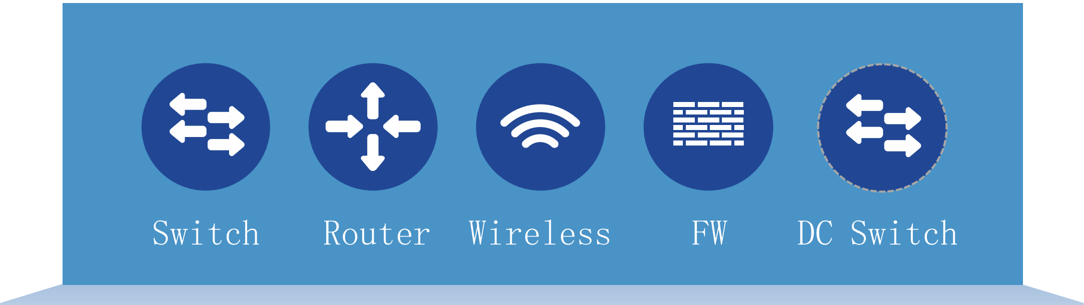
Control all access throughout the network from one place

See and share rich user and device details

Stop and contain threats

Control

Using the Network as an Enforcer



Enforcement Options

- Expulsion
- Observation
- Restriction
- Quarantine
- Remediation

Network Devices

- Cisco® traditional
- Cisco TrustSec®
- Multivendor
- Hybrid

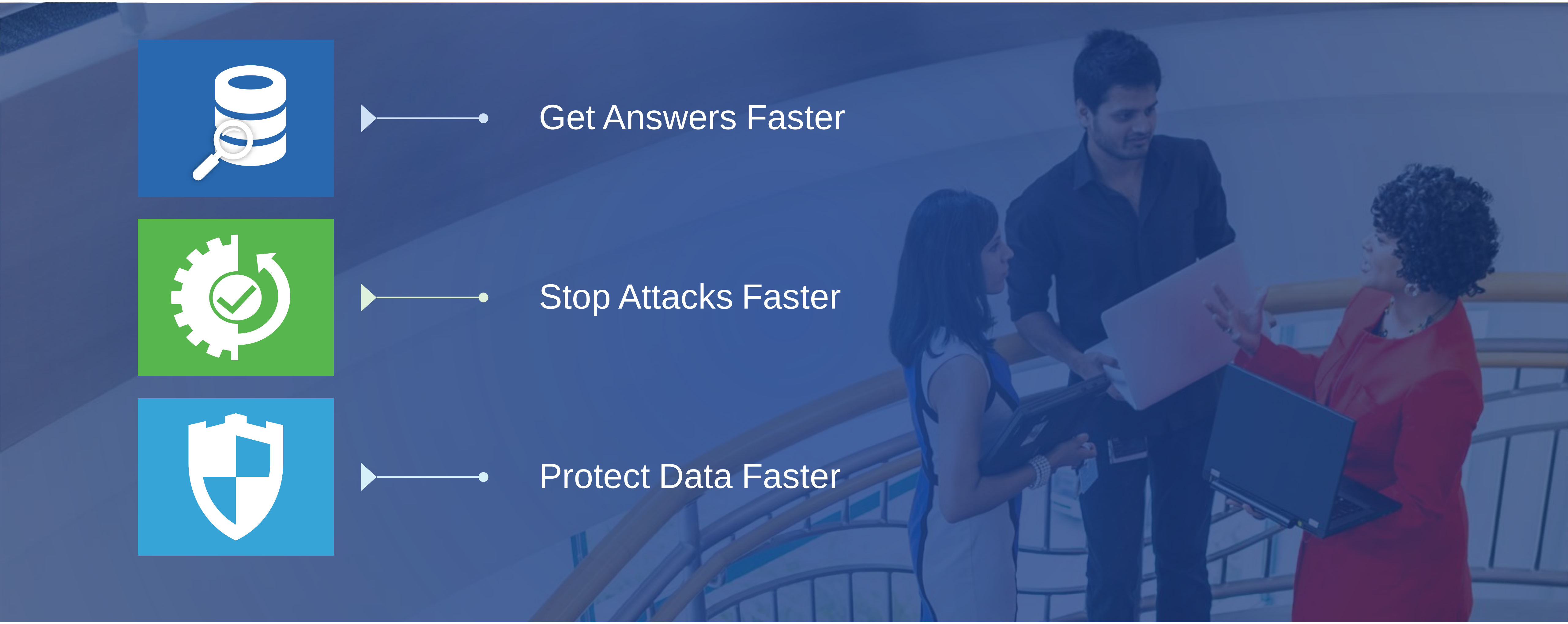
BROCADE

Alcatel·Lucent

aruba NETWORKS an HP company

Ruckus Simply Better Wireless.

Rapid Threat Containment



Get Answers Faster

Stop Attacks Faster

Protect Data Faster

Call to Action

- Go to: dcloud.cisco.com
- dCloud for demo, lab, PoC, etc.
- Live support 24x5… chat, email, Phone