IT Foundation Management

A new approach to security

Thomas Siebold

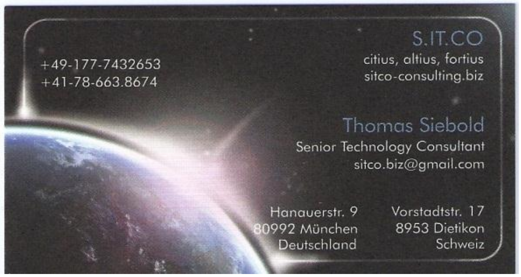
OpenVMS TUD

Bad Homburg, 27. October 2011

Thomas Siebold

- 33 years of experience in IT
- with
  - Digital Equipment GmbH & Corporation
  - Compaq Computers EMEA
  - Hewlett Packard EMEA & GmbH

- Representative for Stromasys (D,A,CH)
- Reseller and service provider for TDi (D,A,CH)
- sitco.biz@gmail.com
- www.sitco-consulting.biz, www.sitco-consulting.de



+49-177-7432653
+41-78-663.8674

S.IT.CO
citius, altius, fortius
sitco-consulting.biz

Thomas Siebold
Senior Technology Consultant
sitco.biz@gmail.com

Hanauerstr. 9
80992 München
Deutschland

Vorstadtstr. 17
8953 Dietikon
Schweiz

Tdi Technologies

- Founded by Bill Johnson
- Headquarter in Dallas, TX Metroplex
- In business >20 years
- ~300 Customers, 3200 Installations
- Privately Held
- Profitable and Growing
- Numerous awards as a high-growth technology company
- Products: ConsoleWorks, ITFM Suite
- www.tditechnologies.com
- http://www.youtube.com/watch?v=VZqpk-ZkNpA

Stromasys

- Founded by Robert Boers
- Headquarter in Geneva, Switzerland
- Main focus of business:
  - Virtualization of **PDP-11**, **VAX** and **Alpha** systems. With this virtualized hardware, all software on those platforms can run unmodified on Windows without requiring source code, conversion or code modification.
  - Migration of applications from older platforms to new and modern platforms and operating systems
- CHARON-VAX, -AXP, -PDP11

IT Foundation Management

The Global Leader in

IT Foundation Management

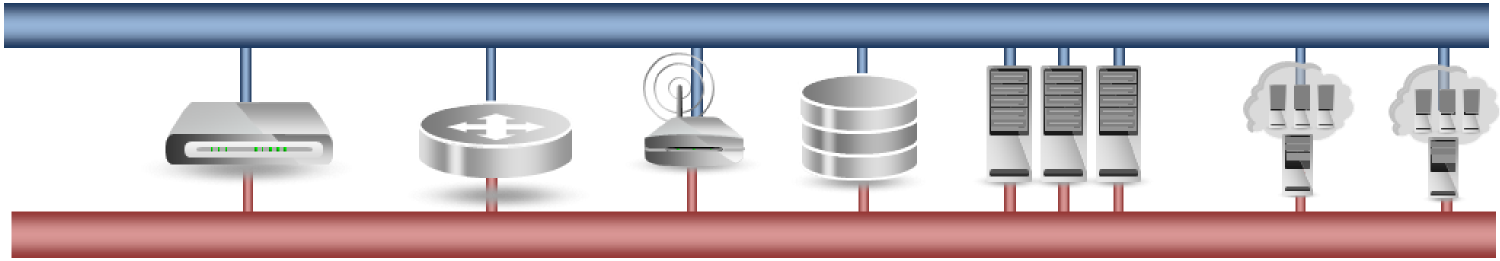
What is the IT Foundation?

The IT Foundation includes all of your:

Servers… Blades… Network Gear… SANs… Operating Systems…

Virtual Machines… Databases… Appliances… Networks… Environment…

Applications…



And is supported by:

I'm Joe…
Solaris Systems
Administrator

Cheryl,
Oracle DBA…

Steve,
I'm a SANs
Administrator

Hi. Raphael.
Network
Administration

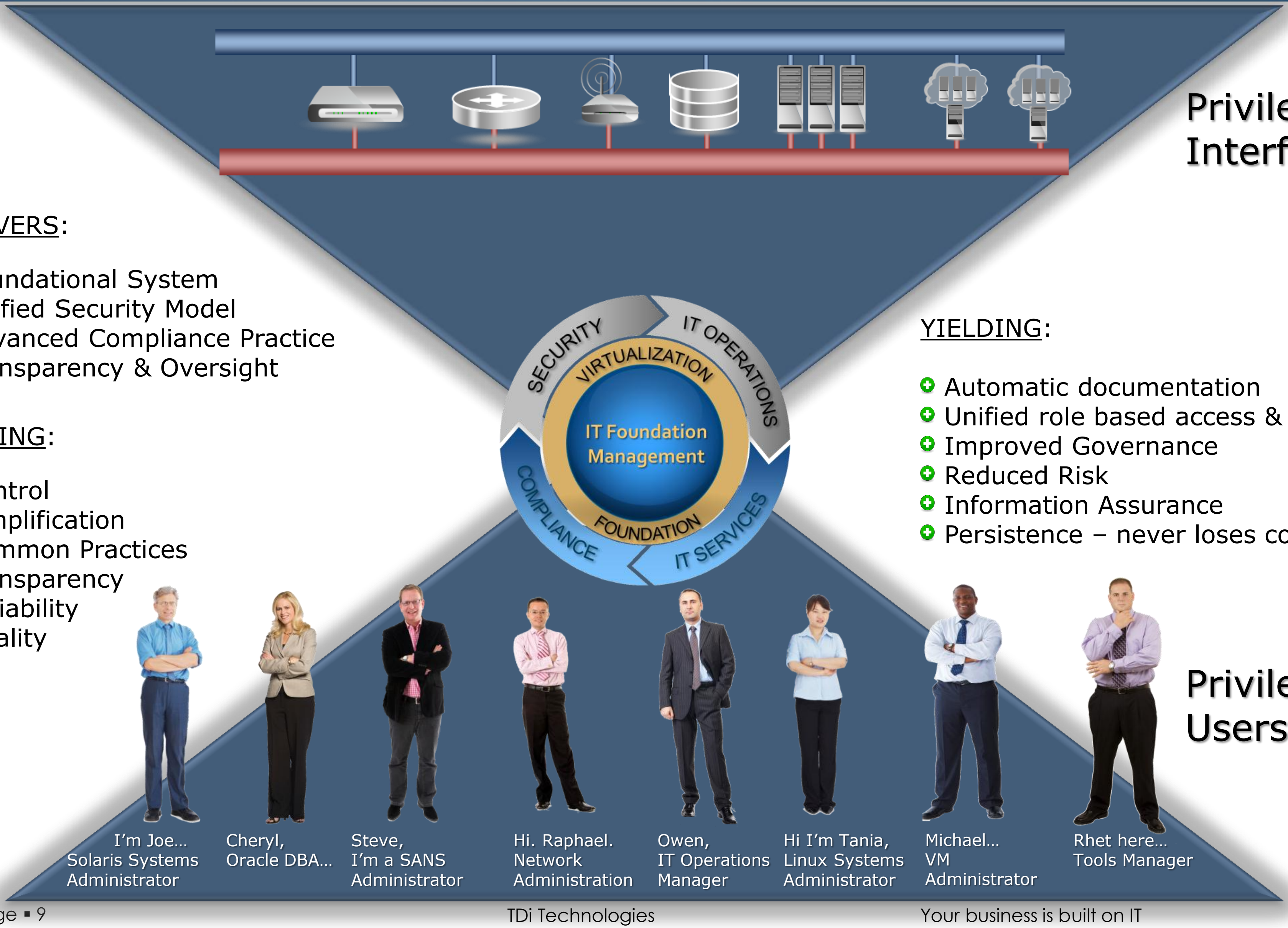
Dave,
Independent
Consultant

Hi I'm Tania,
Linux Systems
Administrator

Michael…
VM
Administrator

Chris here…
Tools Manager

IT Foundation Management



Privileged Interfaces

Privileged Users

DELIVERS:

- Foundational System
- Unified Security Model
- Advanced Compliance Practice
- Transparency & Oversight

DRIVING:

- Control
- Simplification
- Common Practices
- Transparency
- Reliability
- Quality

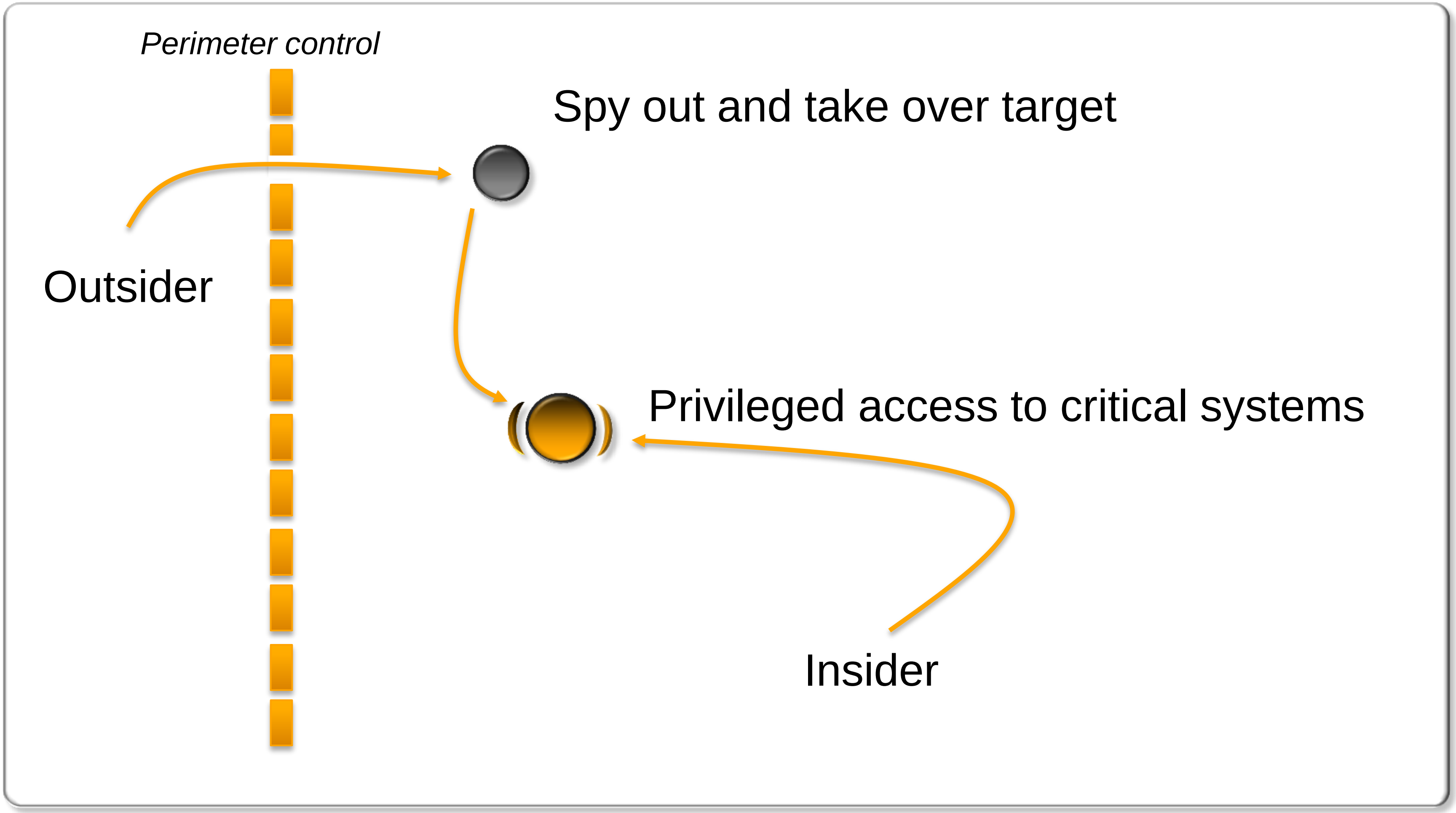
YIELDING:

- Automatic documentation
- Unified role based access & control
- Improved Governance
- Reduced Risk
- Information Assurance
- Persistence – never loses control

SECURITY
IT OPERATIONS
IT SERVICES
COMPLIANCE
VIRTUALIZATION
FOUNDATION
IT Foundation Management

IT Foundation Management Suite
-- Security Foundation Management

Outsider vs Insider, or… low-probability, high-impact



Perimeter control
Spy out and take over target
Outsider
Privileged access to critical systems
Insider

Insider – What ?

- *Insider*
  - is someone who has legitimate access to an organization, its systems, information or other resources.
- Insider threat
  - is a risk that an insider can misuse their access or knowledge to cause harm to the organization/business.
- Insider weakness
  - where an insider performs unsafe actions or fails to apply adequate protection that may expose the organization to accidental damage or malicious attack.

Security Foundation – Questions to ask !

Who has access to the master control interfaces on your hardware?

Who… including employees, contractors, service technicians…?

What can they DO?

What have they DONE?

What authority do these interfaces have? (Senior Engineer)

"I can do <u>ANYTHING</u> I want."

What they have brought in, and what they have taken out?

Have they been compromised?

Are they angry? Tired? Stressed?

Insider Threat – So what !?

- Information Security Group, London:
  - 68% of respondents said that it is the biggest threat to their intellectual property and other sensitive data
    - http://www.isg.rhul.ac.uk/

- Carnegie Mellon University's COMPUTER EMERGENCY RESPONSE TEAM (CERT)

  2010 CYBERSECURITY WATCH SURVEY:
  - 51% of respondents still victims of an insider attack, despite previous experience
  - Remains constant with previous two surveys in 2007 and 2006
  - 67% of respondents: Insider incidents more costly than external breaches
    - http://www.allbusiness.com/crime-law/criminal-offenses-cybercrime/13781867-1.html
    - http://www.cert.org/insider_threat/

Insider data breach costs Bank of America over $10 million

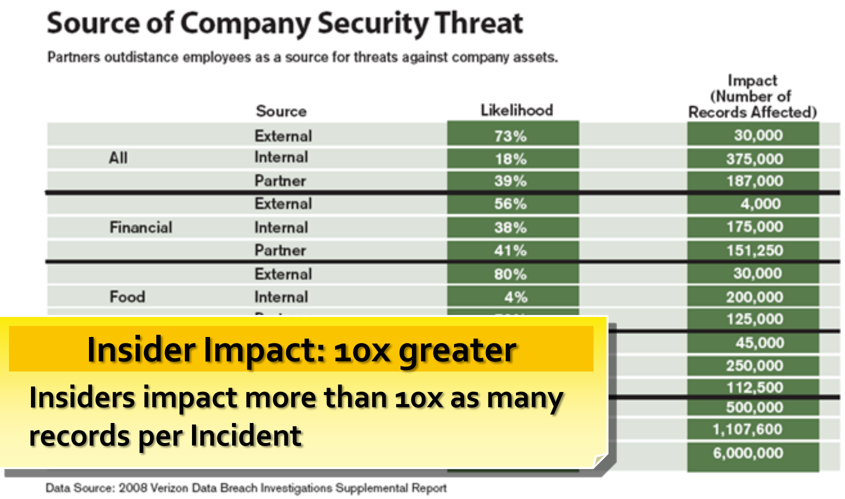
- 26 May 2011
- **The US Secret Service estimates that a data breach at Bank of America in California and other western states cost the bank at least $10 million.**
- *A former bank employee provided customer information to people outside the bank*, who used the data to steal money from around 300 Bank of America customers in California and other western states.
- A report by IDG News Service quoted James Kollar, special agent for the Secret Service in Los Angeles, as estimating that criminals stole at least $10 million from the bank.
- The *Los Angeles Times* reported this week that the criminals were able to obtain names, addresses, social security numbers, phone numbers, bank account numbers, driver's license numbers, birth dates, email addresses, mother's maiden names, PINs, and account balances.

Data theft campaign spanning 14 countries

- 04 August 2011
- **A total of 70 organizations spanning 14 countries were victimized by a five-year operation, likely carried out by a foreign government, that stole intellectual property and other proprietary information, according to a new report by McAfee Labs.**
- The targeted organizations included the US, Canadian, Vietnamese, and Taiwanese governments, the International Olympic Committee, companies from a broad range of industries, and a US national security nonprofit organization.
- The perpetrators stole national security secrets, source code, bug databases, confidential email archives, negotiation plans, document stores, legal contracts, industrial control configurations, design schematics and a lot of other proprietary information.

What does the security Foundation Defend against?

Insider Threat Demographics



Source of Company Security Threat

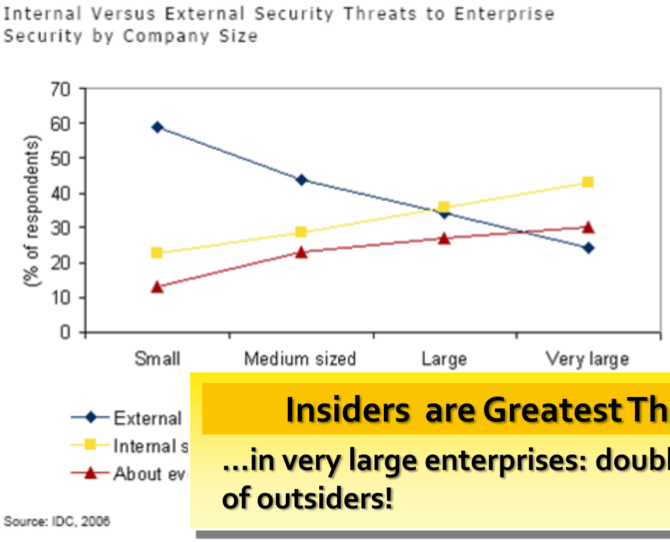
Partners outdistance employees as a source for threats against company assets.

	Source	Likelihood	Impact (Number of Records Affected)
	External	73%	30,000
All	Internal	18%	375,000
	Partner	39%	187,000
	External	56%	4,000
Financial	Internal	38%	175,000
	Partner	41%	151,250
	External	80%	30,000
Food	Internal	4%	200,000
	[illegible]	[illegible]	125,000
			45,000
			250,000
			112,500
			500,000
			1,107,600
			6,000,000

Data Source: 2008 Verizon Data Breach Investigations Supplemental Report

Insider Impact: 10x greater

Insiders impact more than 10x as many records per Incident



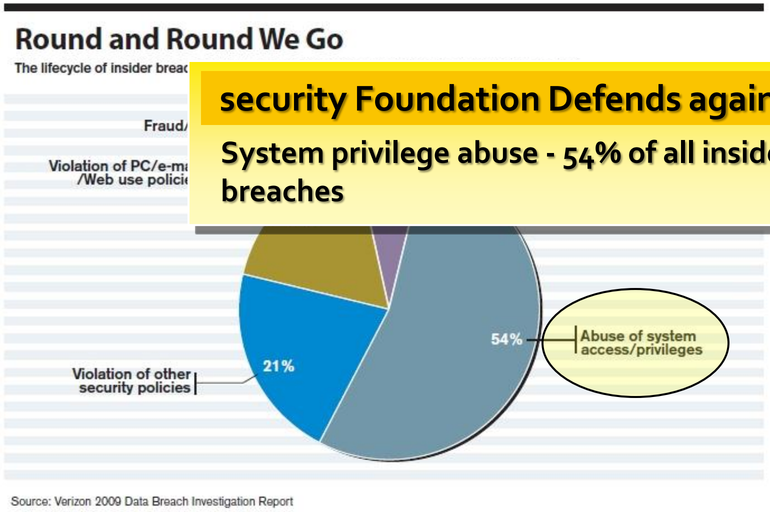
Internal Versus External Security Threats to Enterprise Security by Company Size

Source: IDC, 2006

Insiders are Greatest Threat

...in very large enterprises: double (2x) that of outsiders!

Security Foundation Coverage



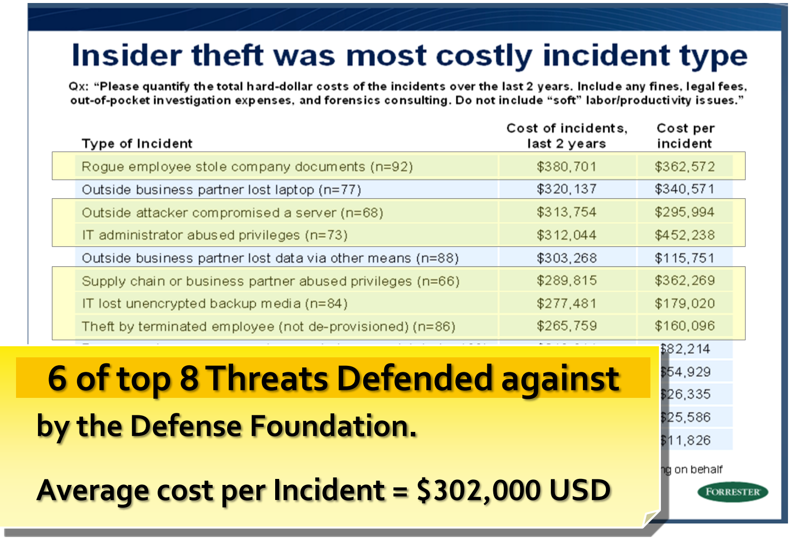
Round and Round We Go

The lifecycle of insider breac

Source: Verizon 2009 Data Breach Investigation Report

security Foundation Defends against

System privilege abuse - 54% of all insider breaches



Insider theft was most costly incident type

Qx: "Please quantify the total hard-dollar costs of the incidents over the last 2 years. Include any fines, legal fees, out-of-pocket investigation expenses, and forensics consulting. Do not include "soft" labor/productivity issues."

Type of Incident	Cost of incidents, last 2 years	Cost per incident
Rogue employee stole company documents (n=92)	$380,701	$362,572
Outside business partner lost laptop (n=77)	$320,137	$340,571
Outside attacker compromised a server (n=68)	$313,754	$295,994
IT administrator abused privileges (n=73)	$312,044	$452,238
Outside business partner lost data via other means (n=88)	$303,268	$115,751
Supply chain or business partner abused privileges (n=66)	$289,815	$362,269
IT lost unencrypted backup media (n=84)	$277,481	$179,020
Theft by terminated employee (not de-provisioned) (n=86)	$265,759	$160,096
		$82,214
		$54,929
		$26,335
		$25,586
		$11,826

g on behalf

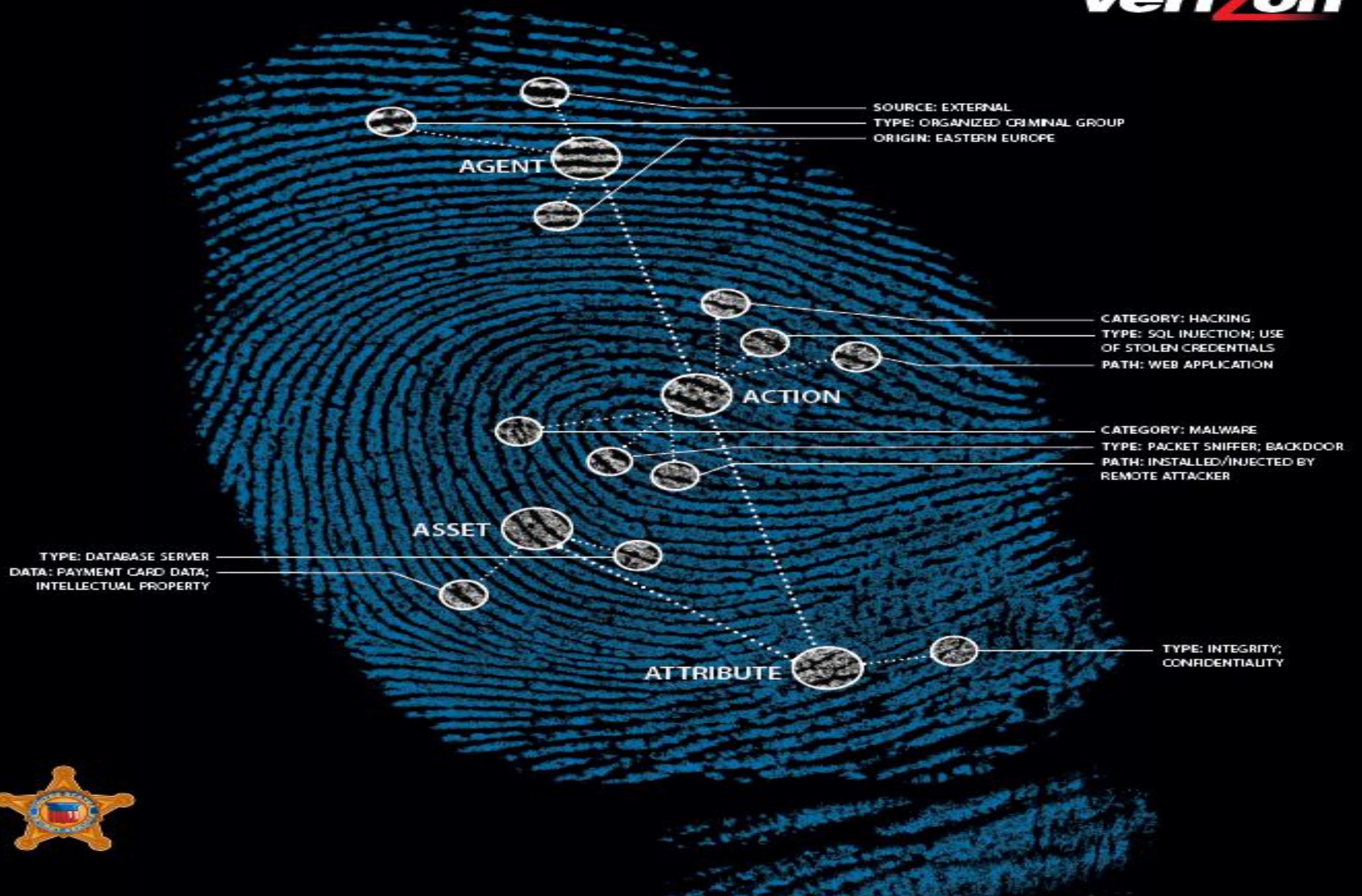
FORRESTER

6 of top 8 Threats Defended against

by the Defense Foundation.

Average cost per Incident = $302,000 USD

verizon


SOURCE: EXTERNAL
TYPE: ORGANIZED CRIMINAL GROUP
ORIGIN: EASTERN EUROPE
AGENT
CATEGORY: HACKING
TYPE: SQL INJECTION; USE OF STOLEN CREDENTIALS
PATH: WEB APPLICATION
ACTION
CATEGORY: MALWARE
TYPE: PACKET SNIFFER; BACKDOOR
PATH: INSTALLED/INJECTED BY REMOTE ATTACKER
ASSET
TYPE: DATABASE SERVER
DATA: PAYMENT CARD DATA; INTELLECTUAL PROPERTY
ATTRIBUTE
TYPE: INTEGRITY; CONFIDENTIALITY

2010 DATA BREACH INVESTIGATIONS REPORT

A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service.

The Insider Threat?

WHO is Behind Data Breaches?
70% resulted from external agents (-9%)
48% were caused by insiders (+26%)
11% implicated business partners (-23%)
27% involved multiple parties (-12%)

Source: 2010 Data Breach Investigations Report

The Insider Threat?

HOW do Breaches Occur?
48% involved privileged misuse (+26%)
40% resulted from hacking (-24%)
38% utilized malware (=)
28% employed social tactics (+16%)
15% comprised physical attacks (+6%)

Source: 2010 Data Breach Investigations Report

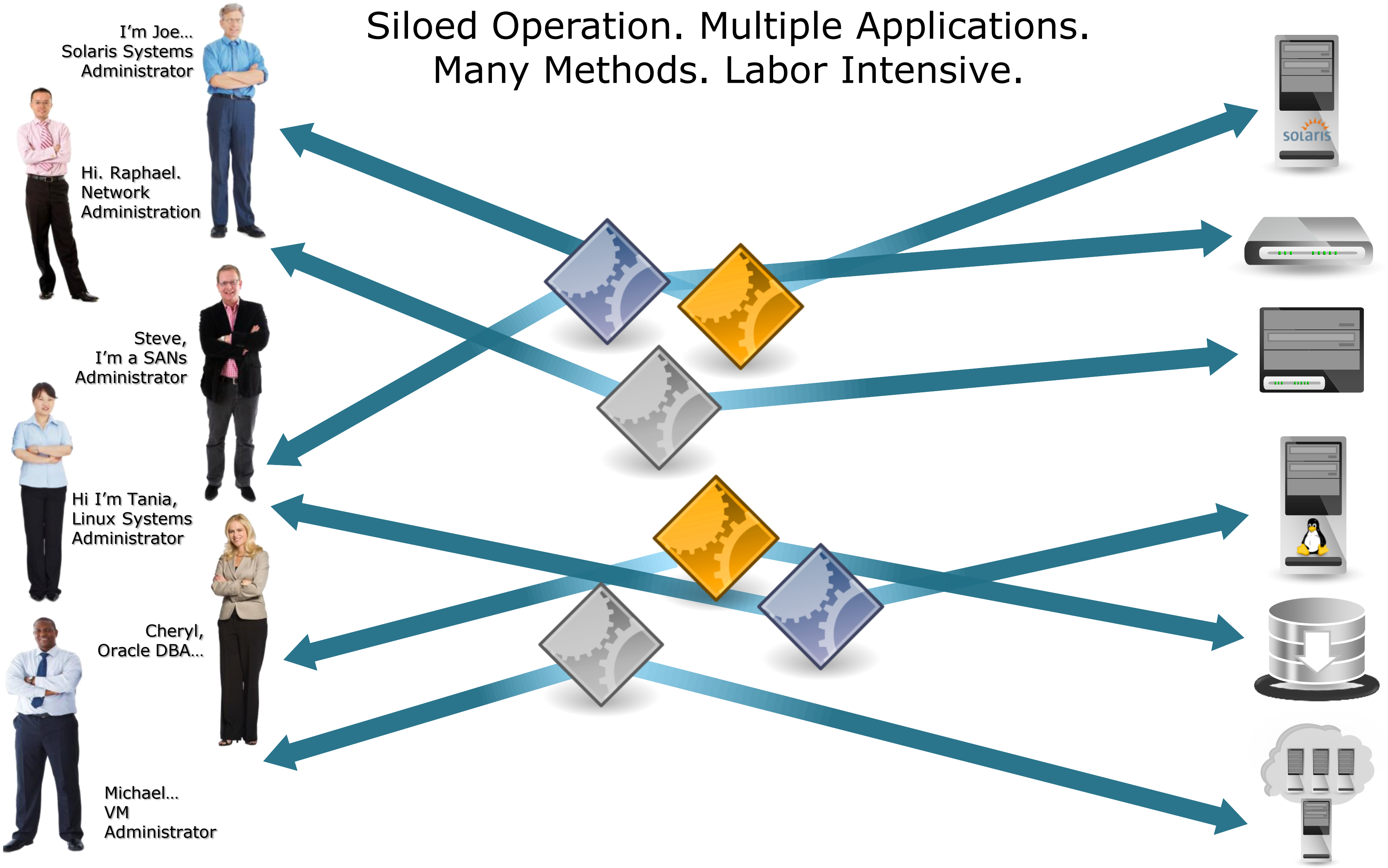
The Insider Threat?

WHAT Commonalities Exist?
98% of all data breached came from servers
85% of attacks were not considered highly difficult
61% were discovered by a third party
86% of victims had evidence of the breach in their logs
96% of breaches were avoidable through simple or intermediate controls
79% of victims subject to PCI DSS had not achieved compliance

Source: 2010 Data Breach Investigations Report

The Challenges are Driven by Complexity

Siloed Operation. Multiple Applications.
Many Methods. Labor Intensive.



I'm Joe…
Solaris Systems
Administrator

Hi. Raphael.
Network
Administration

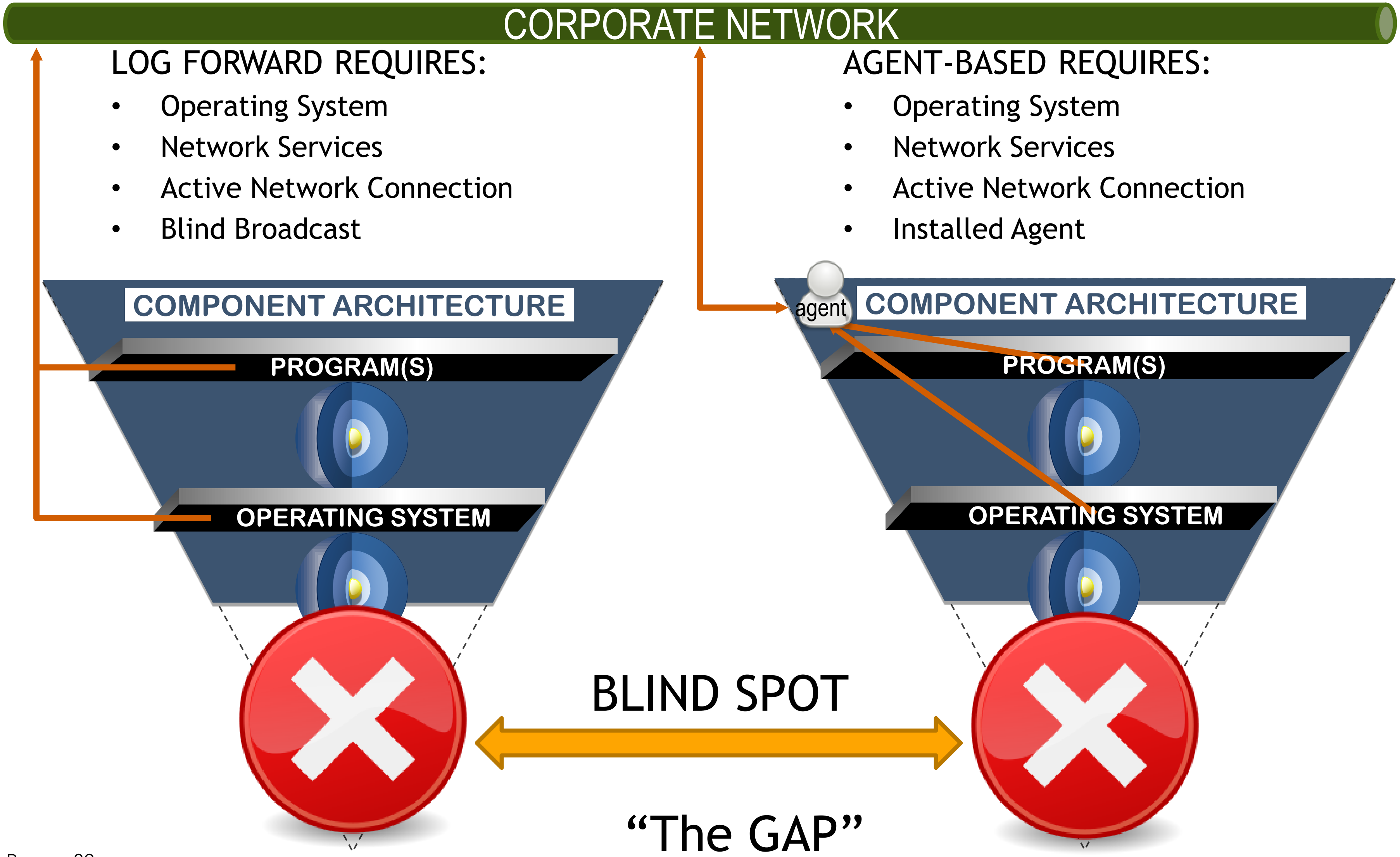
Steve,
I'm a SANs
Administrator

Hi I'm Tania,
Linux Systems
Administrator

Cheryl,
Oracle DBA…

Michael…
VM
Administrator

Common Monitoring Methods



LOG FORWARD REQUIRES:

- Operating System
- Network Services
- Active Network Connection
- Blind Broadcast

AGENT-BASED REQUIRES:

- Operating System
- Network Services
- Active Network Connection
- Installed Agent

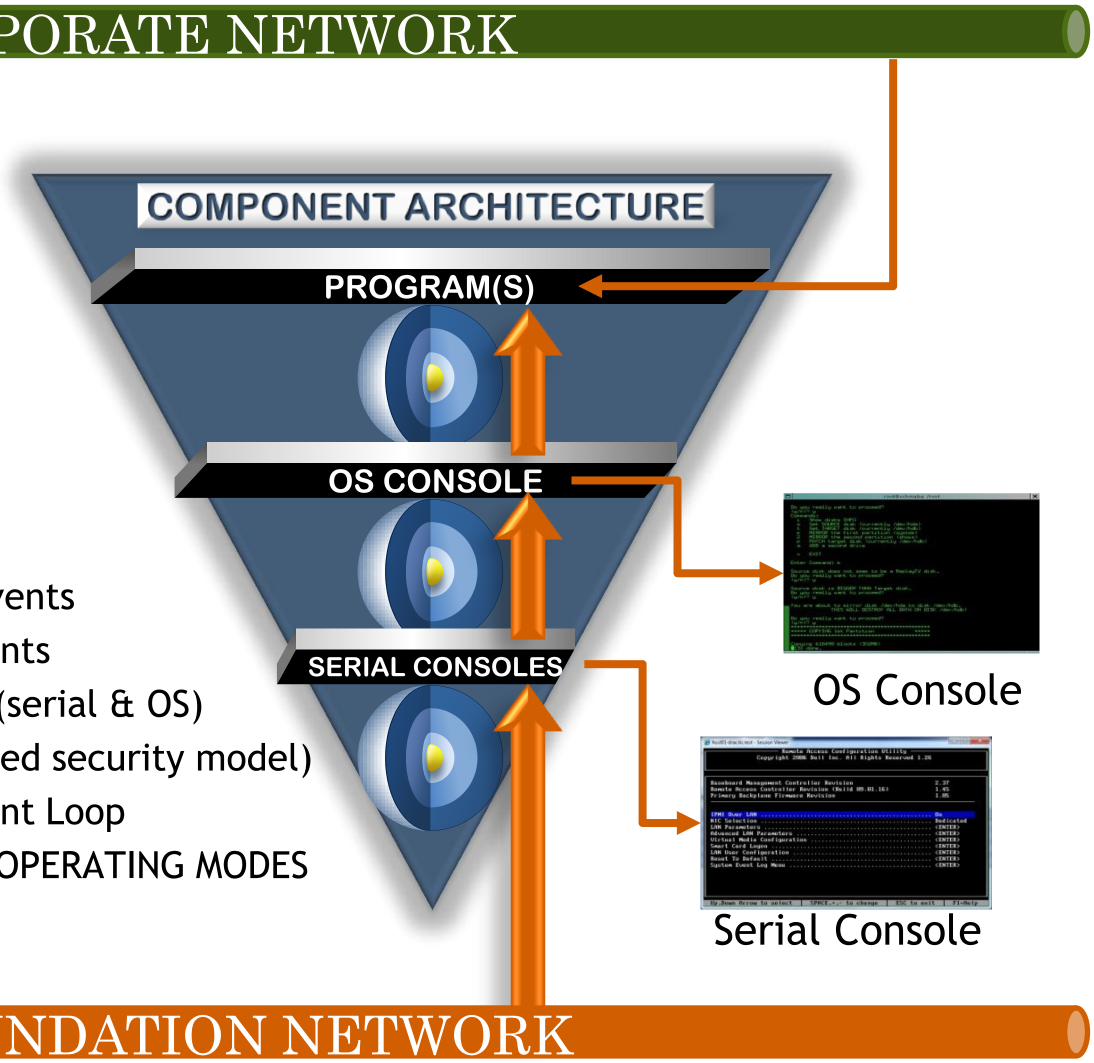
ITFM is bottom-up, outside in, closing the gap

DOESN'T REQUIRE:

- Operating System
- Network Services
- Active Network Connection

ELIMINATES BLINDSPOT BY:

- Capturing Serial Console Events
- Capturing Extended OS Events
- Capturing Console Actions (serial & OS)
- Securing consoles (role-based security model)
- Closing Incident Management Loop
- Maintaining control in ALL OPERATING MODES



```
root@schmabe /root
Do you really want to proceed?
(y/n)? y
Commands:
  i   Show disks INFO
  s   Set SOURCE disk (currently /dev/hda)
  t   Set TARGET disk (currently /dev/hdb)
  1   MIRROR the first partition (system)
  2   MIRROR the second partition (shows)
  p   PATCH target disk (currently /dev/hdb)
  a   ADD a second drive

  x   EXIT

Enter Command: 1

Source disk does not seem to be a ReplayTV disk.
Do you really want to proceed?
(y/n)? y

Source disk is BIGGER THAN Target disk.
Do you really want to proceed?
(y/n)? y

You are about to mirror disk /dev/hda to disk /dev/hdb.
                THIS WILL DESTROY ALL DATA ON DISK /dev/hdb!

Do you really want to proceed?
(y/n)? y
*******************************************
***** COPYING 1st Partition          *****
*******************************************

Copying 6104098 blocks (3000MB)
... done.
```

```
host01-drac.tictest - Session Viewer
                 Remote Access Configuration Utility
           Copyright 2006 Dell Inc. All Rights Reserved 1.25

  Baseboard Management Controller Revision                    2.37
  Remote Access Controller Revision (Build 09.01.16)          1.45
  Primary Backplane Firmware Revision                         1.05

  IPMI Over LAN ............................................. On
  NIC Selection ............................................. Dedicated
  LAN Parameters ............................................ <ENTER>
  Advanced LAN Parameters ................................... <ENTER>
  Virtual Media Configuration ............................... <ENTER>
  Smart Card Logon .......................................... <ENTER>
  LAN User Configuration .................................... <ENTER>
  Reset To Default .......................................... <ENTER>
  System Event Log Menu ..................................... <ENTER>

 Up,Down Arrow to select | SPACE,+,- to change | ESC to exit | F1=Help
```

ITFM is ….., outside in, …….

Inside Out (traditional)

Needs agents, operating system, network

vs

Outside In (ITFM Suite)

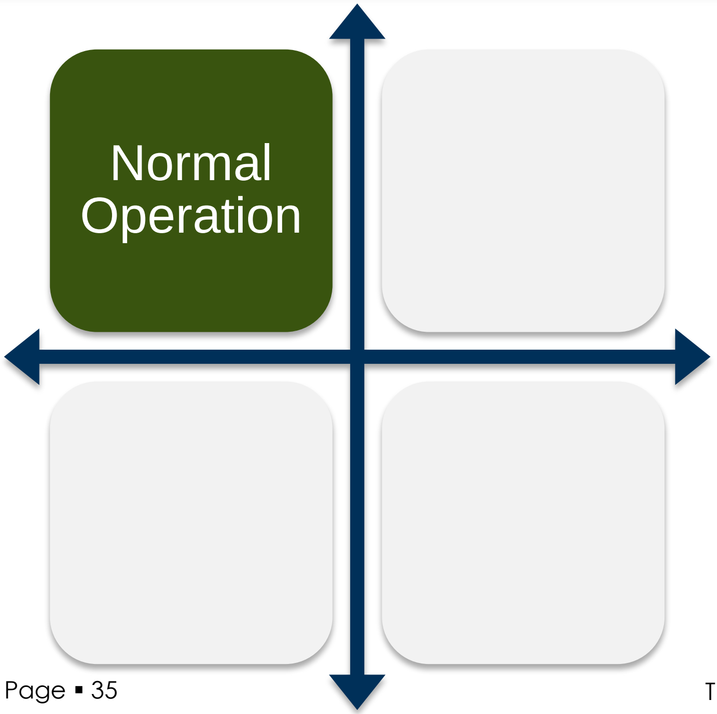
Needs NO agents, NO operating system, NO network

New Capabilities that Drive Success

Traditional Practices

Persistence: Normal Operation
Documentation: Manual

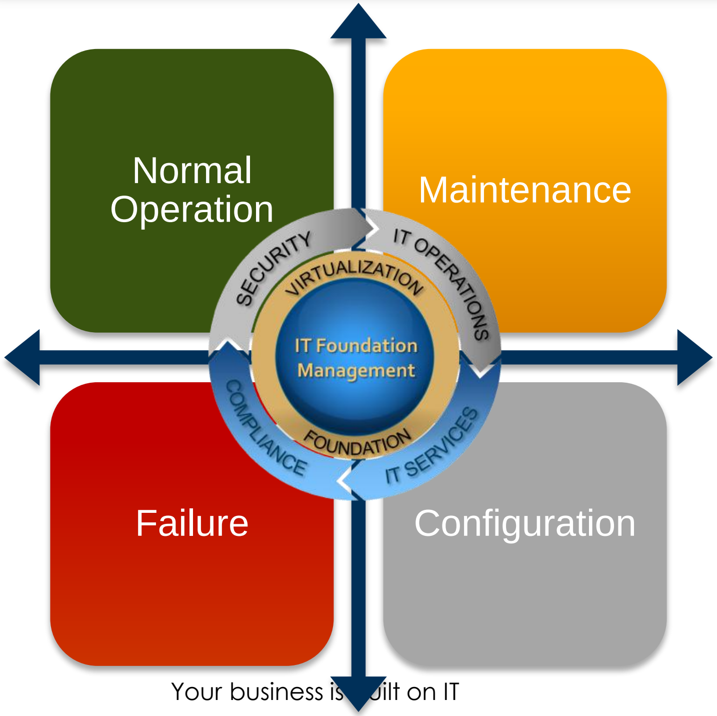
- ⚠ Secured in Normal Mode Only
- ⚠ Documentation is by hand



IT Foundation Management

Persistence: All Modes
Documentation: Automatic

- ● Persistent connection
- ● Full security in all modes
- ● Full documentation in all modes including:
  - ✓ Normal Operation
  - ✓ Maintenance
  - ✓ Configuration
  - ✓ Failure

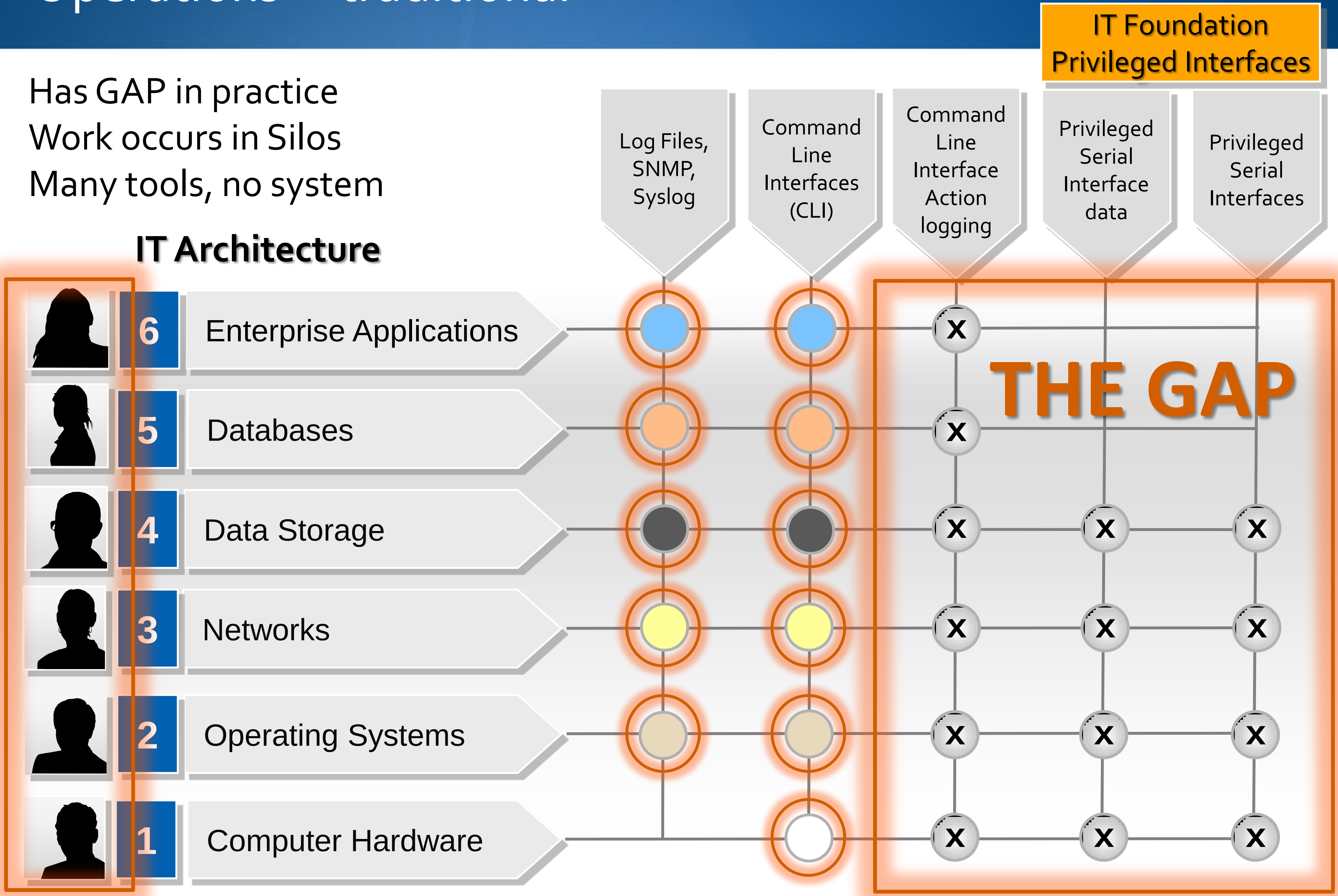


SECURITY
IT OPERATIONS
VIRTUALIZATION
IT Foundation Management
FOUNDATION
COMPLIANCE
IT SERVICES

IT Foundation Management Suite
-- Operations Foundation Management

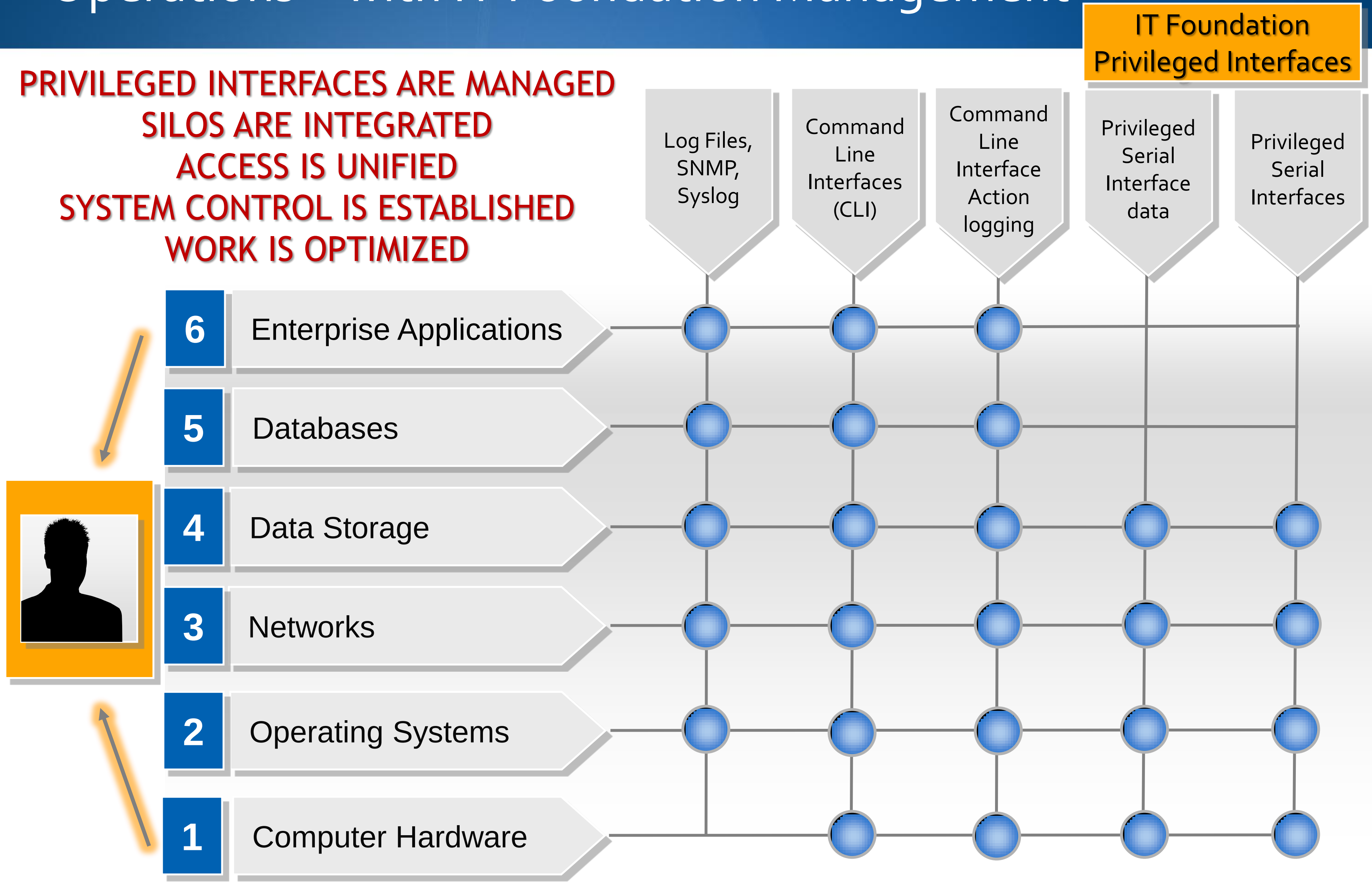
Operations -- traditional

Has GAP in practice
Work occurs in Silos
Many tools, no system


IT Foundation Privileged Interfaces
IT Architecture
Log Files, SNMP, Syslog
Command Line Interfaces (CLI)
Command Line Interface Action logging
Privileged Serial Interface data
Privileged Serial Interfaces
6 Enterprise Applications
5 Databases
4 Data Storage
3 Networks
2 Operating Systems
1 Computer Hardware
THE GAP
X

Operations – with IT Foundation Management

PRIVILEGED INTERFACES ARE MANAGED
SILOS ARE INTEGRATED
ACCESS IS UNIFIED
SYSTEM CONTROL IS ESTABLISHED
WORK IS OPTIMIZED


IT Foundation Privileged Interfaces
Log Files, SNMP, Syslog
Command Line Interfaces (CLI)
Command Line Interface Action logging
Privileged Serial Interface data
Privileged Serial Interfaces
6 Enterprise Applications
5 Databases
4 Data Storage
3 Networks
2 Operating Systems
1 Computer Hardware

Simplification, Oversight, and Management

Simplification

- Manages all Privileged Interfaces with ONE system
- Encodes and automates common tasks
- Provides universal operations methodology
- Centralizes management

Transparency and Oversight

- All Privileged User actions automatically recorded
- Access control centralized
- Authorization centralized
- Compliance automated
- Management centralized

Improved Maintenance

- Automates repetitive actions
- One maintenance methodology
- Automatic forensic history creation
- Serves all platforms
- Improves efficiency

Transparency and Oversight

With the Traditional Approach…

⚠ We require access to be controlled

⚠ We require changes to be documented

❗ I have records, but I do not have a means to verify them

⚠ We are required to manually document changes

⚠ Usually we do that immediately after making a change

⚠ Sometimes things are very busy, and we have to document changes later on

❗ Sometimes changes just don't get documented….

With IT Foundation Management…

✓ Access is enforced against Policy through IT Foundation Management

✓ All change records are available in real-time: recorded down to the key stroke

✓ Verification is simple and accurate: always

✓ The system documents changes for us automatically: in real-time

WE DON'T HAVE TO WORRY ABOUT DOCUMENTING CHANGES – WE JUST CONCENTRATE ON DOING OUR JOBS!

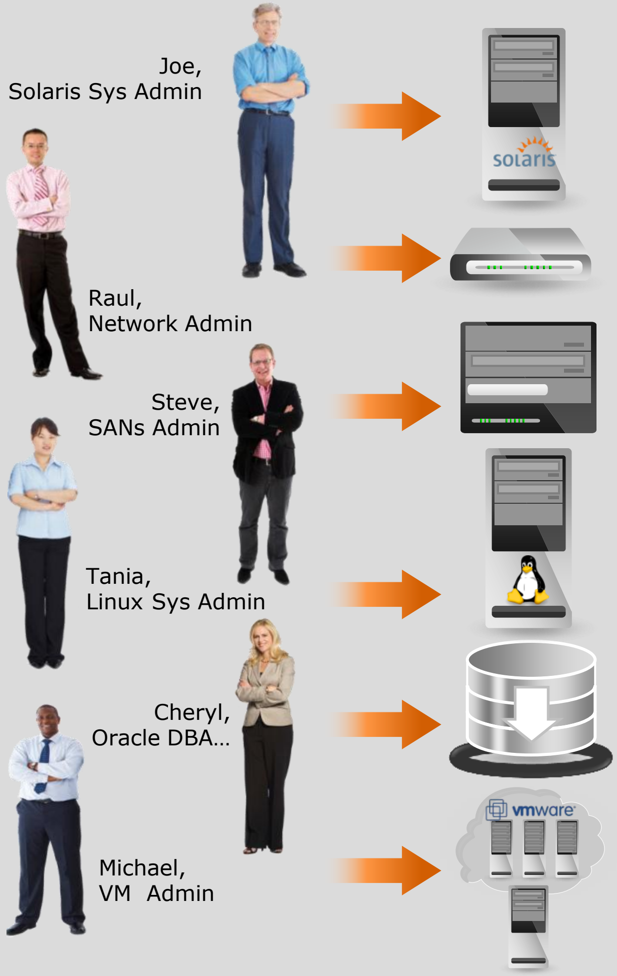
SECURITY
IT OPERATIONS
VIRTUALIZATION
IT Foundation Management
FOUNDATION
COMPLIANCE
IT SERVICES

IT Foundation Management Suite
-- Compliance Foundation Management

IT Foundation Compliance Challenges

Daily Changes Occur:

Break/Fix, Incidents, Configuration, Patching, and Maintenance



Compliance Requires:

Change Control and Documentation

HIPAA Health Insurance Portability & Accountability Act

PCI DSS COMPLIANT

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CISRCP

CISO Executive Membership ISSA

U.S. SECURITIES AND EXCHANGE COMMISSION MCMXXXIV

Sarbanes-Oxley --*SOX*

Yet foundational changes are often recorded manually, resulting in:

- Inaccurate information
- Incomplete records
- Documentation lag
- Large time consumption (cost)
- Impossible to verify
- Lack of transparency/oversight

Consequences Include:

Undo Risk and Cost to the Business

Inadequate Records

- FTE Back-filling Gaps
- Fines

Human Error

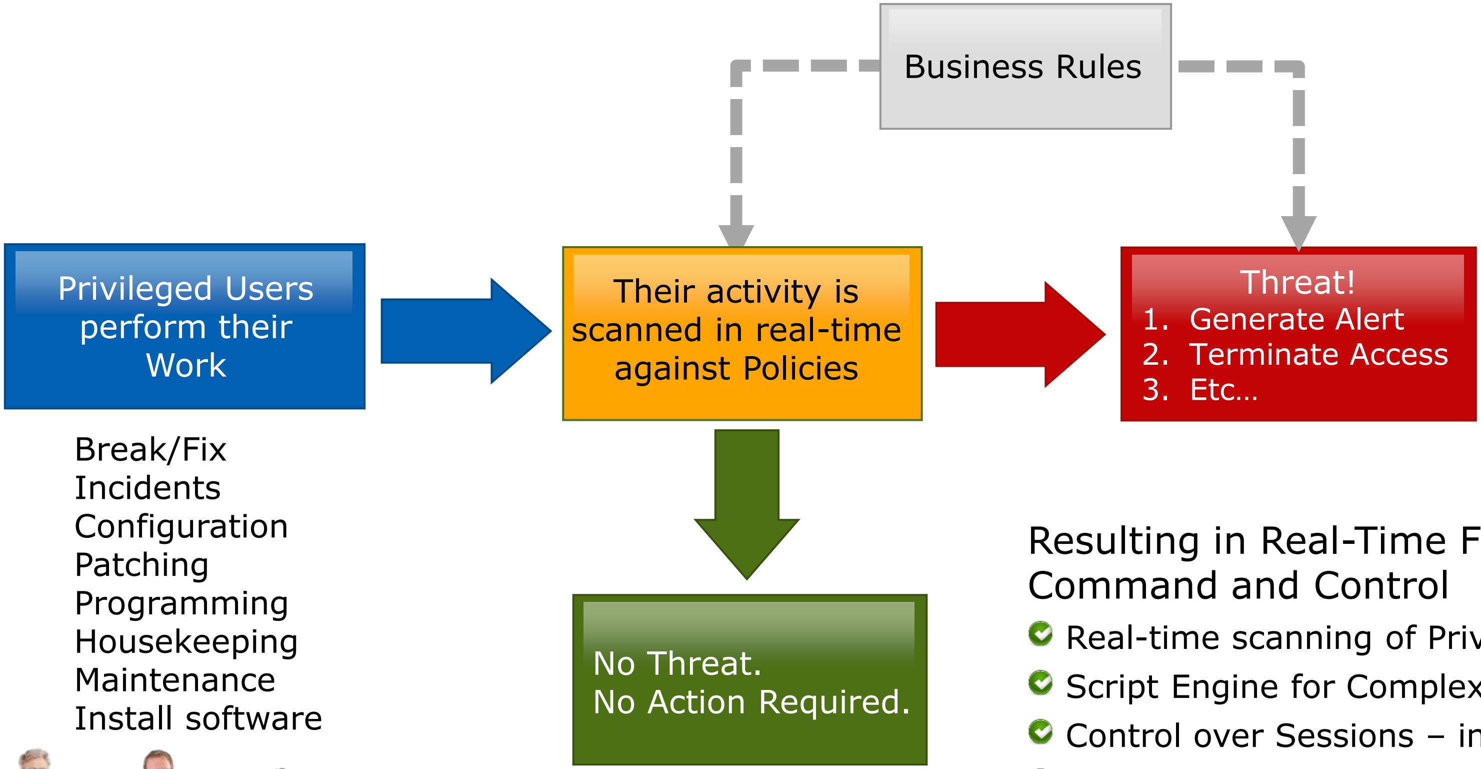
- Service Disruptions
- Sensitive Data Breaches

Lack of Control

- Out-of-policy activity
- Out-of-policy access
- Lagging Response (often long after-the-fact)

Command and Control

IT Foundation Management Delivers Real-time Policy Enforcement

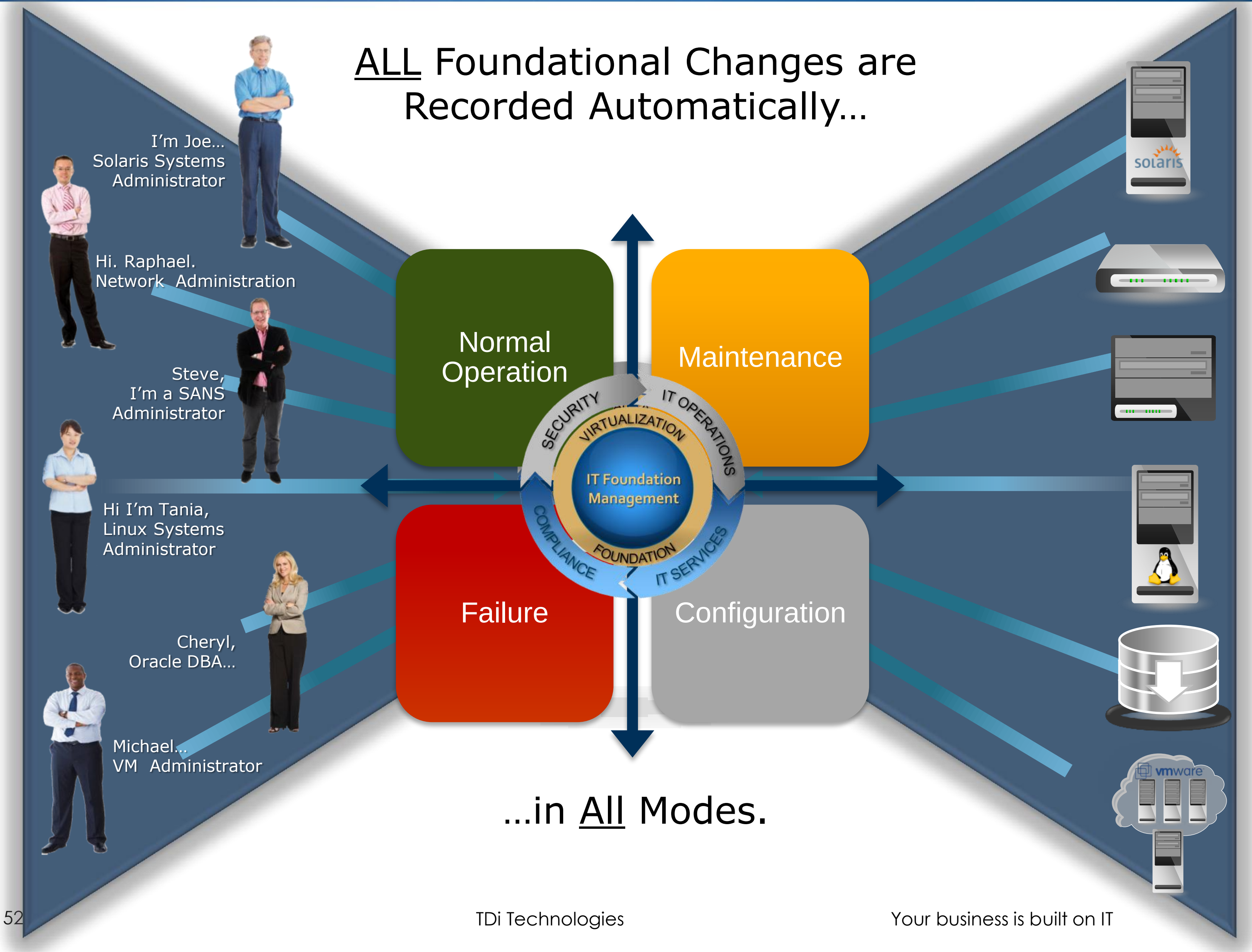


Break/Fix
Incidents
Configuration
Patching
Programming
Housekeeping
Maintenance
Install software

Resulting in Real-Time Foundational Command and Control

- ✓ Real-time scanning of Privileged User Activity
- ✓ Script Engine for Complex and Wildcard Rules
- ✓ Control over Sessions – including Termination
- ✓ Configurable Alert Priorities
- ✓ Custom Actions (email, text, terminate)
- ✓ Unlimited Rules Support
- ✓ Directly Embed Compliance Rules in Scans

With IT Foundation Management:



ALL Foundational Changes are Recorded Automatically…

I'm Joe… Solaris Systems Administrator

Hi. Raphael. Network Administration

Steve, I'm a SANS Administrator

Hi I'm Tania, Linux Systems Administrator

Cheryl, Oracle DBA…

Michael… VM Administrator

Normal Operation

Maintenance

Failure

Configuration

SECURITY

IT OPERATIONS

VIRTUALIZATION

COMPLIANCE

IT SERVICES

FOUNDATION

IT Foundation Management

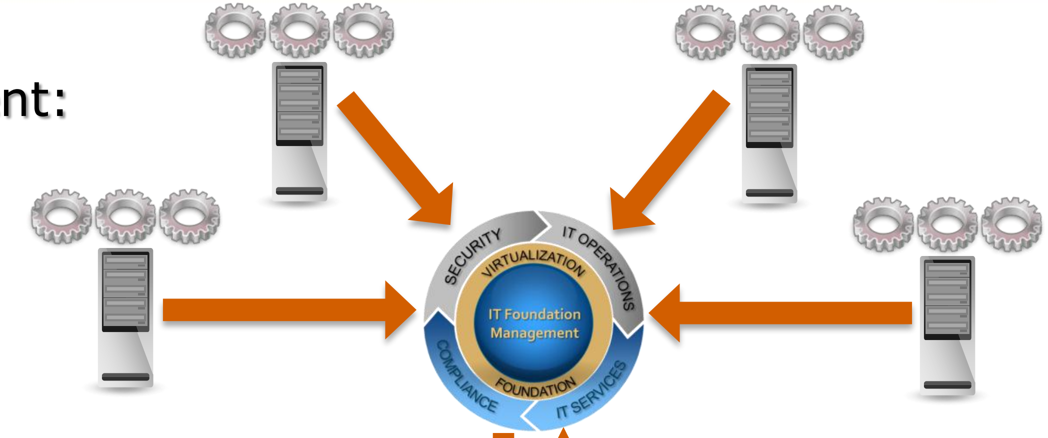
…in All Modes.

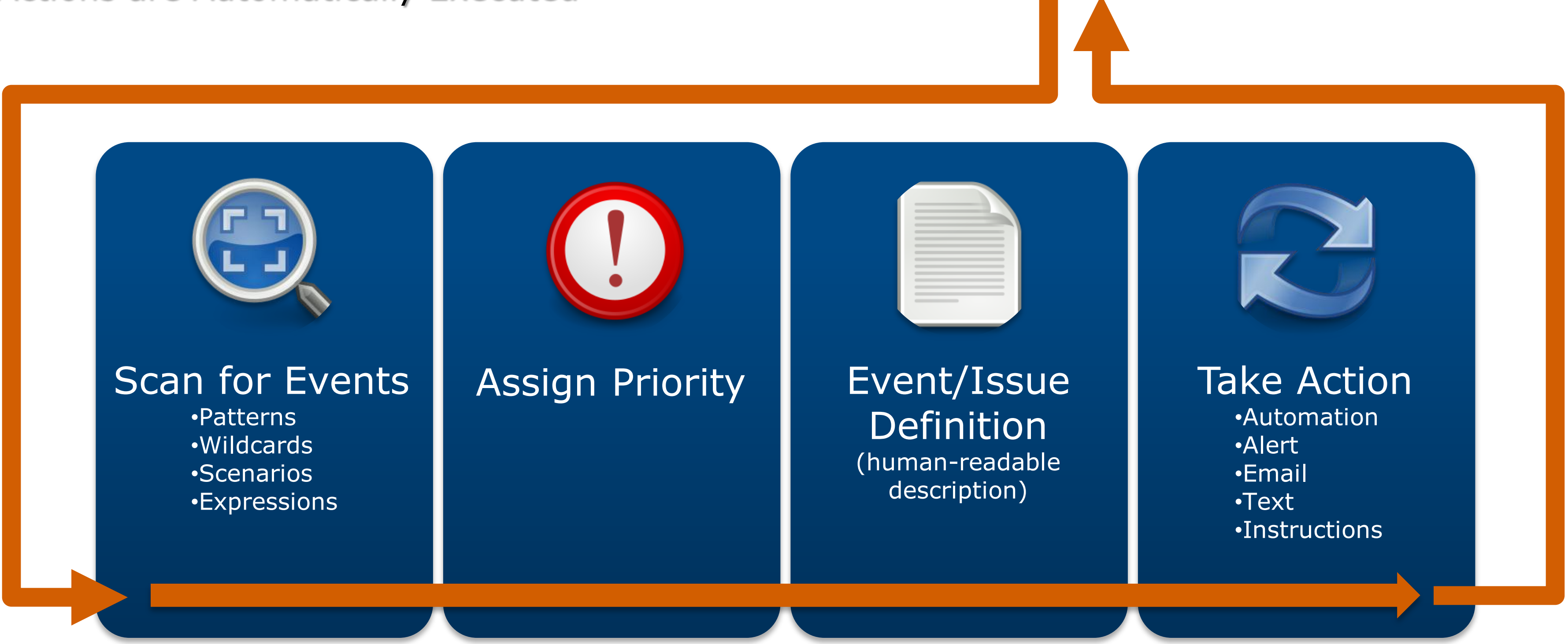
IT Foundation Management Suite
-- Services Foundation Management

IT Foundation Service Management

Foundation Services Management:

1) Applications write data to logs
2) Updates are Captured in Real-Time
3) Information is scanned for Events
4) Events are Assigned Proper Priority
5) Events have Clear Explanations
6) Actions are Automatically Executed





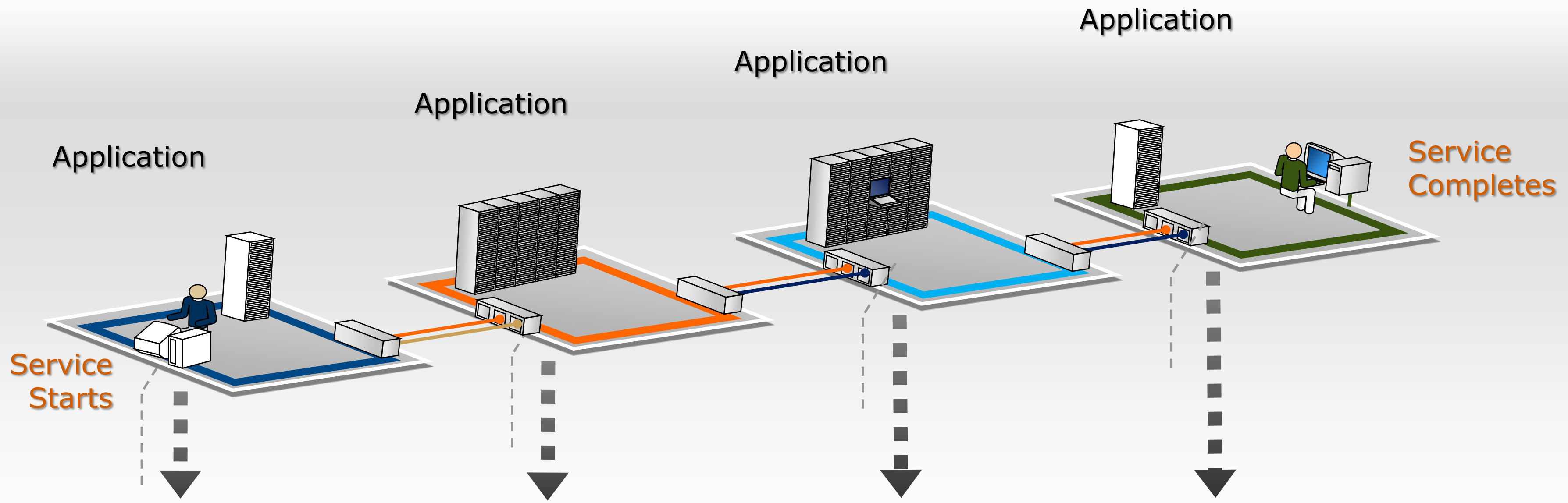
Scan for Events
•Patterns
•Wildcards
•Scenarios
•Expressions

Assign Priority

Event/Issue Definition
(human-readable description)

Take Action
•Automation
•Alert
•Email
•Text
•Instructions

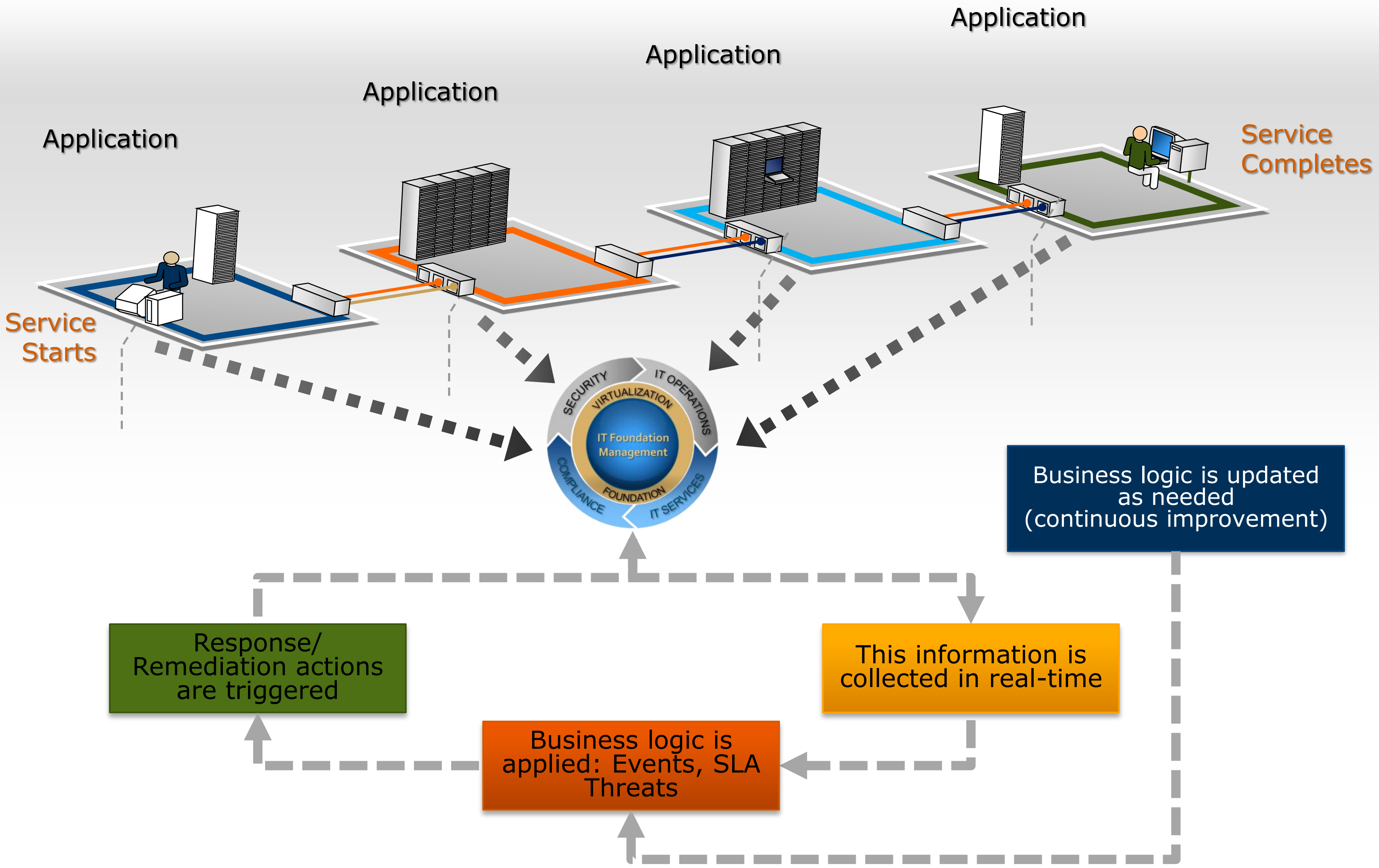
Understanding the IT Services Foundation



SERVICE-RELATED MESSAGES		
Messages are Output from:	**Message Type**	**Description**
•Custom Applications •User Customizations •Packaged Applications	Context	Meaningful dialog: "Credit Limit Exceeded for Customer XYZ"
•Custom Applications •User Customizations •Packaged Applications •Components/Libraries	Activity /Tracking	Status: Received, Start, Stop, Suspend, Resume, Transfer, Complete, etc.

GENERAL MESSAGES		
Messages are Output from:	**Message Types**	**Description**
•Packaged Applications •Components/Libraries •Operating Systems •Hardware	Vendor Defined	Generic: (critical, error, warning, information)
•Custom applications	User Defined	Generic: (critical, error, warning, information)

Managing the IT Services Foundation



Business logic is updated as needed (continuous improvement)

This information is collected in real-time

Business logic is applied: Events, SLA Threats

Response/ Remediation actions are triggered

Key Differentiators

IT Foundation Management Empowers Service Success:

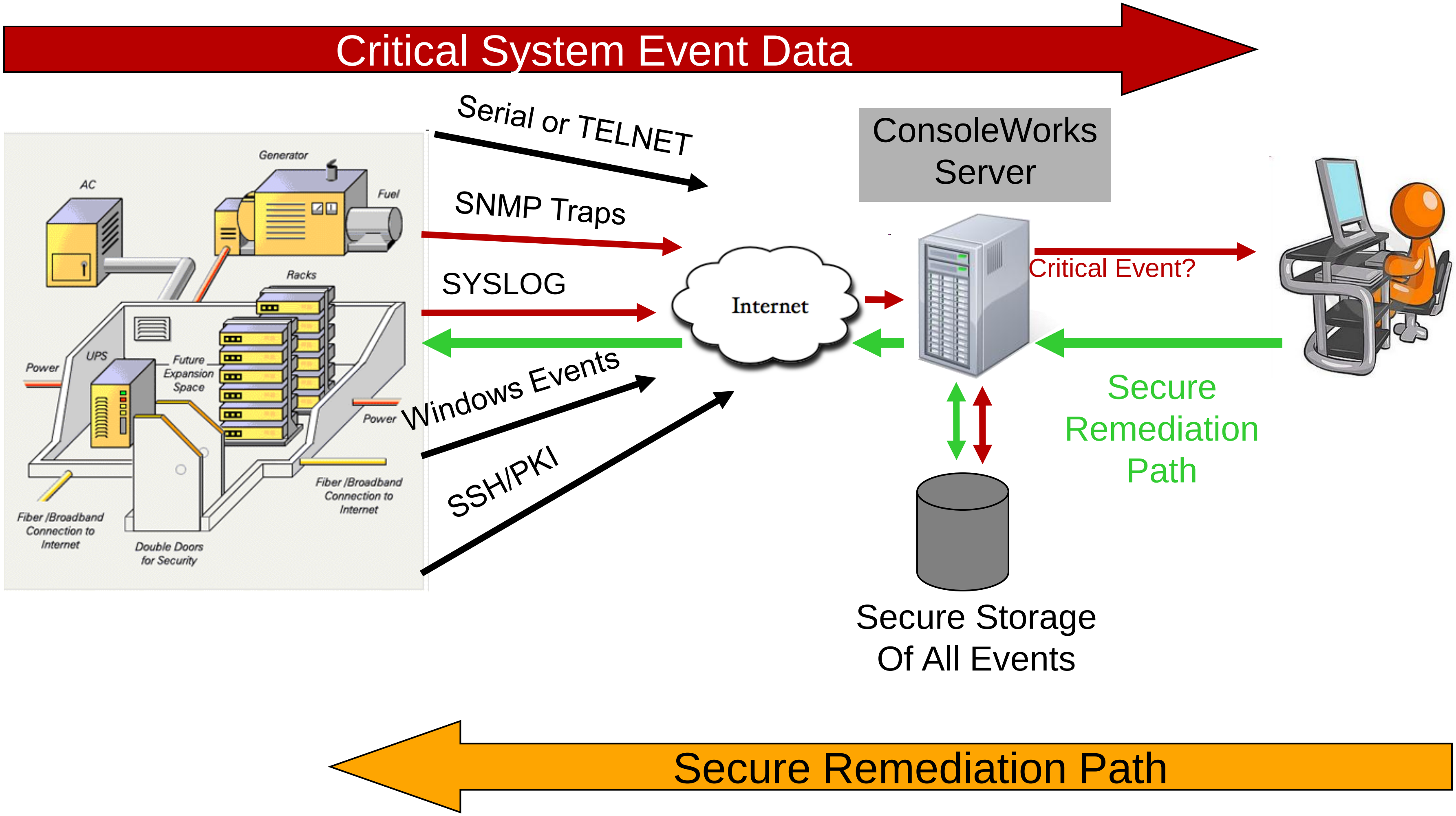
- All message sources monitored in real-time
- Messages captured as they are output
- All messages digitally time-stamped for correlation

- Non-invasive (no agent software to install)
- Virtually no performance impact
- Spans B2B Service Chains

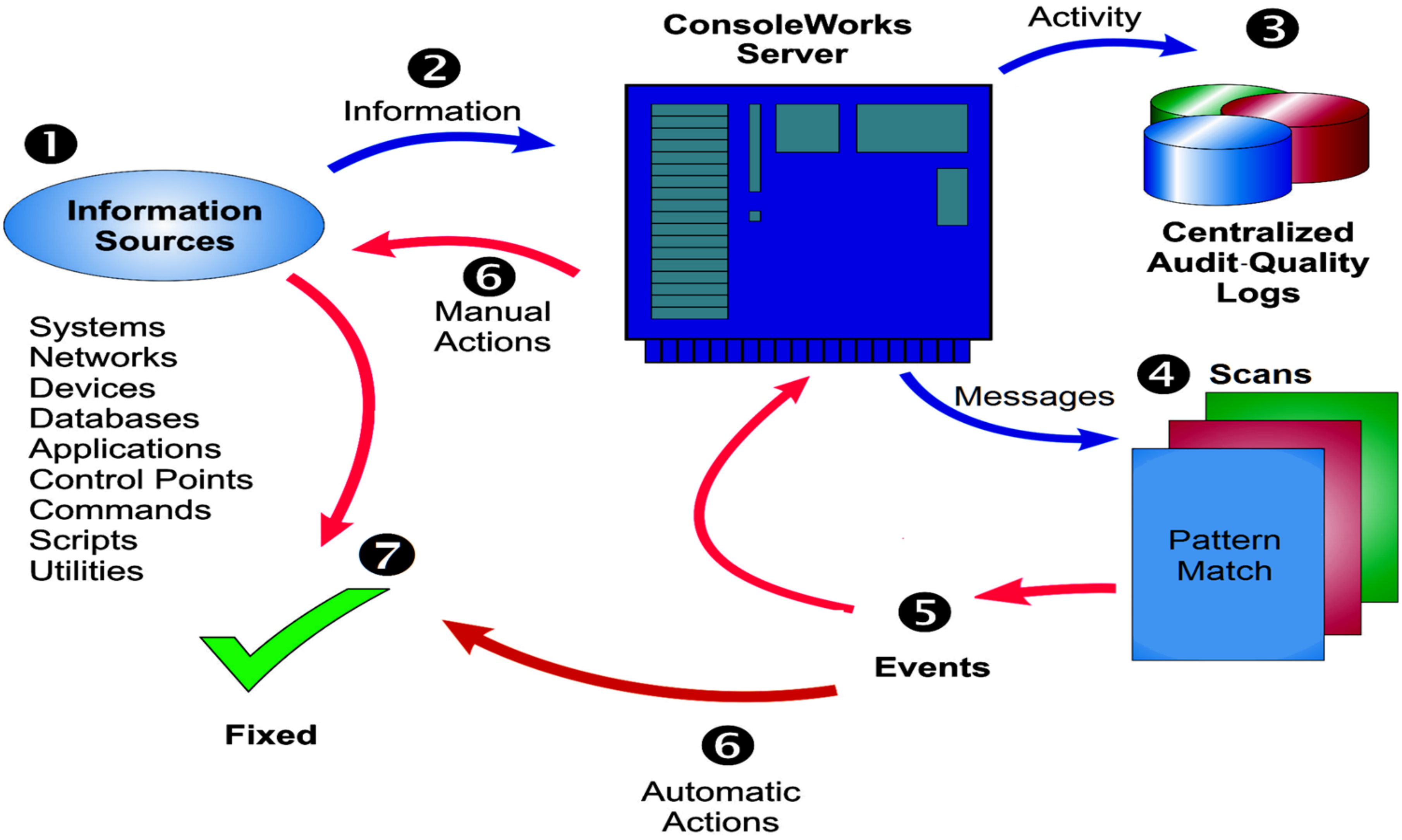
- Comprehensive pattern recognition
- Powerful Script Engine for complex scenarios
- Supports internal and external automation

Technology

Protecting the IT Infrastructure



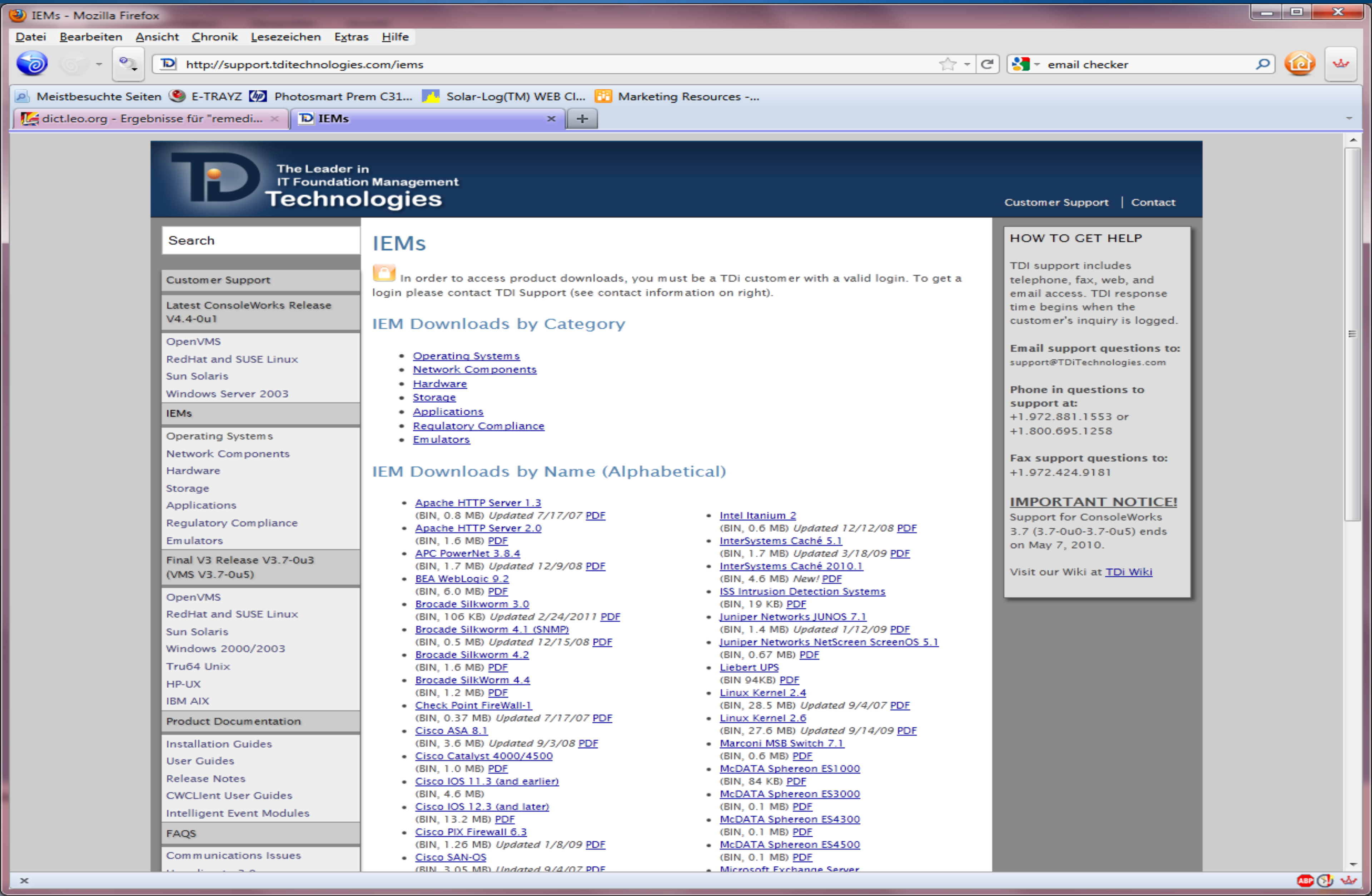
Overview


ConsoleWorks Server
❷
Information
❶
Information Sources
Systems
Networks
Devices
Databases
Applications
Control Points
Commands
Scripts
Utilities
❻
Manual Actions
Activity
❸
Centralized Audit-Quality Logs
Messages
❹
Scans
Pattern Match
❺
Events
❼
Fixed
❻
Automatic Actions

Platforms

OPERATING SYSTEM	HARDWARE PLATFORM
HP OpenVMS 8.2 or later	Alpha™, Itanium™
Windows Server 2003, 2008	Intel®, AMD
Sun™ Solaris™ 8 or 10	UltraSPARC®
Red Hat® Enterprise Linux® Server 4.0 or later	Intel, AMD
Novell® SUSE™ Linux Enterprise Server 9.0 or later	Intel, AMD
Ubuntu latest	Intel, AMD
Debian latest	Intel, AMD

Vendor related data: Intelligent Event Modules


IEMs - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://support.tditechnologies.com/iems
email checker
Meistbesuchte Seiten
E-TRAYZ
Photosmart Prem C31...
Solar-Log(TM) WEB Cl...
Marketing Resources -...
dict.leo.org - Ergebnisse für "remedi...
IEMs

The Leader in IT Foundation Management
Technologies

Customer Support | Contact

Search

Customer Support

Latest ConsoleWorks Release V4.4-0u1

- OpenVMS
- RedHat and SUSE Linux
- Sun Solaris
- Windows Server 2003

IEMs

- Operating Systems
- Network Components
- Hardware
- Storage
- Applications
- Regulatory Compliance
- Emulators

Final V3 Release V3.7-0u3 (VMS V3.7-0u5)

- OpenVMS
- RedHat and SUSE Linux
- Sun Solaris
- Windows 2000/2003
- Tru64 Unix
- HP-UX
- IBM AIX

Product Documentation

- Installation Guides
- User Guides
- Release Notes
- CWCLient User Guides
- Intelligent Event Modules

FAQS

- Communications Issues

IEMs

In order to access product downloads, you must be a TDi customer with a valid login. To get a login please contact TDI Support (see contact information on right).

IEM Downloads by Category

- Operating Systems
- Network Components
- Hardware
- Storage
- Applications
- Regulatory Compliance
- Emulators

IEM Downloads by Name (Alphabetical)

- Apache HTTP Server 1.3
  (BIN, 0.8 MB) *Updated 7/17/07* PDF
- Apache HTTP Server 2.0
  (BIN, 1.6 MB) PDF
- APC PowerNet 3.8.4
  (BIN, 1.7 MB) *Updated 12/9/08* PDF
- BEA WebLogic 9.2
  (BIN, 6.0 MB) PDF
- Brocade Silkworm 3.0
  (BIN, 106 KB) *Updated 2/24/2011* PDF
- Brocade Silkworm 4.1 (SNMP)
  (BIN, 0.5 MB) *Updated 12/15/08* PDF
- Brocade Silkworm 4.2
  (BIN, 1.6 MB) PDF
- Brocade SilkWorm 4.4
  (BIN, 1.2 MB) PDF
- Check Point FireWall-1
  (BIN, 0.37 MB) *Updated 7/17/07* PDF
- Cisco ASA 8.1
  (BIN, 3.6 MB) *Updated 9/3/08* PDF
- Cisco Catalyst 4000/4500
  (BIN, 1.0 MB) PDF
- Cisco IOS 11.3 (and earlier)
  (BIN, 4.6 MB)
- Cisco IOS 12.3 (and later)
  (BIN, 13.2 MB) PDF
- Cisco PIX Firewall 6.3
  (BIN, 1.26 MB) *Updated 1/8/09* PDF
- Cisco SAN-OS
  (BIN, 3.05 MB) *Updated 9/4/07* PDF
- Intel Itanium 2
  (BIN, 0.6 MB) *Updated 12/12/08* PDF
- InterSystems Caché 5.1
  (BIN, 1.7 MB) *Updated 3/18/09* PDF
- InterSystems Caché 2010.1
  (BIN, 4.6 MB) *New!* PDF
- ISS Intrusion Detection Systems
  (BIN, 19 KB) PDF
- Juniper Networks JUNOS 7.1
  (BIN, 1.4 MB) *Updated 1/12/09* PDF
- Juniper Networks NetScreen ScreenOS 5.1
  (BIN, 0.67 MB) PDF
- Liebert UPS
  (BIN 94KB) PDF
- Linux Kernel 2.4
  (BIN, 28.5 MB) *Updated 9/4/07* PDF
- Linux Kernel 2.6
  (BIN, 27.6 MB) *Updated 9/14/09* PDF
- Marconi MSB Switch 7.1
  (BIN, 0.6 MB) PDF
- McDATA Sphereon ES1000
  (BIN, 84 KB) PDF
- McDATA Sphereon ES3000
  (BIN, 0.1 MB) PDF
- McDATA Sphereon ES4300
  (BIN, 0.1 MB) PDF
- McDATA Sphereon ES4500
  (BIN, 0.1 MB) PDF
- Microsoft Exchange Server

HOW TO GET HELP

TDI support includes telephone, fax, web, and email access. TDI response time begins when the customer's inquiry is logged.

Email support questions to:
support@TDiTechnologies.com

Phone in questions to support at:
+1.972.881.1553 or
+1.800.695.1258

Fax support questions to:
+1.972.424.9181

IMPORTANT NOTICE!
Support for ConsoleWorks 3.7 (3.7-0u0-3.7-0u5) ends on May 7, 2010.

Visit our Wiki at TDi Wiki

References

Reference Customers

- Bank of America, Bank of England, BNY Mellon, Commerzbank, BNP Paribas, AIG, Handelsbanken, Computershare,…
- Direct TV, British Library,…
- Pfizer, Lahey Clinic, UCSF Medical Center, Mayo Clinic,…
- Fairchild, TriQuint Semiconductor, ESA,…
- HP & IBM (Managed Services)
- Verizon
- Utilities:
  - Kansas City, PECO (Philadelphia), Tacoma Power
  - Westar Energy (Kansas), CAISO (California), Pacificorp (Oregon)
  - Exelon Corp. (USA, $18Bill revenue)

We focus on….

making software do what it can,

so that people can concentrate on what only humans can do!

Questions