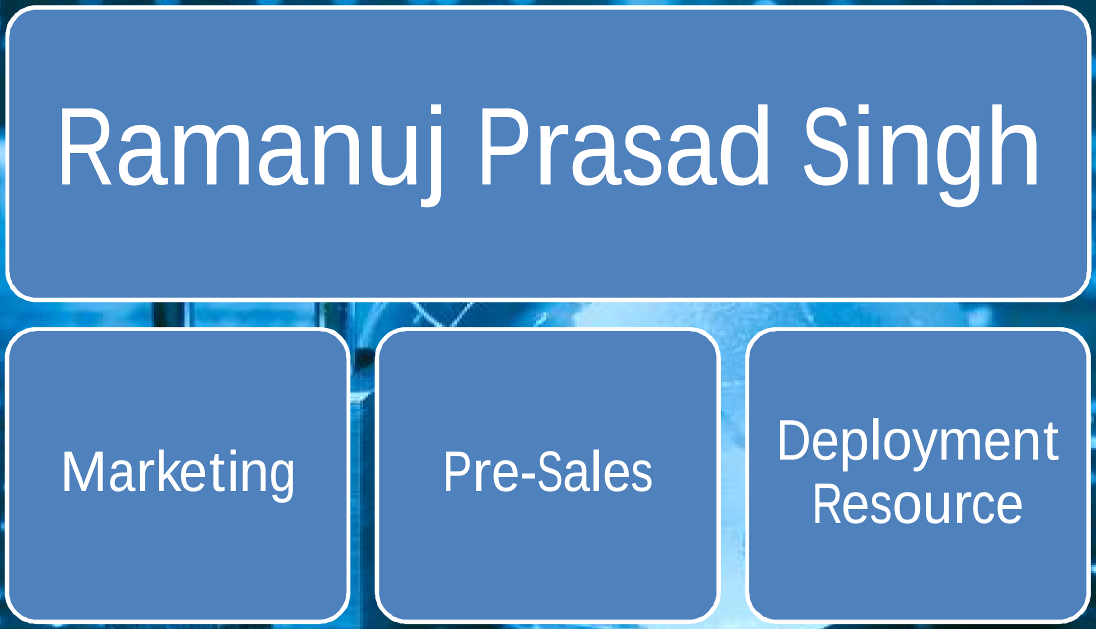
Information Security services Planning & Roadmap

Ramanuj Prasad Singh

ISS Practice Structure



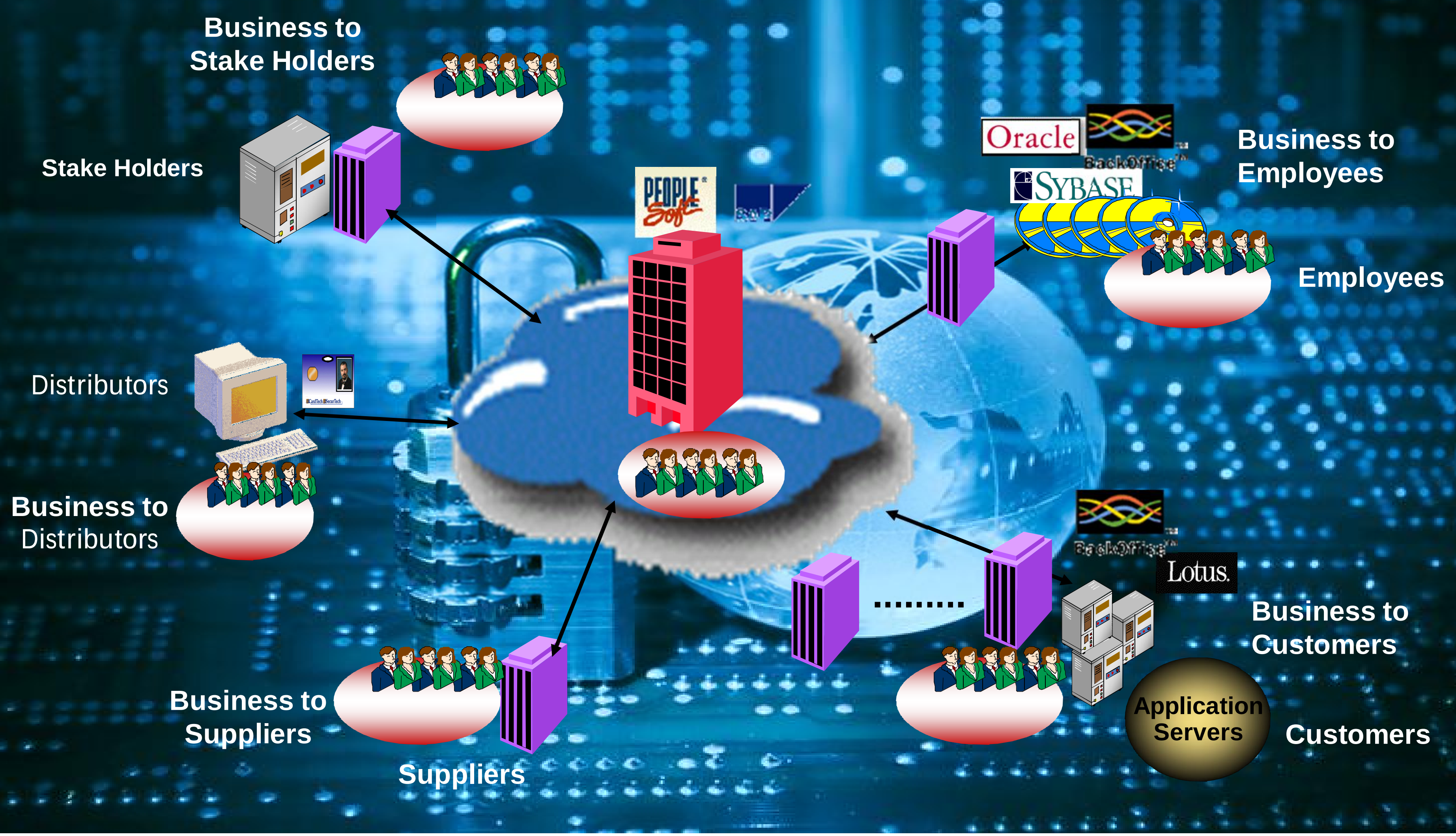
Ramanuj Prasad Singh

Marketing

Pre-Sales

Deployment Resource

Current Enterprise Scenario – Beyond Boundaries..



Business to Stake Holders

Stake Holders

Business to Employees

Employees

Distributors

Business to Distributors

Business to Suppliers

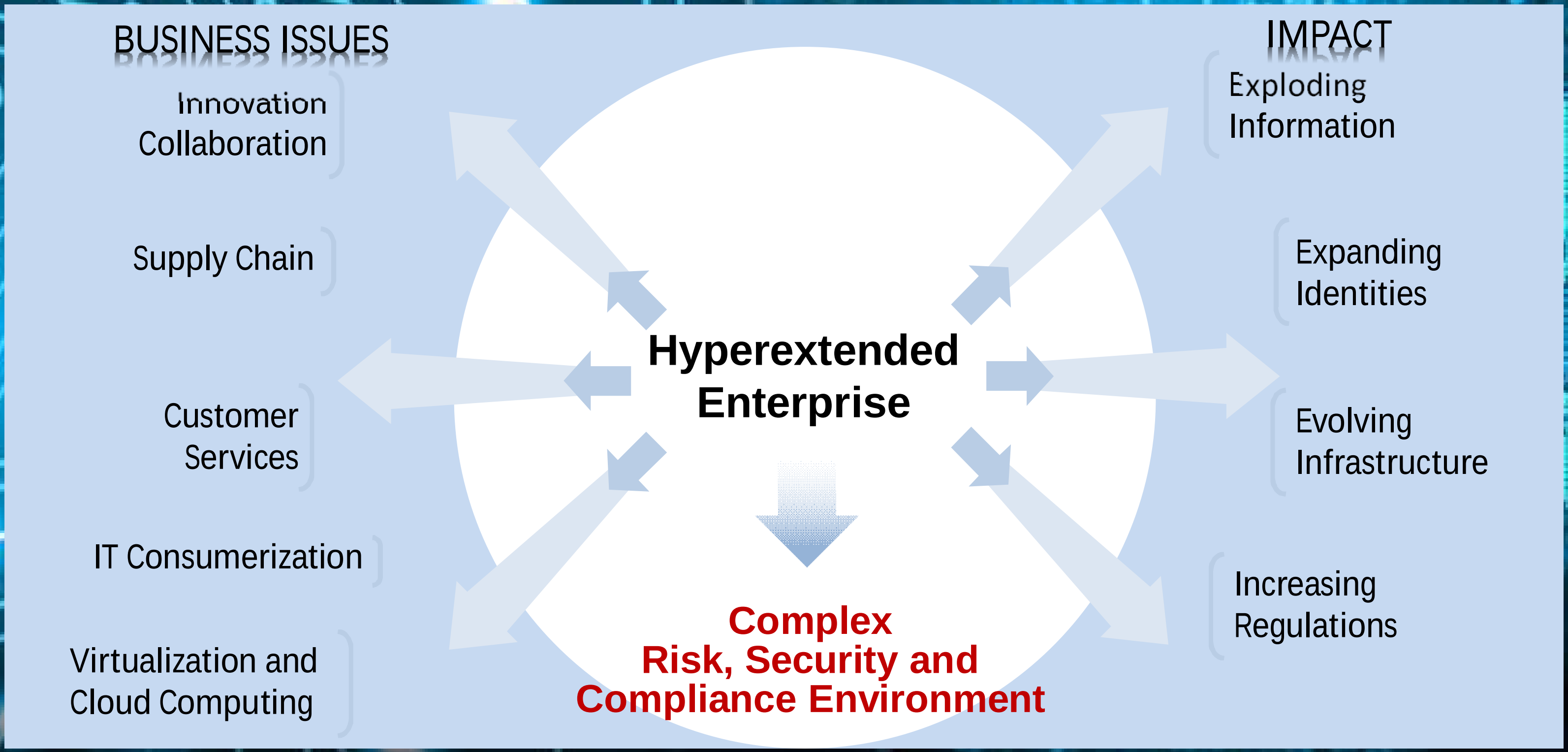
Suppliers

Business to Customers

Application Servers

Customers

The Age of the Hyperextended Enterprise



BUSINESS ISSUES

- Innovation Collaboration
- Supply Chain
- Customer Services
- IT Consumerization
- Virtualization and Cloud Computing

Hyperextended Enterprise

IMPACT

- Exploding Information
- Expanding Identities
- Evolving Infrastructure
- Increasing Regulations

Complex Risk, Security and Compliance Environment

Companies are Opening Up

Tele-Working

Email on PDAs

IP Telephony

Application Sharing

Extranets

Instant Messaging

Connecting branch offices

Mobile Workers

Web Applications

Email with Outsiders

The Customer Environment...

Manageability

Complicated

Complex

Can such complexity deliver a high level of security?

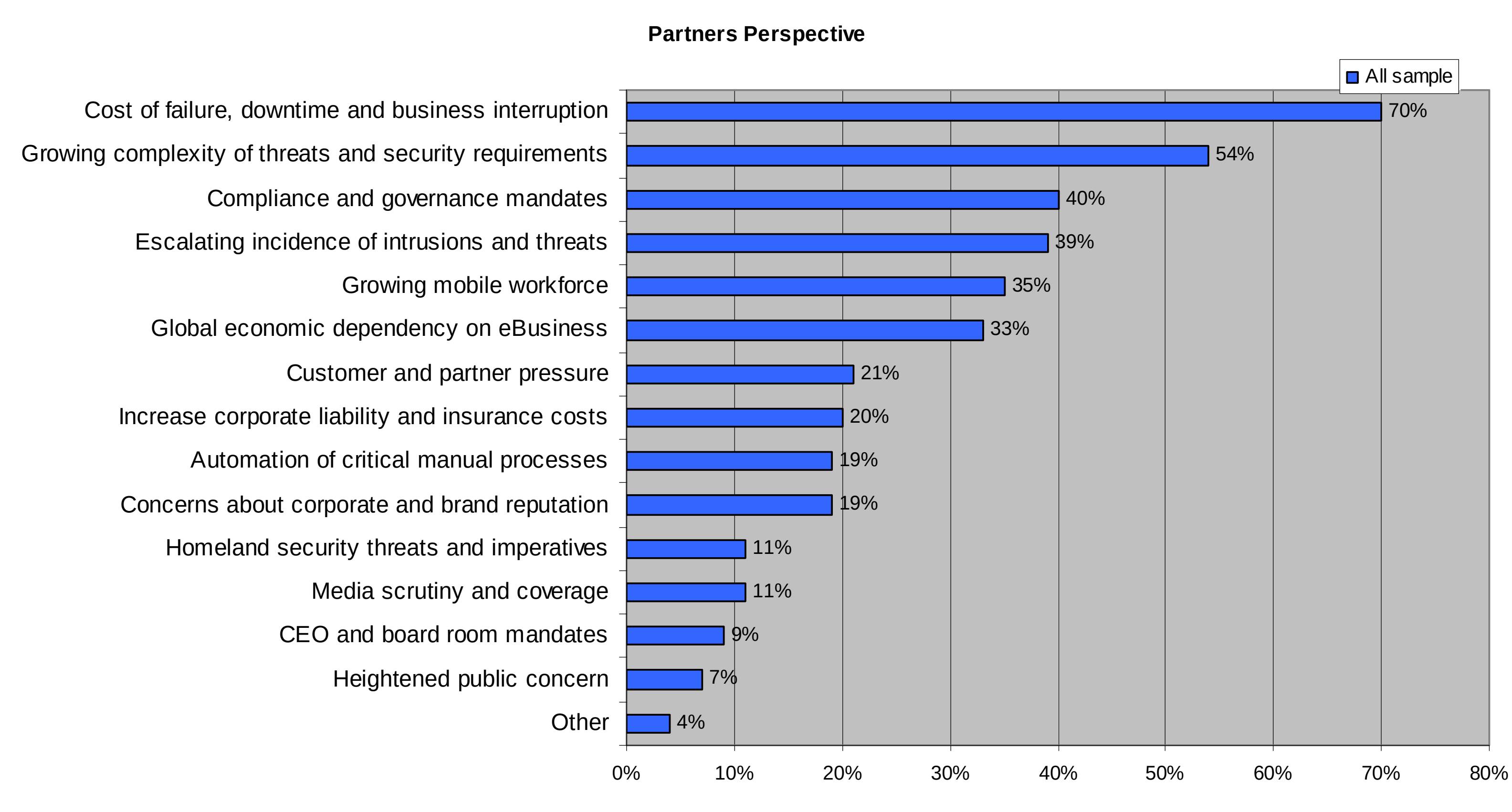
Security needs

Key Operational Challenges

Cost of Failure, Downtime

Growing Complexity of Threats

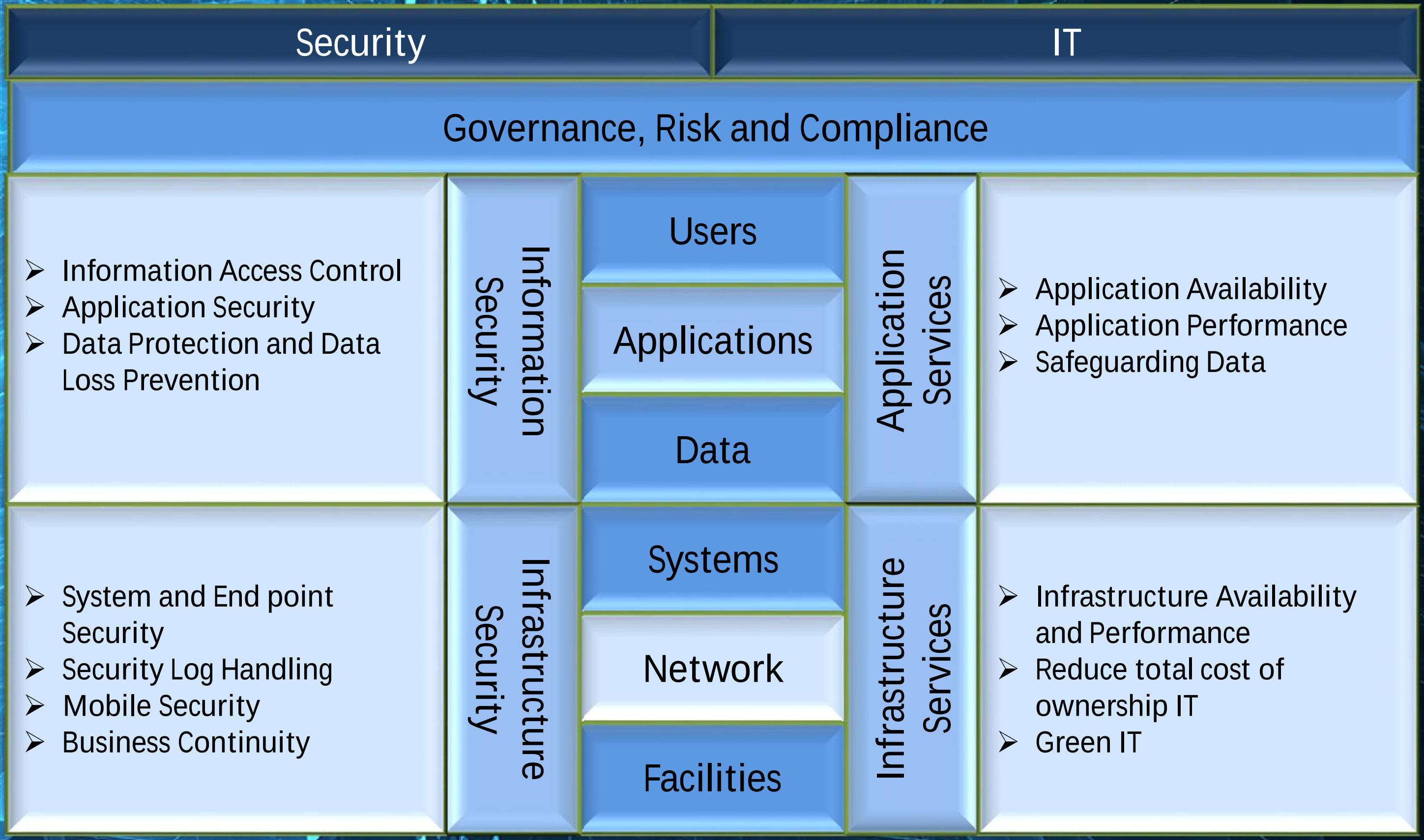
Compliance and Regulatory Mandates



Managing Risk and Threats

No clear visibility to threats and exposures → Inability to adequately address exposures → Slow to respond

IT and Security Challenges



Security

IT

Governance, Risk and Compliance

- Information Access Control
- Application Security
- Data Protection and Data Loss Prevention

Information Security

Users

Applications

Data

Application Services

- Application Availability
- Application Performance
- Safeguarding Data

- System and End point Security
- Security Log Handling
- Mobile Security
- Business Continuity

Infrastructure Security

Systems

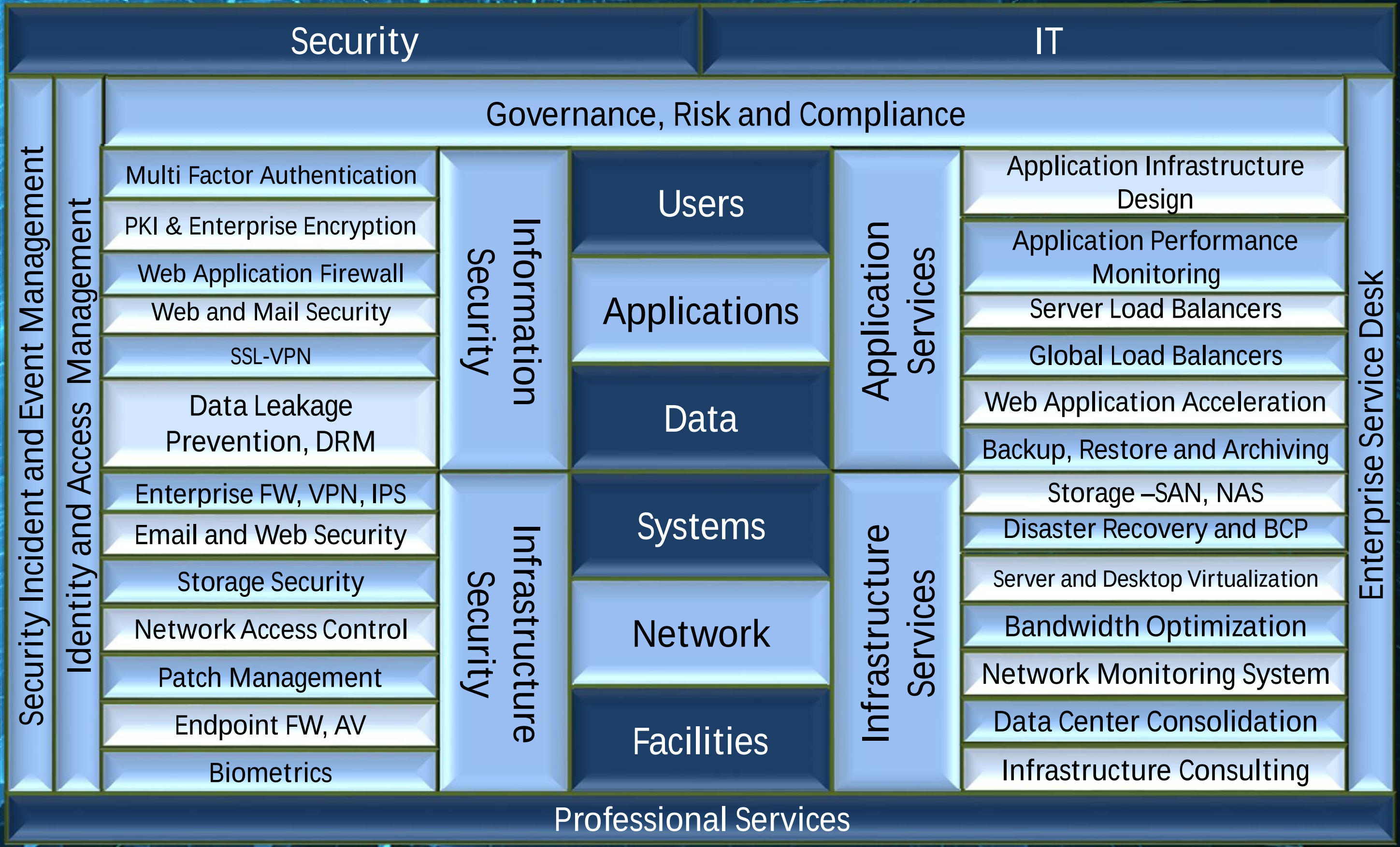
Network

Facilities

Infrastructure Services

- Infrastructure Availability and Performance
- Reduce total cost of ownership IT
- Green IT

Security Solutions



Security

IT

Security Incident and Event Management

Identity and Access Management

Governance, Risk and Compliance

Information Security

- Multi Factor Authentication
- PKI & Enterprise Encryption
- Web Application Firewall
- Web and Mail Security
- SSL-VPN
- Data Leakage Prevention, DRM

Infrastructure Security

- Enterprise FW, VPN, IPS
- Email and Web Security
- Storage Security
- Network Access Control
- Patch Management
- Endpoint FW, AV
- Biometrics

Users

Applications

Data

Systems

Network

Facilities

Application Services

- Application Infrastructure Design
- Application Performance Monitoring
- Server Load Balancers
- Global Load Balancers
- Web Application Acceleration
- Backup, Restore and Archiving

Infrastructure Services

- Storage –SAN, NAS
- Disaster Recovery and BCP
- Server and Desktop Virtualization
- Bandwidth Optimization
- Network Monitoring System
- Data Center Consolidation
- Infrastructure Consulting

Enterprise Service Desk

Professional Services

Targeted OEM

S. No.	Technology	OEM
1	Antivirus, HIPS, Antispam	Symantec, Trend Micro, Mcafee
2	Load Balance (Link & Servers)	F5 Networks, Array Networks, A10, Radware
3	SIEM (Security Incident & Event Management)	Arcsight, RSA, Symantec
4	Two Factor Authentication	RSA, Nexus, Vasco
5	Proxy & Caching Solution	Websense & Bluecoat
6	WAN Optimisation	Riverbed, Silver peak
7	DLP	Websense, RSA, Symantec
8	Web Application Firewall	F5, Palo Alto, Imperva
9	Encryption	Symantec, IBM
10	VA/PT	Nessus, Burp suit

Key Alliances Targeted

Information Security Solutions

f5

Entrust

tufin

ArcSight
An HP Company

symantec.

McAfee

nexus

ORACLE

RSA

TREND MICRO
Securing Your Journey to the Cloud

Blue Coat

Palo Alto Networks Recognized as a Leader in the Gartner Magic Quadrant for Enterprise Network Firewalls
VIEW REPORT
Gartner

radware

OPTENET

riverbed
Think fast.

websense
ESSENTIAL INFORMATION PROTECTION

Allot
communications

Our Strength- ISS Training & Certification Pool

Security Training/Certifications

- ✓CISSP
- ✓CISM
- ✓ITIL V3
- ✓ISO 27001
- ✓PMI
- ✓Checkpoint
- ✓Fortinet
- ✓Symantec
- ✓McAfee
- ✓Juniper
- ✓RSA
- ✓Arc Sight
- ✓Websense
- ✓Bluecoat
- ✓F5
- ✓Radware
- ✓Cisco

IT Training/Certifications

- ✓Microsoft Certified System Administrator
- ✓Microsoft Certified System Engineer
- ✓Sun Certified System Administrator
- ✓Sun Certified Network Administrator
- ✓Sun Certified System Administrator for Cluster
- ✓Linux Certified System Administrator
- ✓Linux Certified Network Administrator
- ✓VERITAS Storage Foundation Administrator
- ✓EMC Certified Storage Consultants
- ✓VMware Certified Professionals
- ✓NetApp Certified Data Management Administrator
- ✓NetApp Accredited Storage Architect Professionals
- ✓NetApp Accredited Sales Professionals

13

Few Important Technologies

- Two Factor
- SIEM
- WAF

What is Two-Factor Authentication?

Two-Factor Authentication:

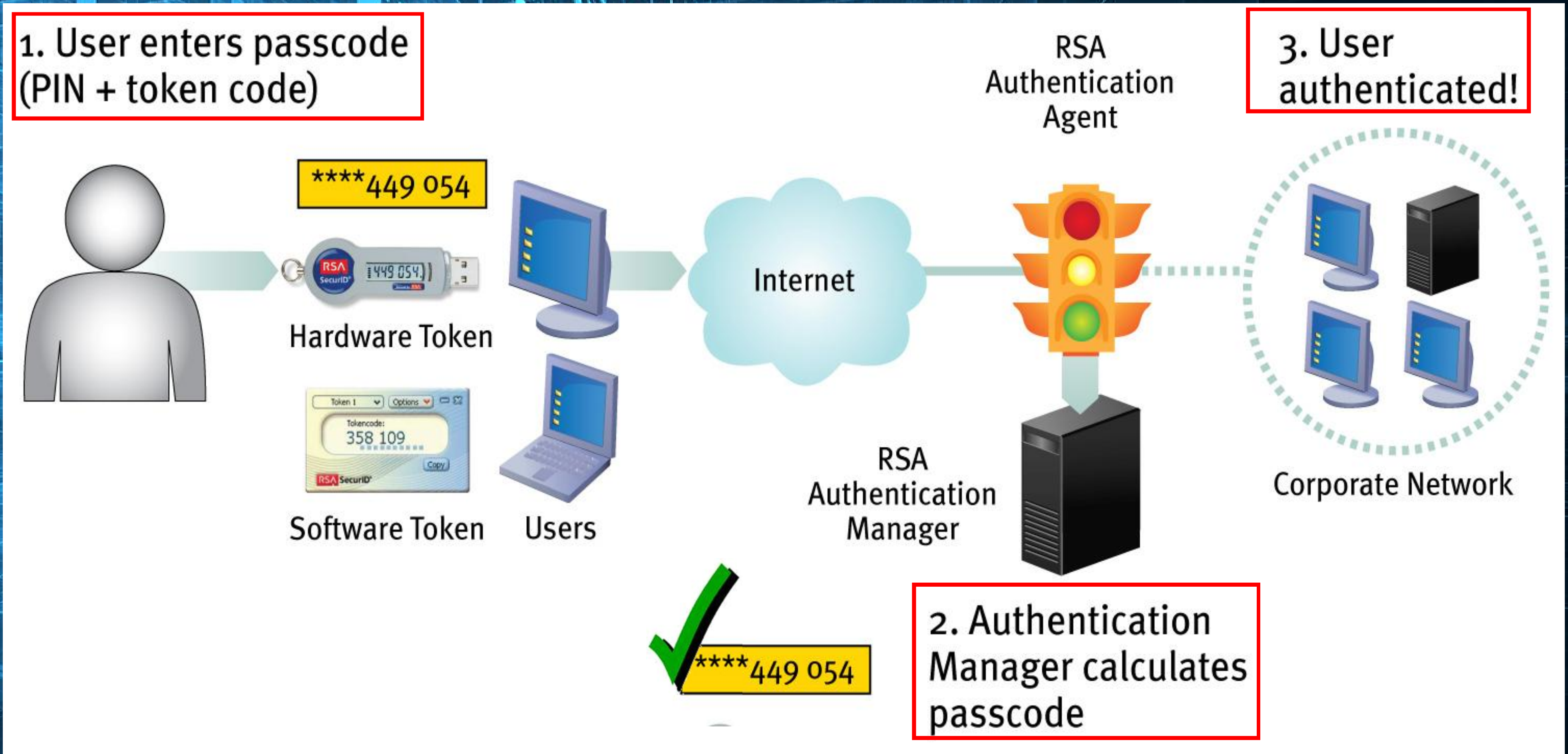
“The act of identifying an individual by using any combination of something they know, something they have or something they are.”

“Something you know” = PIN, password, life question

“Something you have” = Token, Smartcard, Trusted Device

“Something you are” = Biometrics (fingerprint, retinal scan, etc)

How does It works?

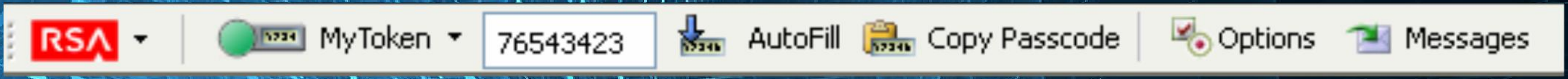


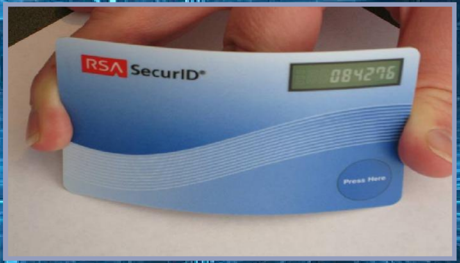
1. User enters passcode (PIN + token code)

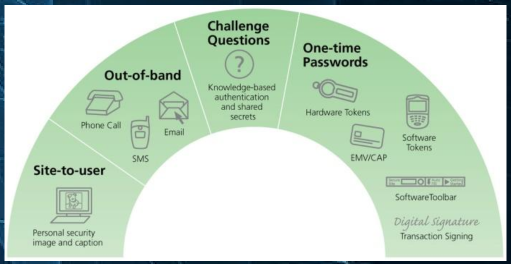
2. Authentication Manager calculates passcode

3. User authenticated!

Two Factor Authentication Solution







Site-to-user

Personal security image and caption

Out-of-band

Phone Call

SMS

Email

Challenge Questions

Knowledge-based authentication and shared secrets

One-time Passwords

Hardware Tokens

EMV/CAP

Software Tokens

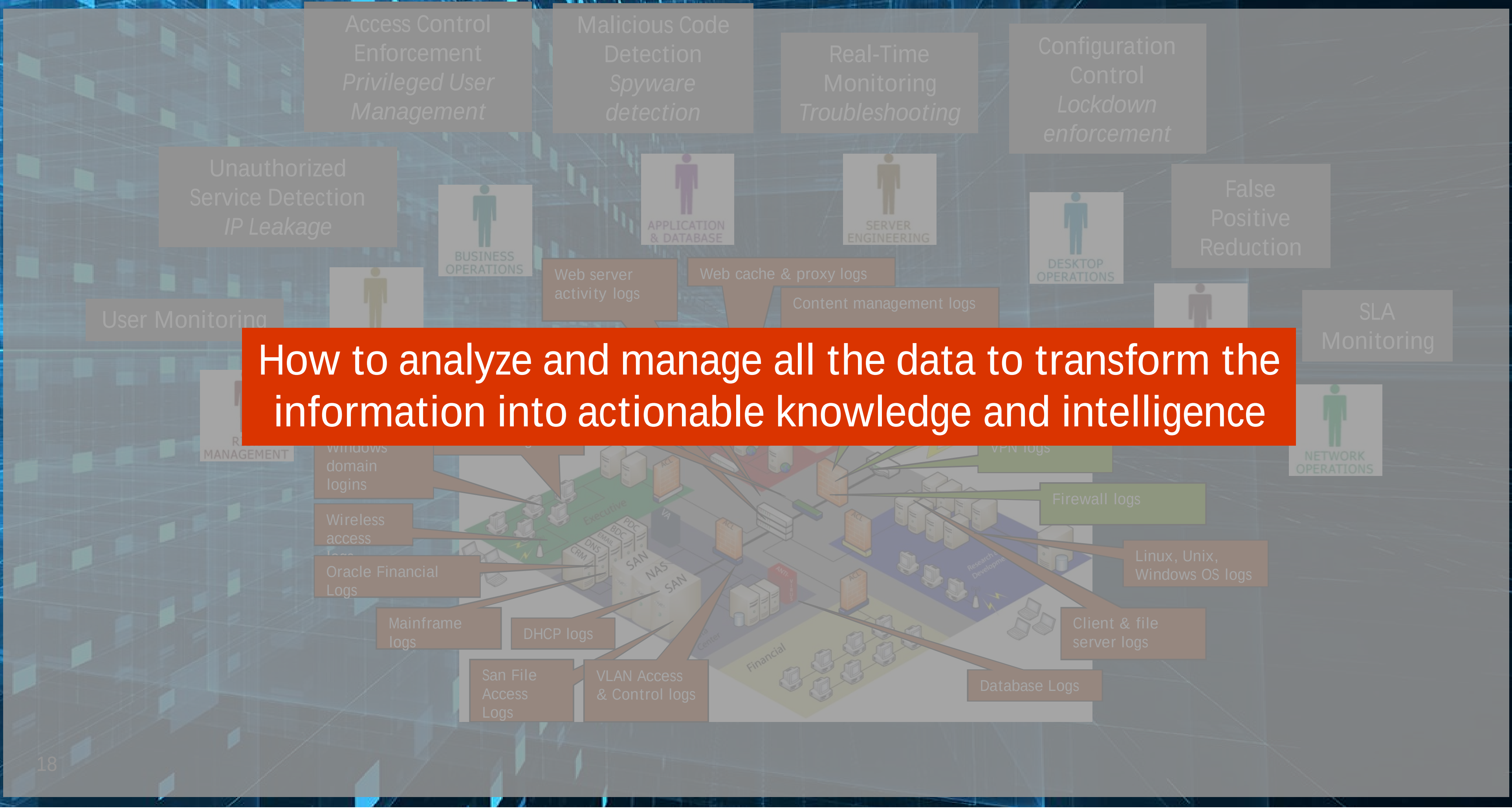
SoftwareToolbar

Digital Signature

Transaction Signing

SIEM-The Enterprise Today

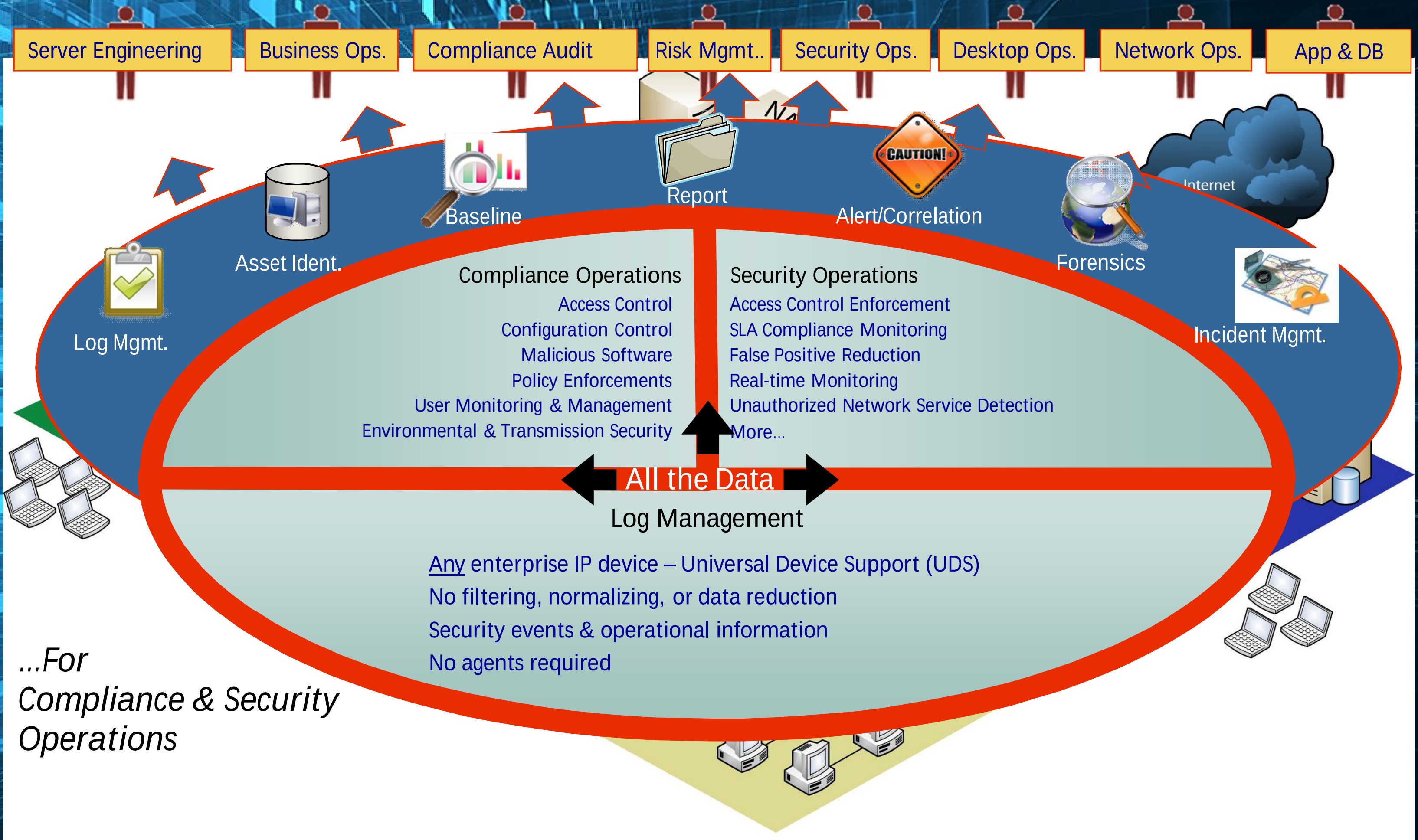
Mountains of data, many stakeholders



How to analyze and manage all the data to transform the information into actionable knowledge and intelligence

Solution: SIEM

An Information Management Platform…



Server Engineering

Business Ops.

Compliance Audit

Risk Mgmt..

Security Ops.

Desktop Ops.

Network Ops.

App & DB

Log Mgmt.

Asset Ident.

Baseline

Report

Alert/Correlation

Forensics

Incident Mgmt.

Compliance Operations

- Access Control
- Configuration Control
- Malicious Software
- Policy Enforcements
- User Monitoring & Management
- Environmental & Transmission Security

Security Operations

- Access Control Enforcement
- SLA Compliance Monitoring
- False Positive Reduction
- Real-time Monitoring
- Unauthorized Network Service Detection
- More…

All the Data

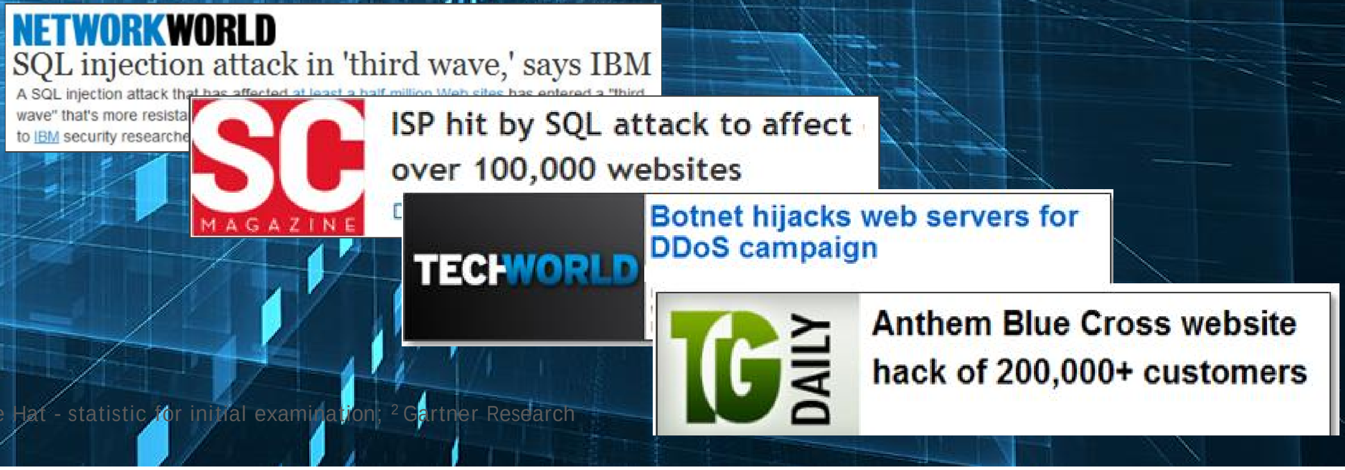
Log Management

- Any enterprise IP device – Universal Device Support (UDS)
- No filtering, normalizing, or data reduction
- Security events & operational information
- No agents required

…For Compliance & Security Operations

Why Protect Web Applications?

- 82% of Web applications have vulnerabilities[1]
- 75% of all Internet attacks target applications[2]
- Attacks are getting more sophisticated
  - Increasing in scale due to automation, Google hacking
  - Growing threats: L7 DDoS, CSRF, botnets, massive SQLi, scraping



SQL injection attack in 'third wave,' says IBM

A SQL injection attack that has affected at least a half million Web sites has entered a "third wave" that's more resista to IBM security researche

ISP hit by SQL attack to affect over 100,000 websites

Botnet hijacks web servers for DDoS campaign

Anthem Blue Cross website hack of 200,000+ customers

[1] White Hat - statistic for initial examination; [2] Gartner Research

Web Application Firewall - WAF

Challenges with Legacy Security Solutions

- Network Firewalls
  - Blindly allow HTTP/S Web traffic
- IPS/IDS
  - Signature matching only, not application aware
  - Cannot protect from zero-day attacks
  - No protection for encrypted traffic
  - Non deterministic protection
  - Cannot “normalize” traffic to detect attacks

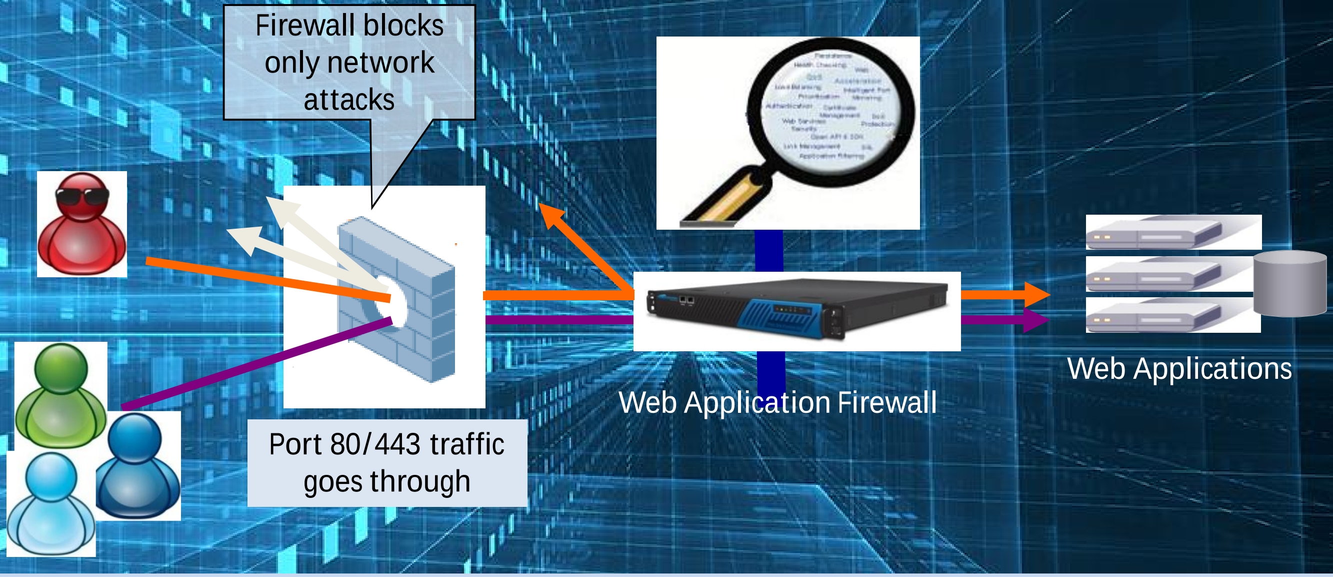
What is Missing?

More insight and control into application structure:

URLs, cookies, headers, FORMs, Session, SOAP actions, XML elements …

Application Threat	IPS/Network Firewall	Application Firewall
Cookie poisoning	Well known signatures only	✓
Hidden field manipulation	Well known signatures only	✓
Cross Site scripting	Well known signatures only	✓
Injection Attacks	None	✓
Stealth Commanding	None	✓
Parameter Tampering	None	✓
Buffer overflow	None	✓
Google Hacks	None	✓
Forceful Browsing	None	✓
Identity Theft	None	✓
Application DoS	None	✓
Data Theft	None	✓

The solution: Layer 7 security



Firewall blocks only network attacks

Port 80/443 traffic goes through

Web Application Firewall

Web Applications

The solution: Web Application Firewall

✓ Understands web traffic

✓ Layer 4 and Layer 7 load balancing for Web servers

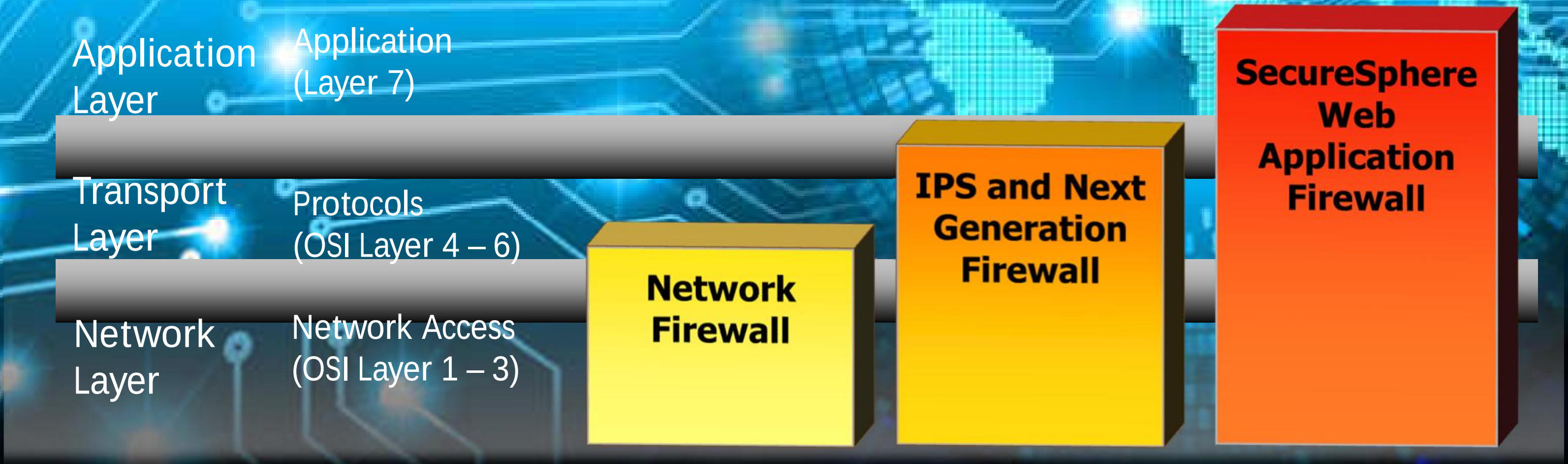
✓ Accelerates application delivery

✓ Protects against common web attacks

✓ Mitigates broken access control

A New Type of Security is Needed

- Traditional firewalls only detect network attacks
  - Only inspect IP address, port/service number
- IPS and NG firewalls only detect known signatures
  - No application understanding; high rate of false positives/negatives
  - No user/session tracking; No protection of SSL traffic
- Web Application Firewalls alone detect application attacks!



Application Layer

Application (Layer 7)

Transport Layer

Protocols (OSI Layer 4 – 6)

Network Layer

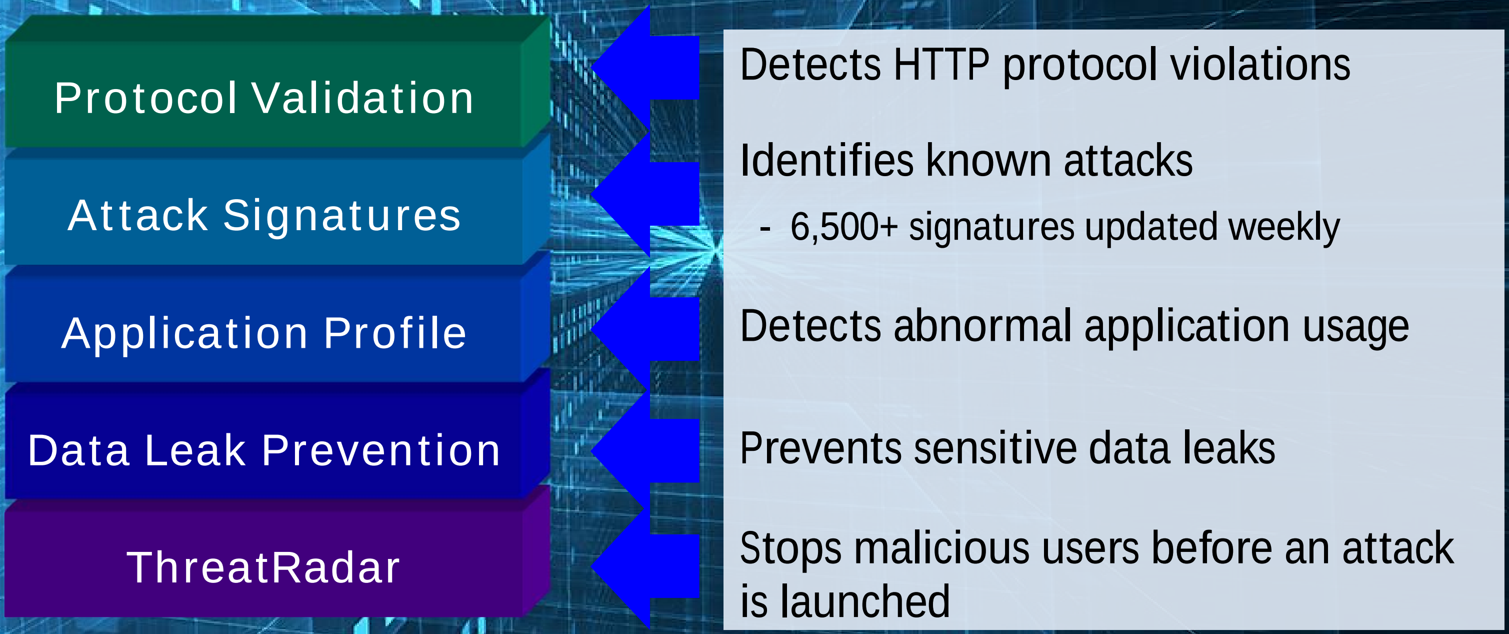
Network Access (OSI Layer 1 – 3)

Network Firewall

IPS and Next Generation Firewall

SecureSphere Web Application Firewall

Multiple Layers of Protection



Protocol Validation

Attack Signatures

Application Profile

Data Leak Prevention

ThreatRadar

Detects HTTP protocol violations

Identifies known attacks

- 6,500+ signatures updated weekly

Detects abnormal application usage

Prevents sensitive data leaks

Stops malicious users before an attack is launched

Let’s begin!