Security-as-an-Enabler
The new security "delivery model"

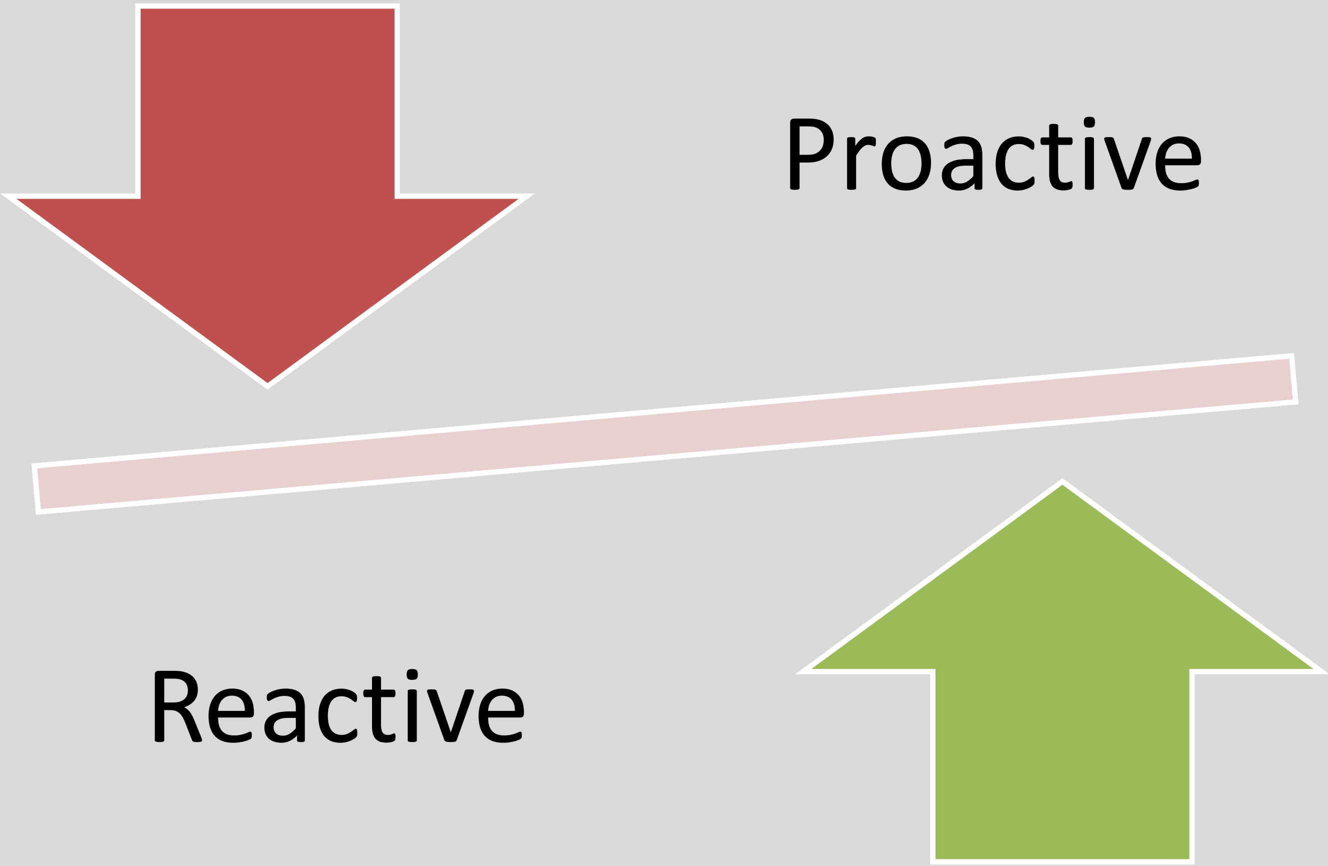
Infocom Security 2015

Andreas Athanasoulias, CISM, CISSP
Information Security Officer & Security Consultant

The fragile equilibrium of Information Security (1)

- Am I secure **enough**?
- Is there 100% security?
- Securing business or “securing security”?
- Balance between:
  - Needs (business, user)
    - Working efficiently
    - Achieving goals
  - Security & Protection
    - Operations
    - Assets
    - Goals & Expectations
- Chasing 100% is like chasing Chimera.
- Business Enabler ≠ Security Paranoia

The fragile equilibrium of Information Security (2)



Proactive

Reactive

Approaching Information Security (1)

- Awareness of Information Security
  - “Security says no”
  - “Security is a regulatory requirement”
  - “I am not the target of a cyber attack”
- “Selling” Information Security: Fear oriented, not business oriented.
  - Examples:
    - Lose confidential data
    - Hackers
    - Industrial Espionage
    - Fraud

Approaching Information Security (2)

DATA LOSS EXPERIENCED (EXTERNAL THREATS)
27% OF ORGANIZATIONS HAVE LOST SENSITIVE BUSINESS DATA DUE TO EXTERNAL
THREATS IN THE LAST 12 MONTHS; DATA LOSS FROM SOFTWARE VULNERABILITIES HAS
FALLEN SHARPLY BUT IS RISING FOR SEVERAL OTHER THREATS
Vulnerabilities / flaws in existing software
Accidental leaks / sharing of data by staff
Loss /theft of mo
Intentional leaks
Information leaked /inappropriate
Secu
Did data l
7%
13%
16%
7%
14%
7%
THE MOST DANGEROUS INSIDERS
ADMINISTER & MANAGE INFRASTRUCTURE
55%
Privileged Users
Privileged Users incl
System Administ
Network Ad
Linux/Un
Dom
YOU HAVE
BEEN HACKED
12%
Forensics
10%
Technical support
8%
Compliance Regulatory

Investing in Security:
Why it 's hard to "convince" (1)

- Regular investment
  - Return on Investment (ROI)
  - Example:

Alice would like to run a lemonade business for summer. She needs money for setting up the business. Bob gives her 200€ to start her business. In return, Alice agrees to give Bob 50% of the benefits.

At the end of summer, Alice made 1000€ of benefits. Bob gets 500€. Bob's Return on Investment is calculated as follow:

$$ROI = \frac{500 \;\; - 200}{200} = 150\%$$

Reference "Return on Security Investment" ENISA 2012

Investing in Security: Why it ‘s hard to “convince” (2)

- Security investment:
  - Does not offer **tangible** revenue (return on investment).
  - Investing in security ~ Buying insurance
  - The more we buy, the lack of security costs less.
- Return on Security Investment (ROSI)

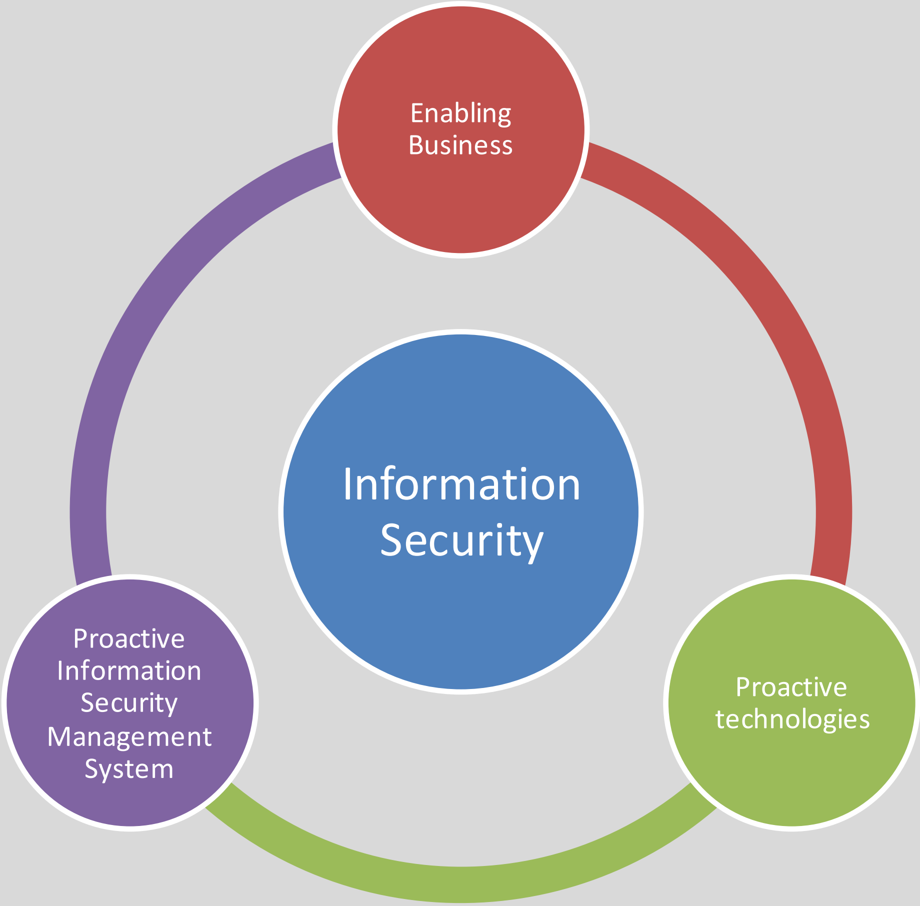
$$ROSI = \frac{ALE\ - mALE\ - Cost\ of\ the\ security\ solution}{Cost\ of\ the\ security\ solution}$$

Where:

$$Annual\ Loss\ Exectancy\ (ALE) = Annual\ Rate\ of\ Occurence\ (ARO) * Single\ Loss\ Expectancy\ (SLE)$$

Reference “Return on Security Investment” ENISA 2012

Our Approach (1)



Enabling Business

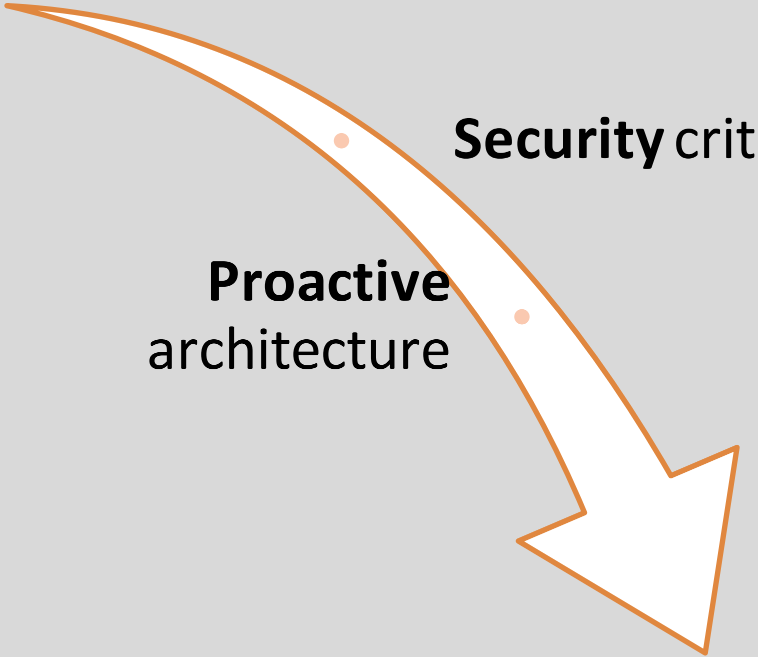
Information Security

Proactive Information Security Management System

Proactive technologies

uni.systems

Our Approach (2)



Business needs

Security criteria

Proactive architecture

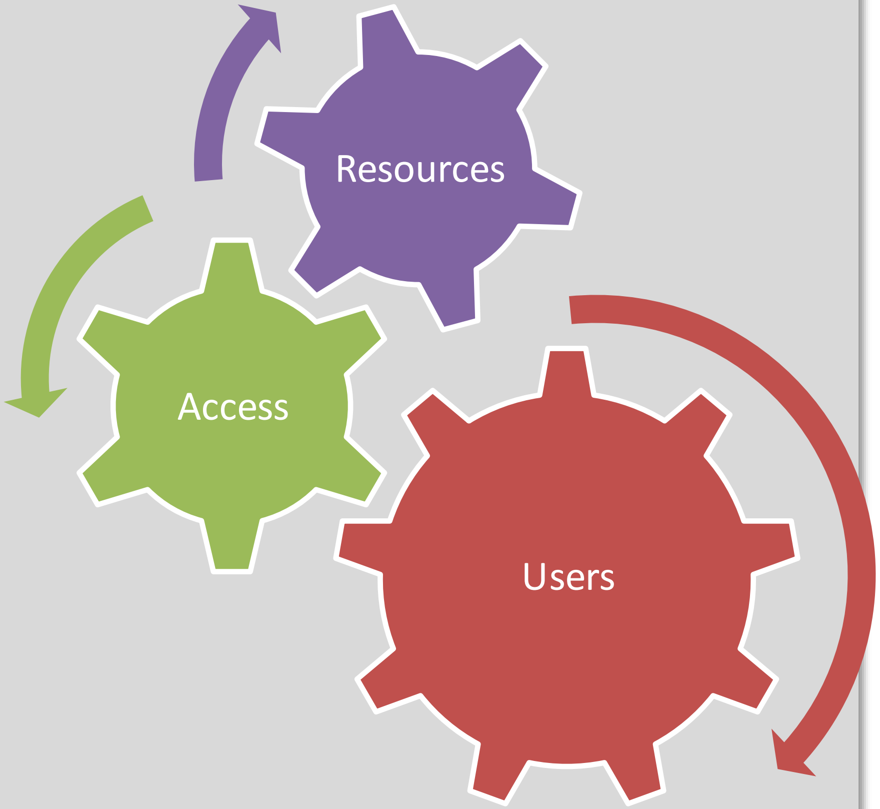
Security as an Enabler

Modern Standards address Security as an "Enabler"

- ISO 27001:2013 (ISMS)
  - "It is important that the **information security management system** is part of and **integrated** with the organization's **processes** and overall **management** structure [..]. It is expected that an information security management system implementation will **be scaled in accordance with the needs of the organization**."
- Cobit Framework (ISACA)
  - COBIT is an IT governance framework and supporting toolset that allows managers to bridge the **gap** between control requirements, technical issues and business risks.
- Solvency II
  - Pillar 2: Governance & Supervision
  - Effective risk management system.

Our approach:
Uni Systems Case Study

- Our approach in action
- It' all about **users** and **access** to company **resources.**
- Secure access **of** users **to** resources.
- Users may be internal or external.
  - Insider threat
  - External threats (e.g. remote support)



User & Access & Resources

User

- Identity
- Location
- Workspaces (e.g. Mobility)

Access

- Identification
- Authentication
- Authorization

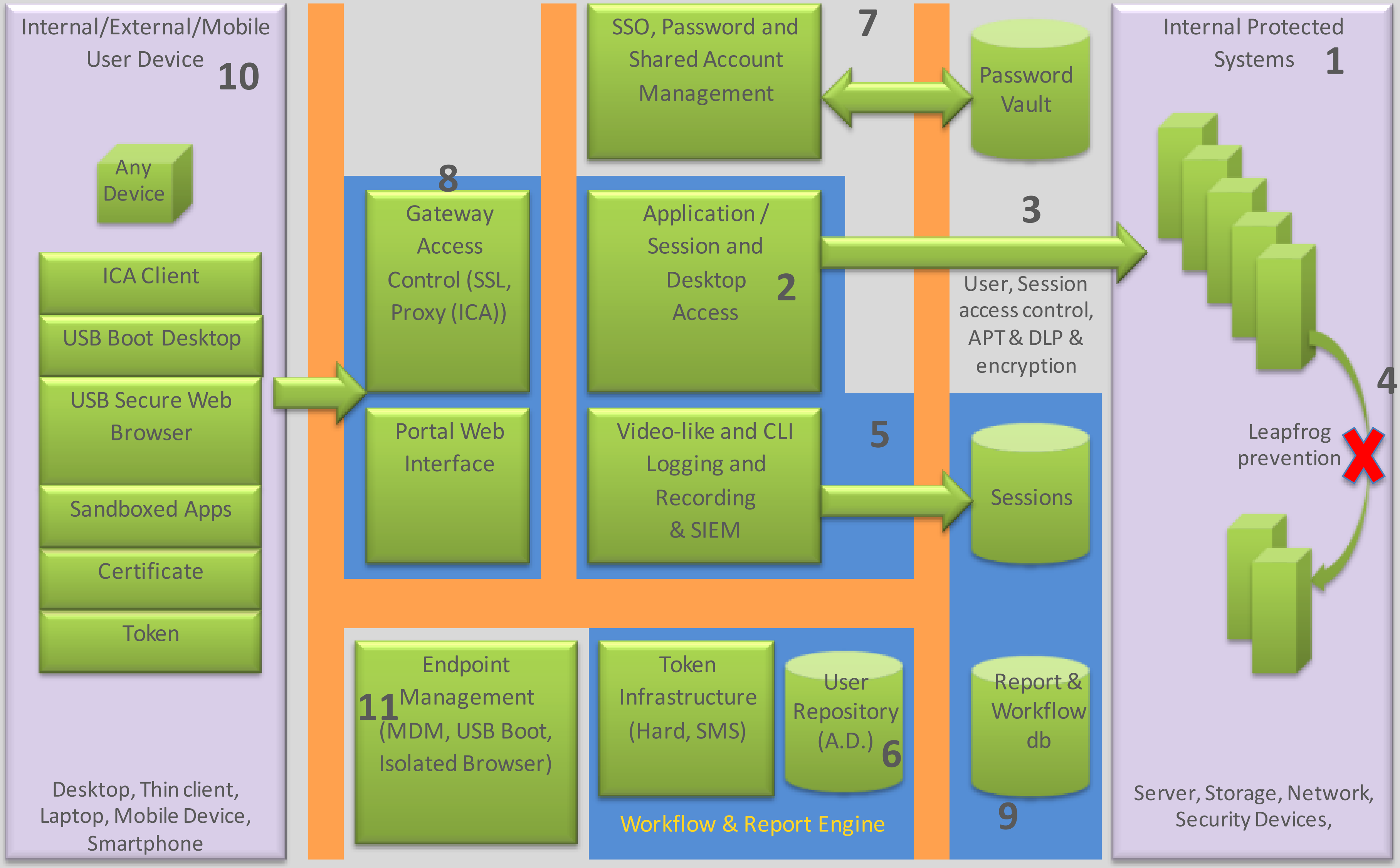
Resources

- Shares
- Privileged accounts
- Systems & Services

Which are the risks?

- Insider threat
- Exposing internal, trusted resources to external parties
- Privileged accounts
  - Shared?
  - Leapfrogging?
  - Limitations of network access controls? (e.g. firewalls)
- Multiple - shared accounts & identities
- Non-conformities (regulations)
- Advanced persistent threats

Solution Architecture



User Zone

Secure Access Component Zone

Trusted and Protected Zone

Internal/External/Mobile User Device 10

Any Device

ICA Client

USB Boot Desktop

USB Secure Web Browser

Sandboxed Apps

Certificate

Token

Desktop, Thin client, Laptop, Mobile Device, Smartphone

8 Gateway Access Control (SSL, Proxy (ICA))

Portal Web Interface

SSO, Password and Shared Account Management 7

Password Vault

Application / Session and Desktop Access 2

3 User, Session access control, APT & DLP & encryption

Video-like and CLI Logging and Recording & SIEM 5

Sessions

11 Endpoint Management (MDM, USB Boot, Isolated Browser)

Token Infrastructure (Hard, SMS)

User Repository (A.D.) 6

Workflow & Report Engine

Report & Workflow db 9

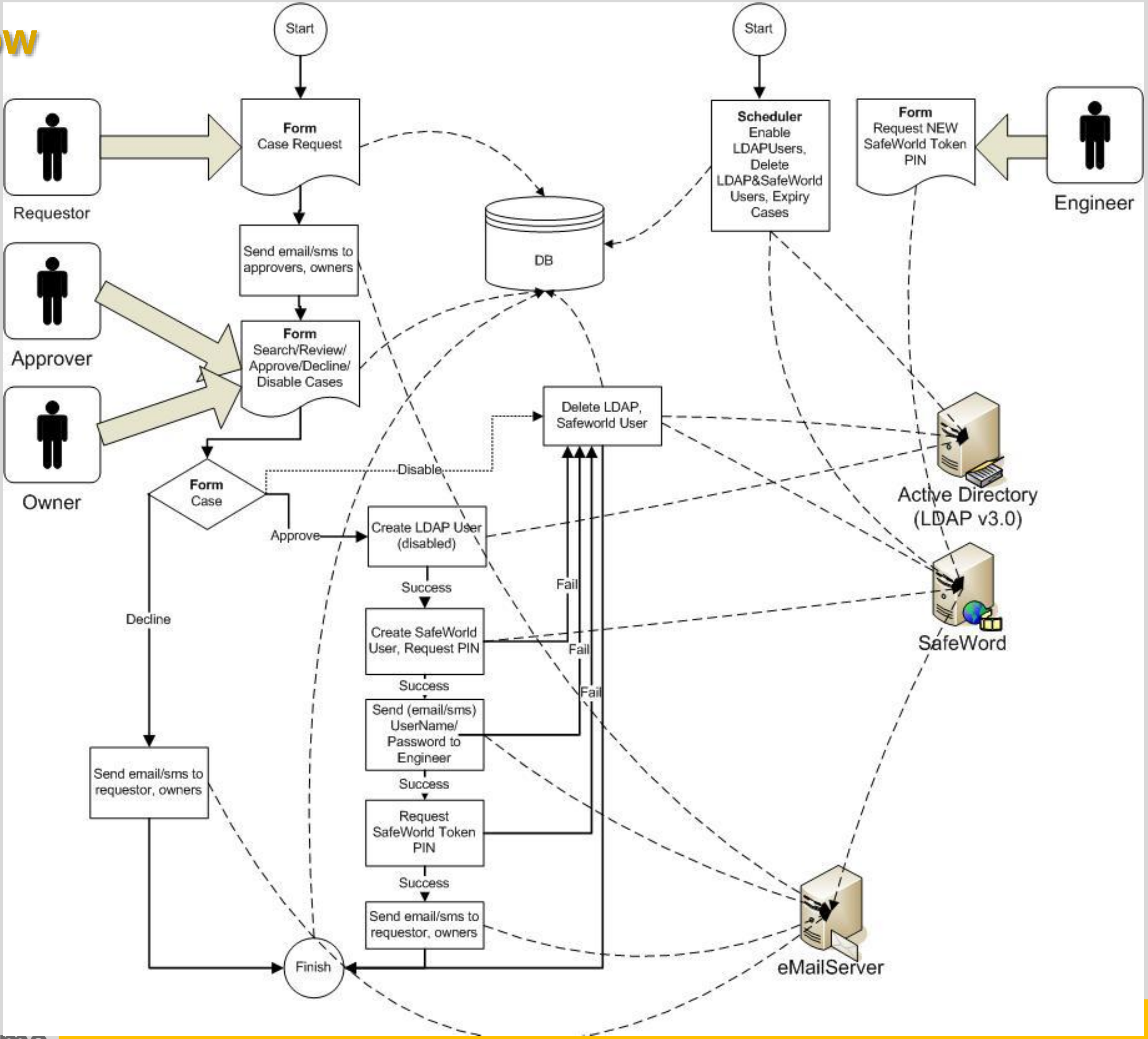
Internal Protected Systems 1

4 Leapfrog prevention

Server, Storage, Network, Security Devices,

uni.systems

Workflow


Start
Form
Case Request
Requestor
Send email/sms to approvers, owners
Approver
Form
Search/Review/ Approve/Decline/ Disable Cases
Owner
Form
Case
Disable
Approve
Decline
DB
Start
Scheduler
Enable LDAPUsers, Delete LDAP&SafeWorld Users, Expiry Cases
Form
Request NEW SafeWorld Token PIN
Engineer
Delete LDAP, Safeworld User
Create LDAP User (disabled)
Success
Create SafeWorld User, Request PIN
Fail
Fail
Fail
Success
Send (email/sms) UserName/ Password to Engineer
Success
Request SafeWorld Token PIN
Success
Send email/sms to requestor, owners
Send email/sms to requestor, owners
Finish
Active Directory (LDAP v3.0)
SafeWord
eMailServer

Business Scenarios

- Privileged User Access Management
  - Perpetual - On-demand
- Remote Access Scenario
  - Support engineers
- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Data Loss Prevention
  - Trusted & protected zone
- Compliance monitoring on critical infrastructure:
  - Session Recording
  - Security Incident & Event Management (SIEM)
- Enforcing compliance & governance
  - Regulatory mandates (e.g. PCI)

What is being offered…

- … through a secure architecture.

- Workspaces
  - Mobile | Virtual | Secure
- Risk Reduction
  - Access Provisioning & De-provisioning Workflow
  - Control on data. Prevention on leakage.
  - Security Incidents Recorded. Guaranteed Audit Trail.
- Costs Reduction
  - Access solution for both internal & external users
- Confidentiality & Availability

Technologies offering both proactive & reactive approach

Proactive

- Risk Assessment
- Two factor authentication
- Network & Application Access Controls
- Network & Application Firewalls
- Command white/blacklisting
- Data Loss Prevention
- Advanced Persistent Threat Detection

Reactive

- Session recording
- Security Information & Event Management
- Encryption
- Advanced Persistent Threat Remediation

Security as an Enabler - Conclusions
Proactive or… Pro-acting?

- Security must be proactive.
  - When designing solutions.
  - But…
- What about pro-acting?
  - Technology and needs drive IT
  - Security is reactive; criteria are set & met when technology has dominated the market
  - What about smartphones and tablets? Modern workplaces? Internet of Things?
  - Virtualization has practically changed the classic model of "perimeter security"
  - Cloud service changed the landscape of how users consume services
- "Every business need should be injected with security doses"!

uni.systems

Thank you

Andreas Athanasoulias, CISM, CISSP
Information Security Officer & Security Consultant