Entrust®

Securing the Internet

Enhanced Internet Security

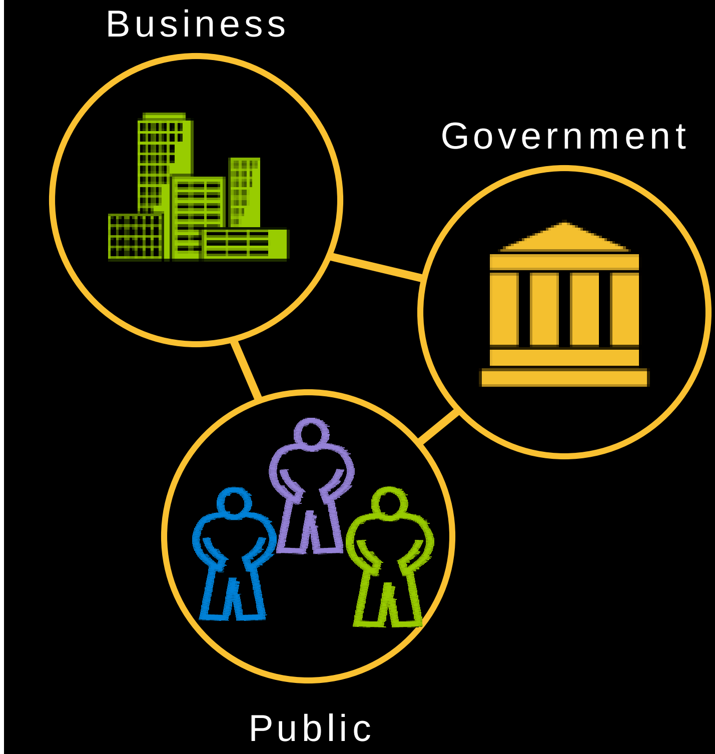
Brian O’Higgins

CTO

Agenda

- Internet Security Landscape
- Portals, Enterprise, Web Services
- Trust and Identity Management
- Interoperability

Governments and Businesses Have Moved On-Line...



98% of respondents have WWW sites...

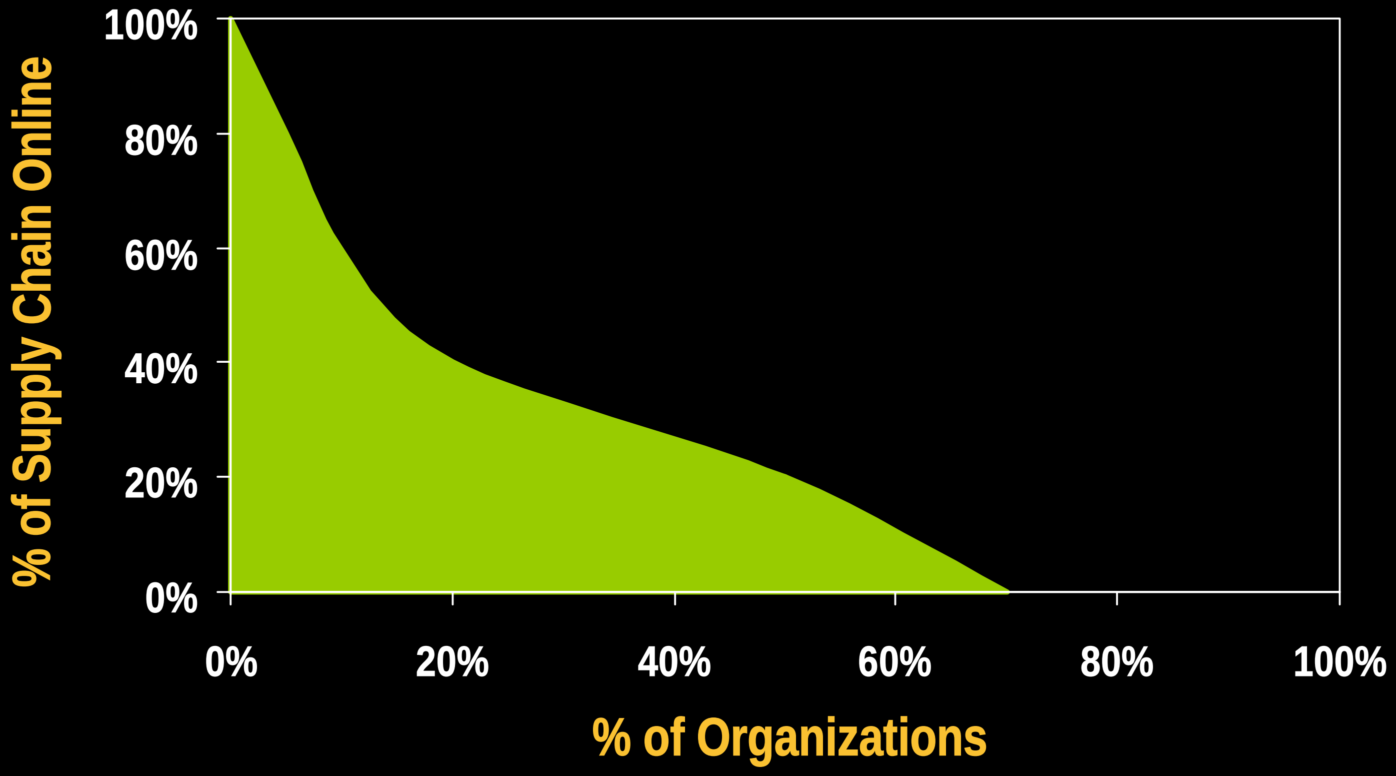
52% conduct electronic commerce on their sites

--- FBI / CSI, 2002

8% of B2B commerce is now done on the Web

--- Forrester, 2002

. . . Only Initial Steps have been taken with Critical Applications



Source: Gartner, April 2002

E-Government Scorecard

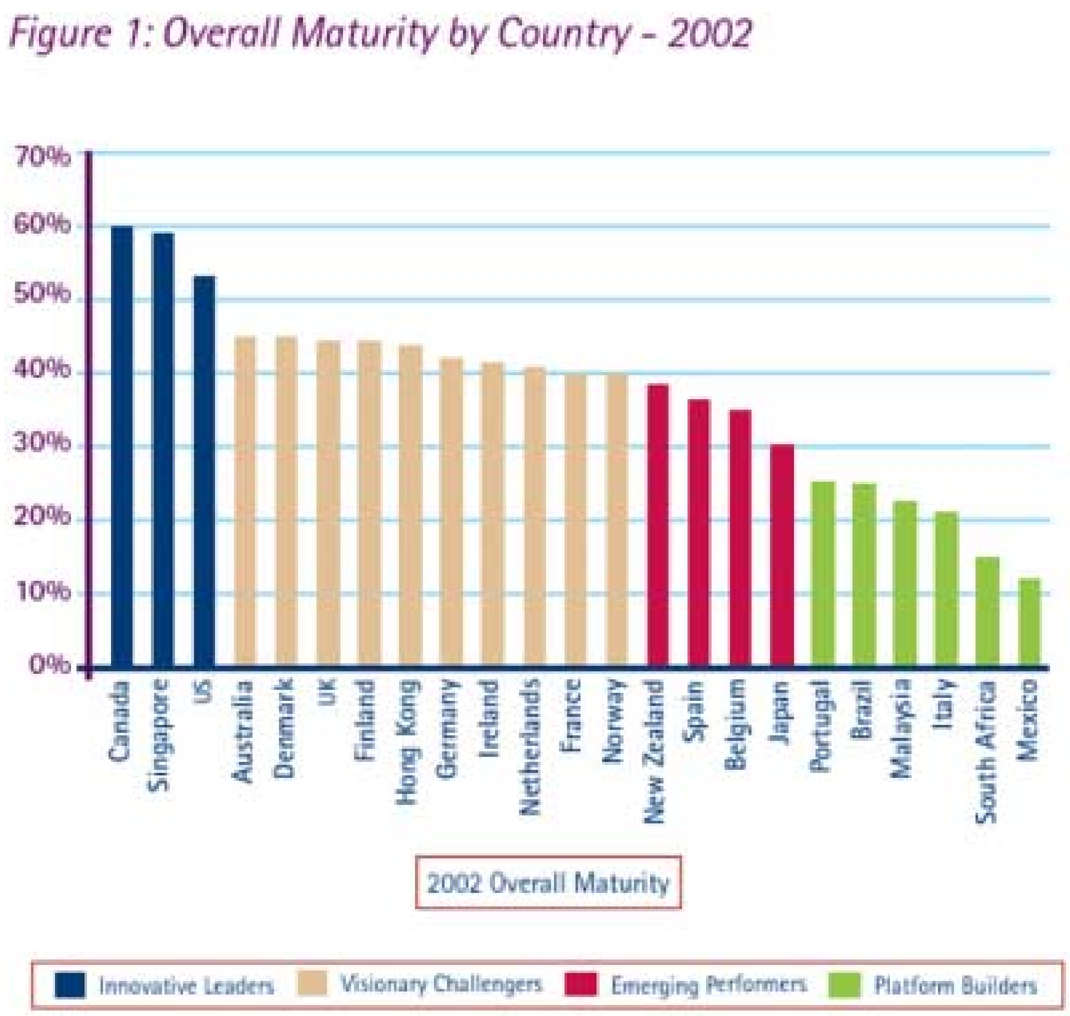


Figure 1: Overall Maturity by Country - 2002

Leaders: High number of mature services

Visionary Challengers: Large breadth of services

Emerging Performers: Beginnings of solid base

Platform Builders: Low levels of services

Source: Accenture
March 2002

Gained administrative control of computers in

75 % of tests

NO global laws

64 %
Avg. l
$2

MS Windows

413
military network

95 %
of Pentagon's
unications
ied on
mercial
works

Issues are escalating

Government and financial services are targets

Threat increase = *f* (known vulnerabilities + smart hackers+ script kiddies)

85
of resp
had b
— F

00
ate
cidents
00

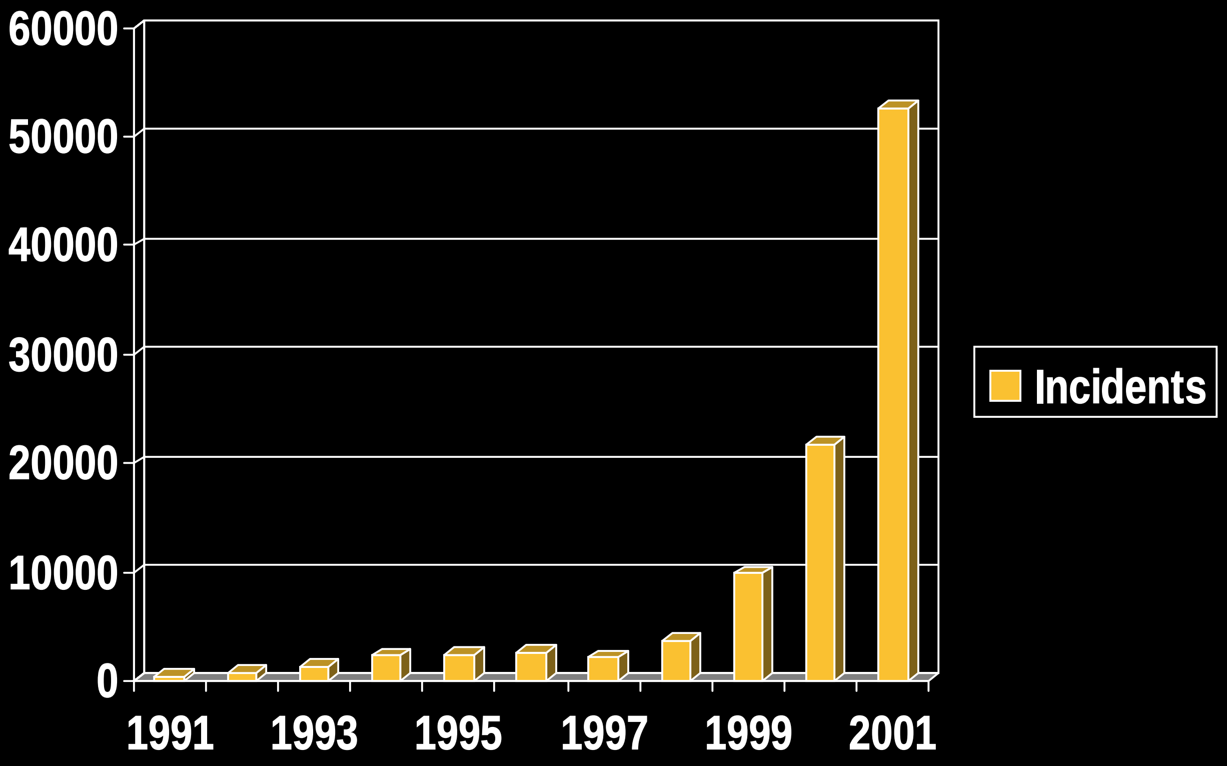
of breaches are
internal

group declares
Cyber-Jihad
against U.S

computer systems

3 %
Rate security
"Very Important"

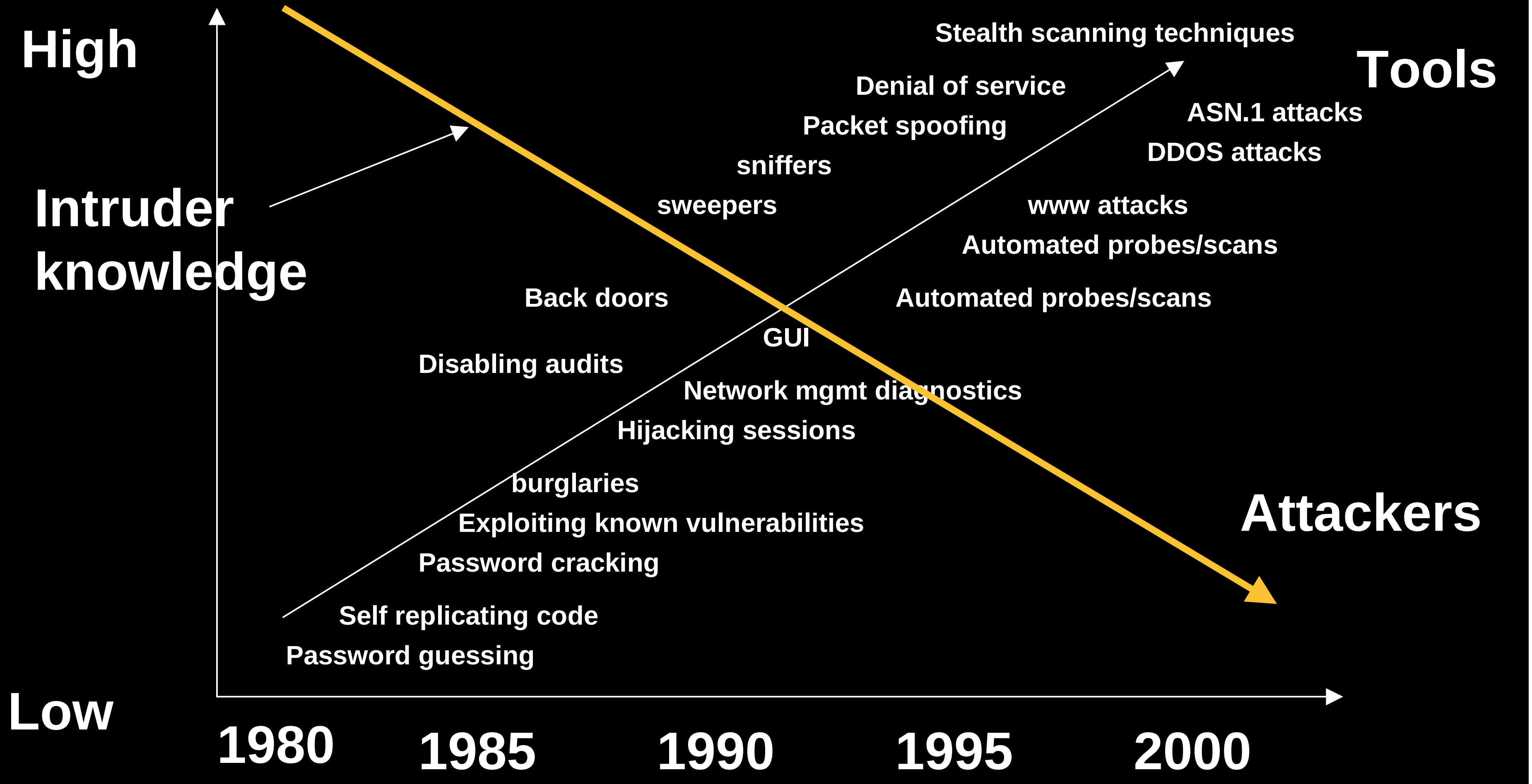
CERT/CC Number of Incidents Reported



2002 Q1: 26,000 incidents

www.cert.org/stats

Attack Sophistication



High

Stealth scanning techniques

Tools

Denial of service

ASN.1 attacks

Packet spoofing

DDOS attacks

sniffers

Intruder knowledge

sweepers

www attacks

Automated probes/scans

Back doors

Automated probes/scans

GUI

Disabling audits

Network mgmt diagnostics

Hijacking sessions

burglaries

Attackers

Exploiting known vulnerabilities

Password cracking

Self replicating code

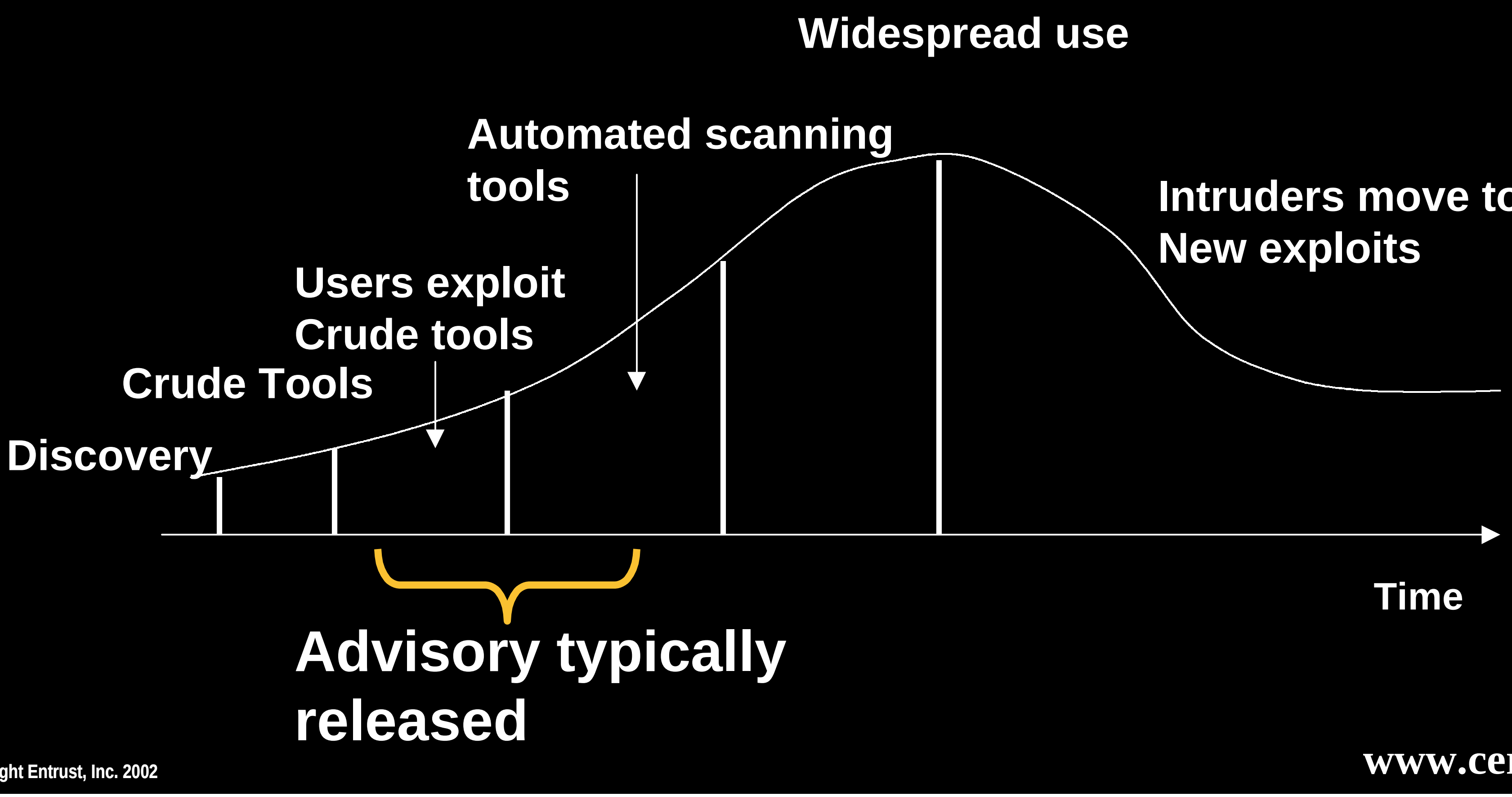
Password guessing

Low

1980 1985 1990 1995 2000

www.cert.org

Vulnerability Cycle

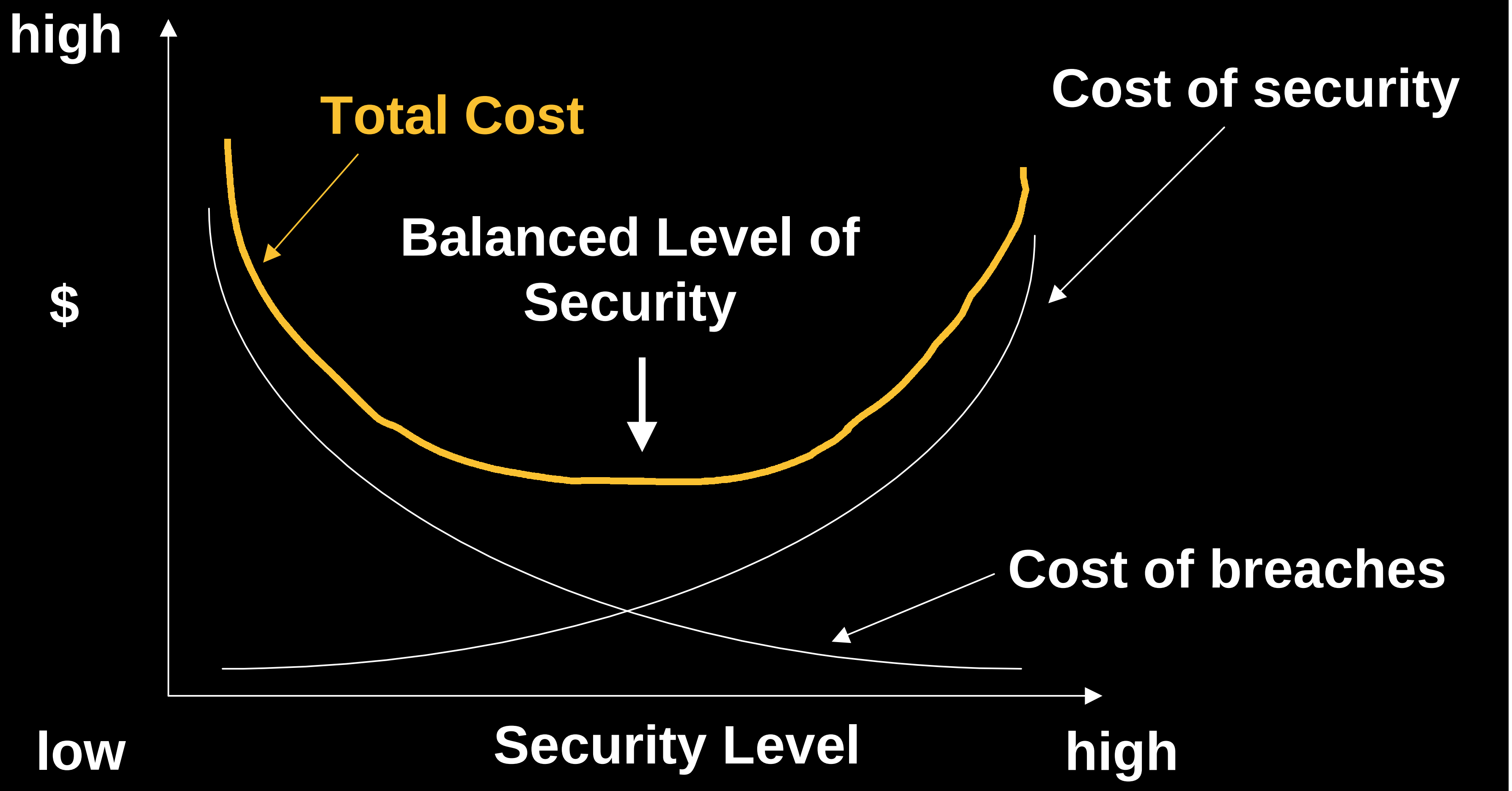


www.cert.org

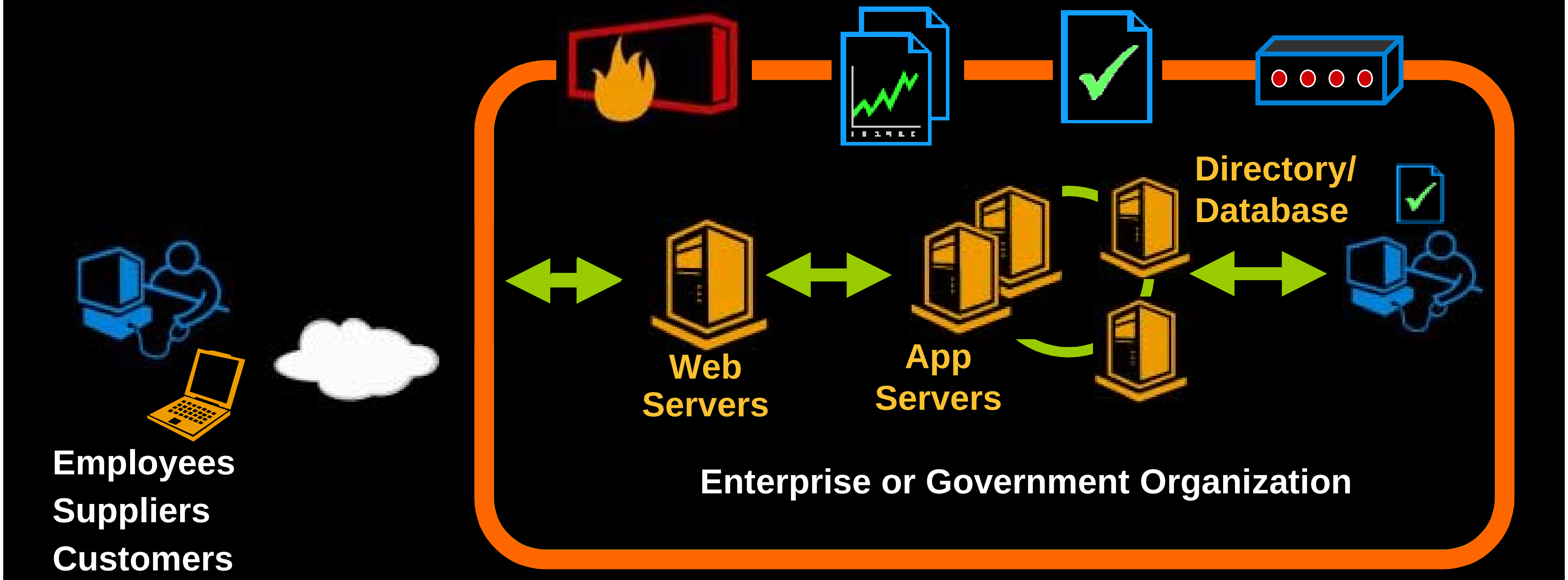
Trends

- Users, complexity, breaches: all increasing
- Number of people with security expertise is growing at a smaller rate than the number of internet users
- Security tools are increasing, but not as fast as the complexity of software and systems

Security in Balance



‘Basic’ Perimeter Security



Directory/
Database

Web
Servers

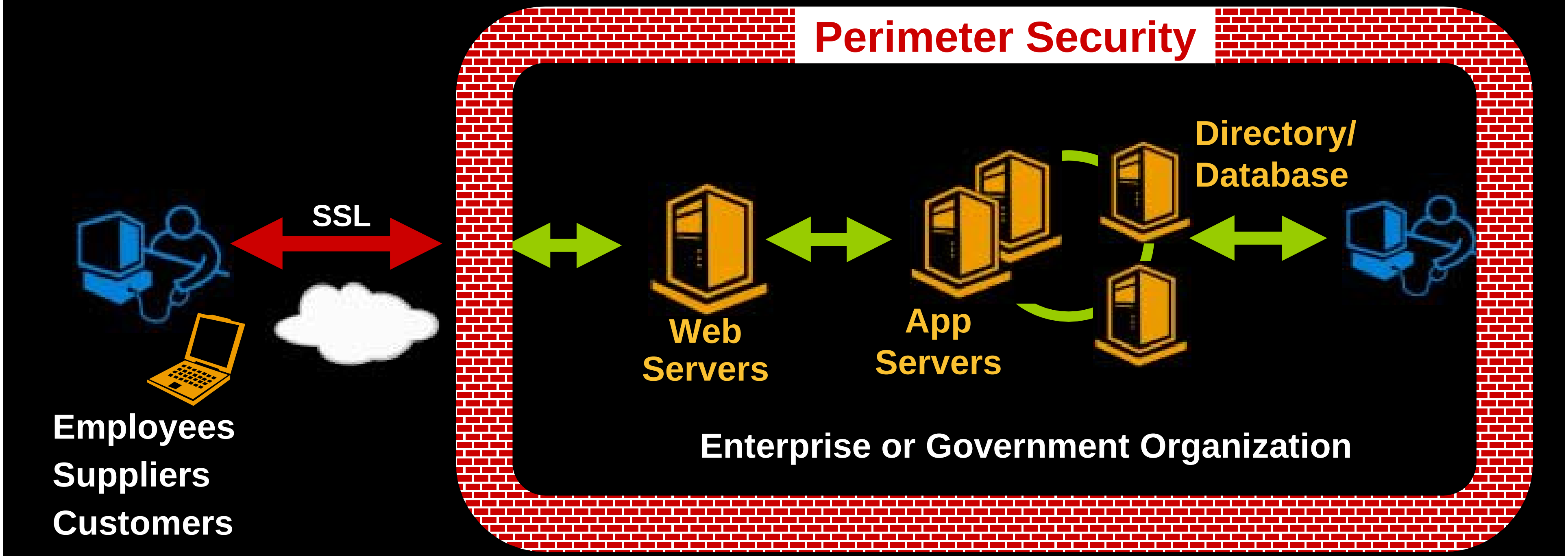
App
Servers

Employees
Suppliers
Customers

Enterprise or Government Organization

Firewalls, Virus Scanning, Intrusion Detection, E-mail Scanning

Perimeter Security and SSL

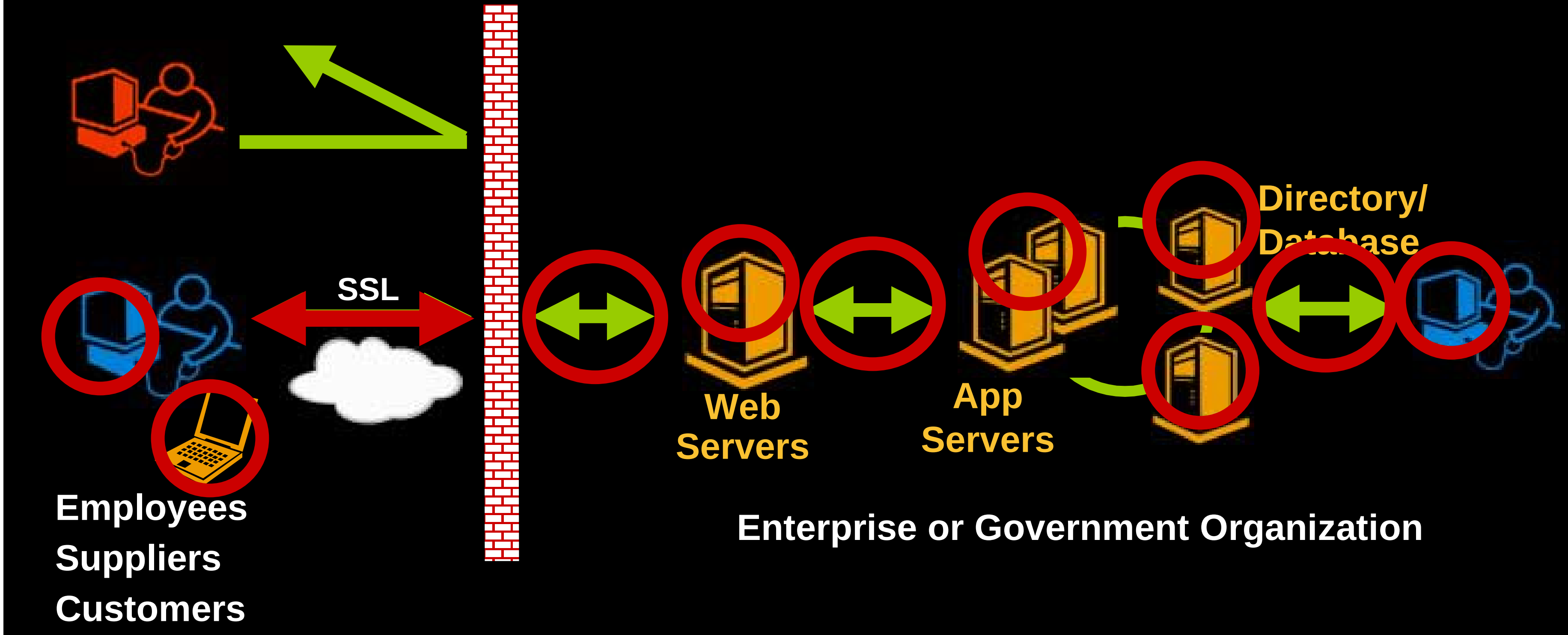


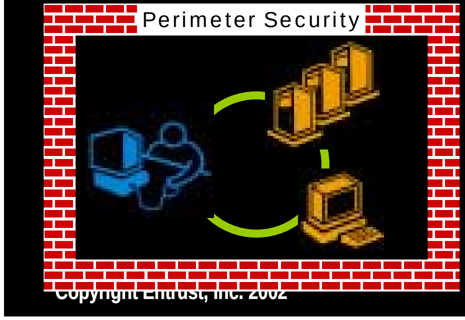
Perimeter Security

Employees
Suppliers
Customers

Enterprise or Government Organization

Basic Security is not Enough

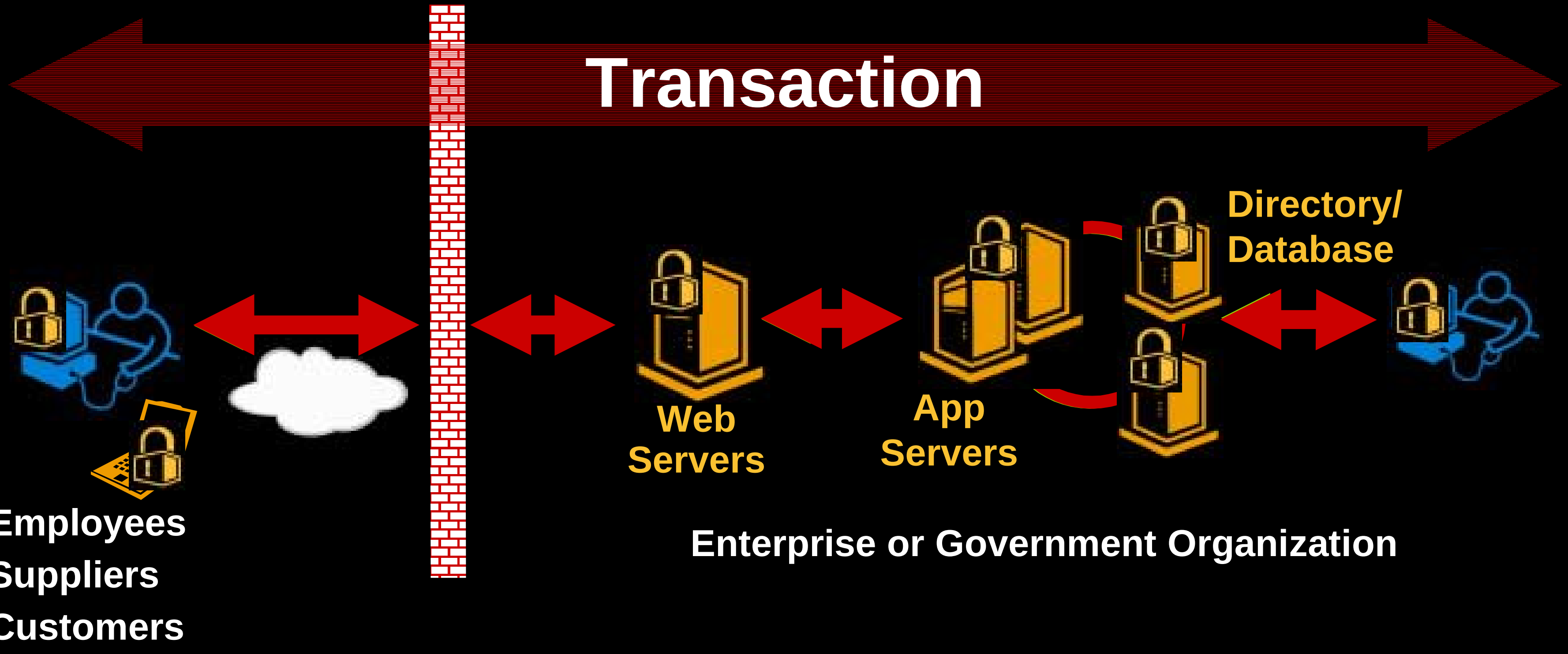




$4.5B will be spent this year on *defensive protection*

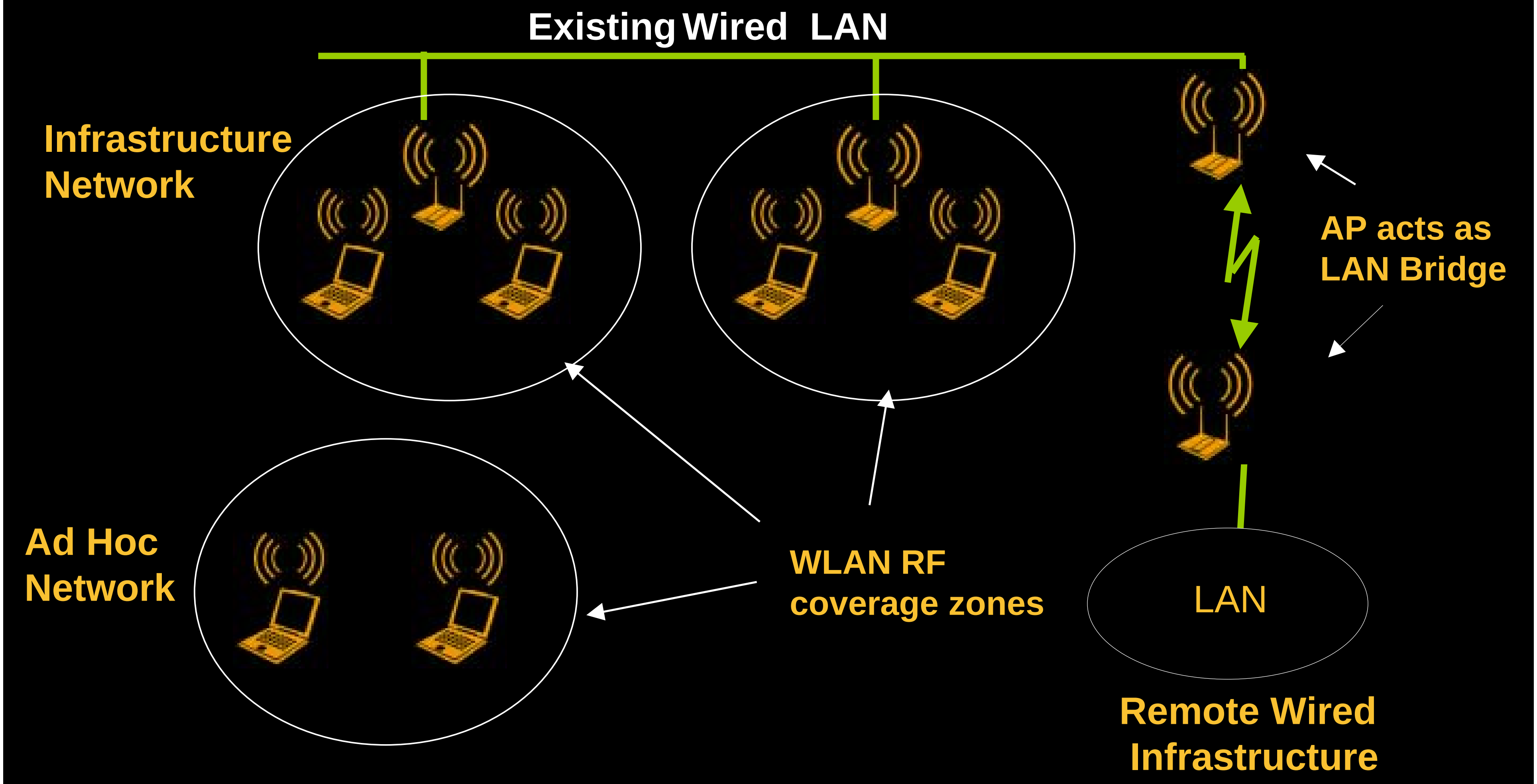
(Firewalls, Viruses, Intrusion Detection, E-mail Scanning)

Transaction and End to End Data Security Required

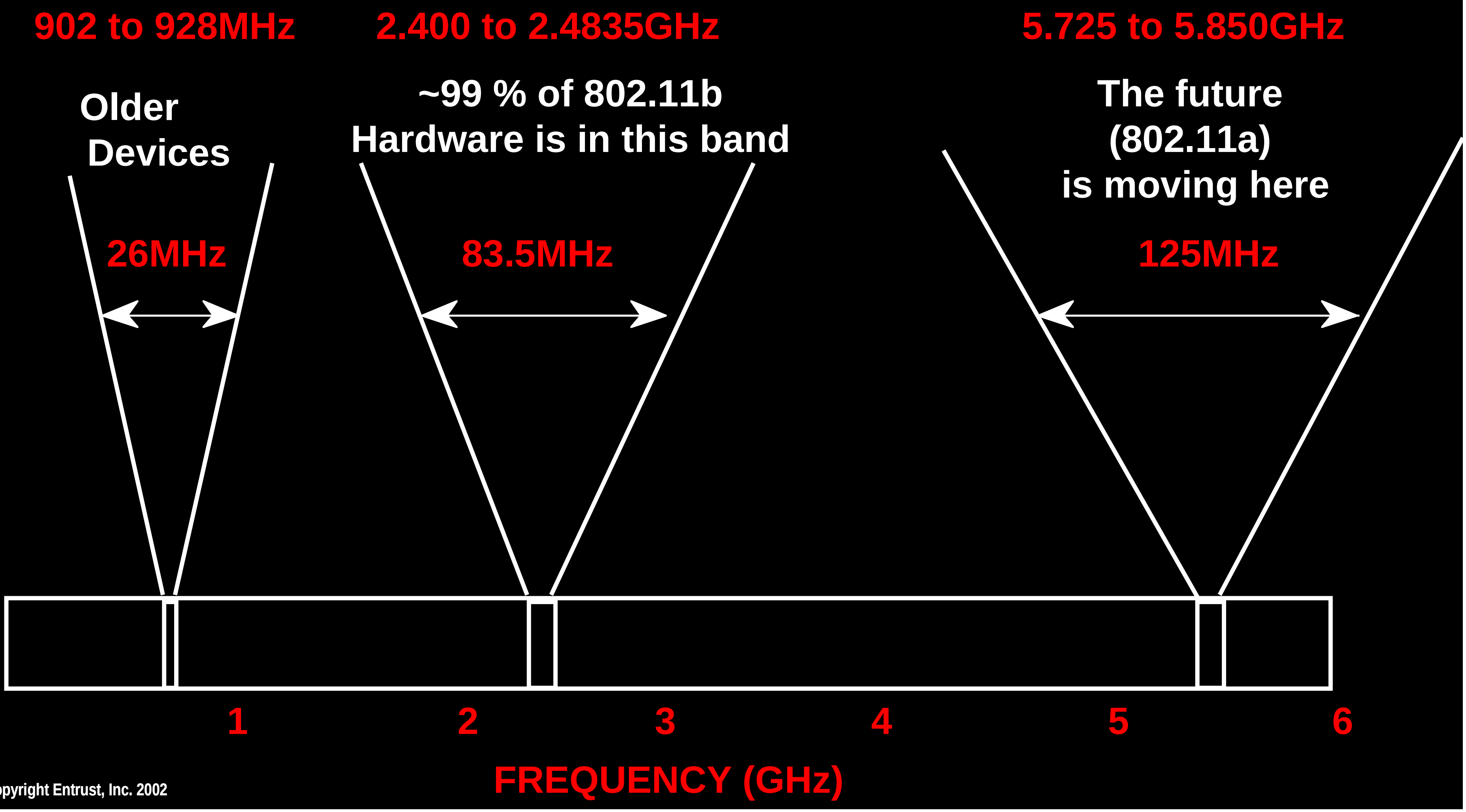


802.11b Wireless LAN

WLAN Architecture



WLAN Frequency Bands



902 to 928MHz

Older Devices

26MHz

2.400 to 2.4835GHz

~99 % of 802.11b Hardware is in this band

83.5MHz

5.725 to 5.850GHz

The future (802.11a) is moving here

125MHz

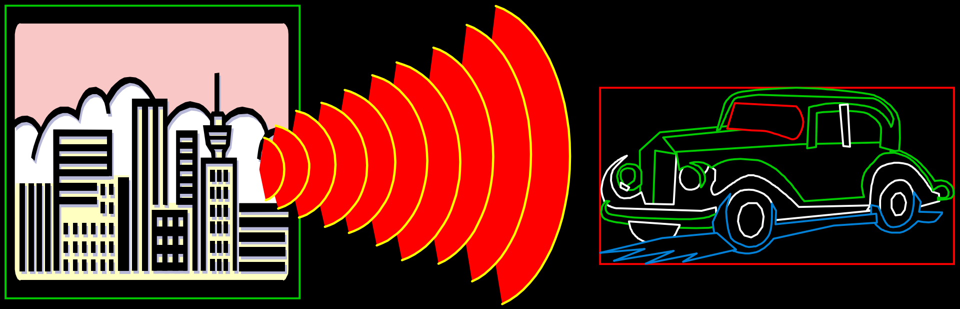
1 2 3 4 5 6

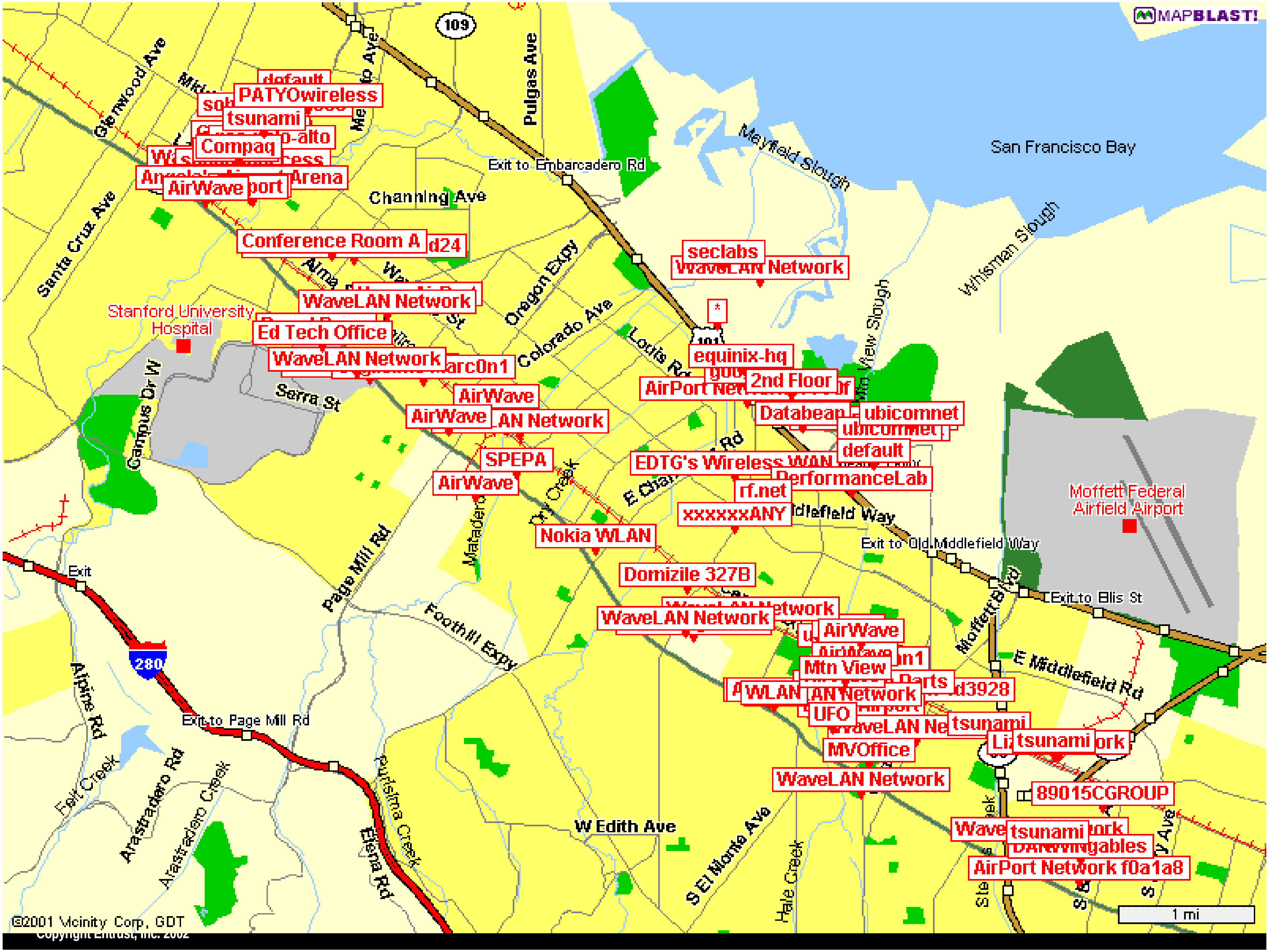
FREQUENCY (GHz)

War Driving

Issues:

- WLANs are proliferating providing a ‘target rich’ environment for the attacker.
- How close to an AP does the War Driver need to be?
- Can War Driver intercept useful Data?
- Can he get on the network and mount other attacks?

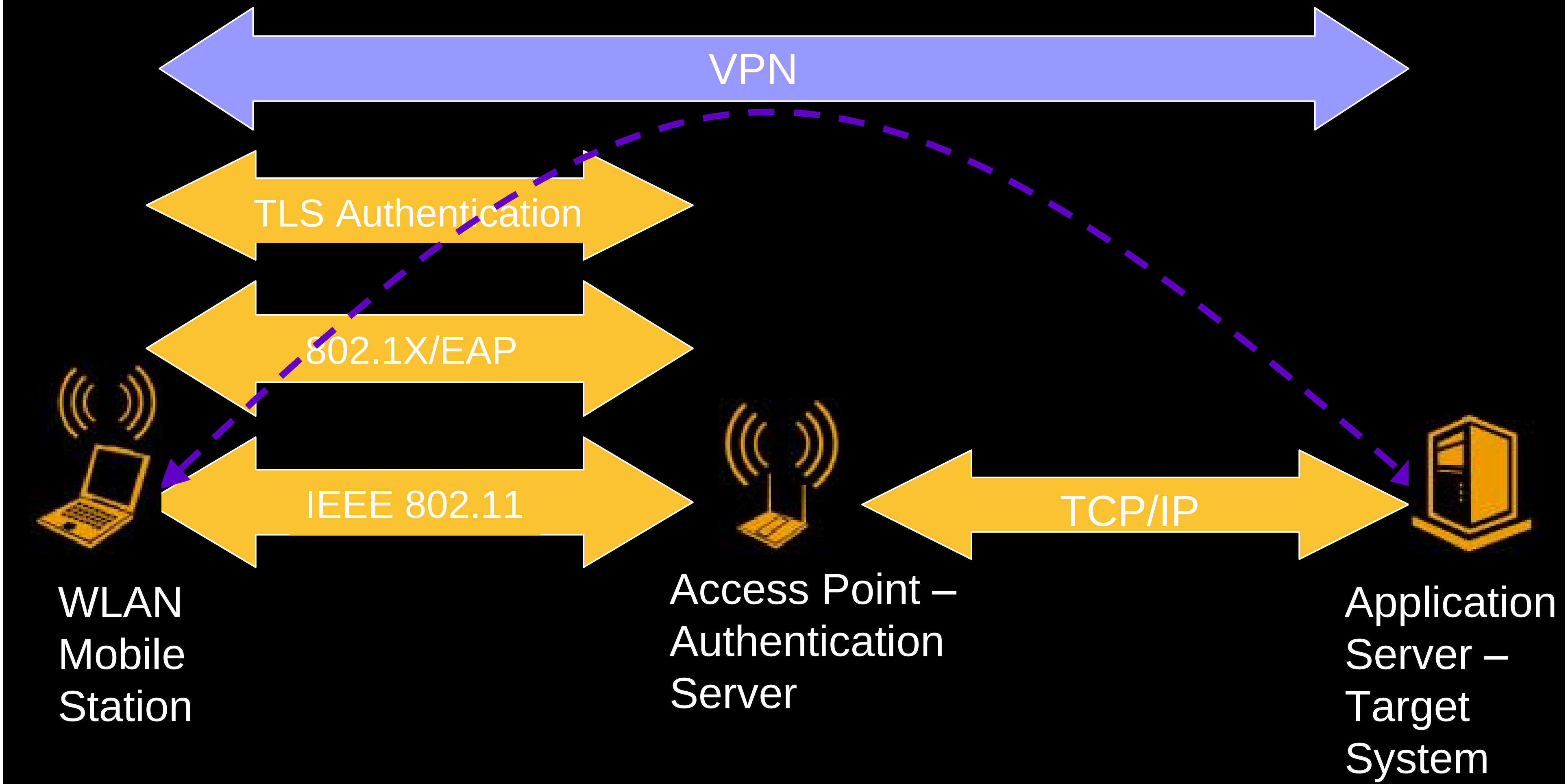



MAPBLAST!
109
Pulgas Ave
San Francisco Bay
Exit to Embarcadero Rd
Mayfield Slough
Whisman Slough
Channing Ave
Glenwood Ave
Santa Cruz Ave
default
PATYOwireless
tsunami
Compaq
AirWave
Arena
Conference Room A
d24
seclabs
WaveLAN Network
Alma
Oregon Expy
Stanford University Hospital
WaveLAN Network
Ed Tech Office
WaveLAN Network
arc0n1
Colorado Ave
Loma Verde
*
101
equinix-hq
2nd Floor
AirPort Network
Mtn View Slough
Serra St
Campus Dr W
AirWave
AirWave
AN Network
Databeam
ubicomnet
ubicomnet
default
SPEPA
AirWave
EDTG's Wireless WAN
PerformanceLab
rf.net
xxxxxxANY
Middlefield Way
Moffett Federal Airfield Airport
Exit to Old Middlefield Way
Nokia WLAN
Matadero
Dry Creek
E Charleston
Exit
Page Mill Rd
Domizile 327B
WaveLAN Network
WaveLAN Network
AirWave
Exit to Ellis St
Moffett Blvd
Foothill Expy
280
Mtn View
AirWave
WLAN
AN Network
Parts
d3928
E Middlefield Rd
UFO
WaveLAN Ne
tsunami
tsunami
ork
MVOffice
WaveLAN Network
89015CGROUP
Alpine Rd
Exit to Page Mill Rd
Felt Creek
Arastradero Rd
Arastradero Creek
Purisima Creek
Elena Rd
W Edith Ave
S El Monte Ave
Hale Creek
Wave
tsunami
ork
DARwingables
AirPort Network f0a1a8
1 mi

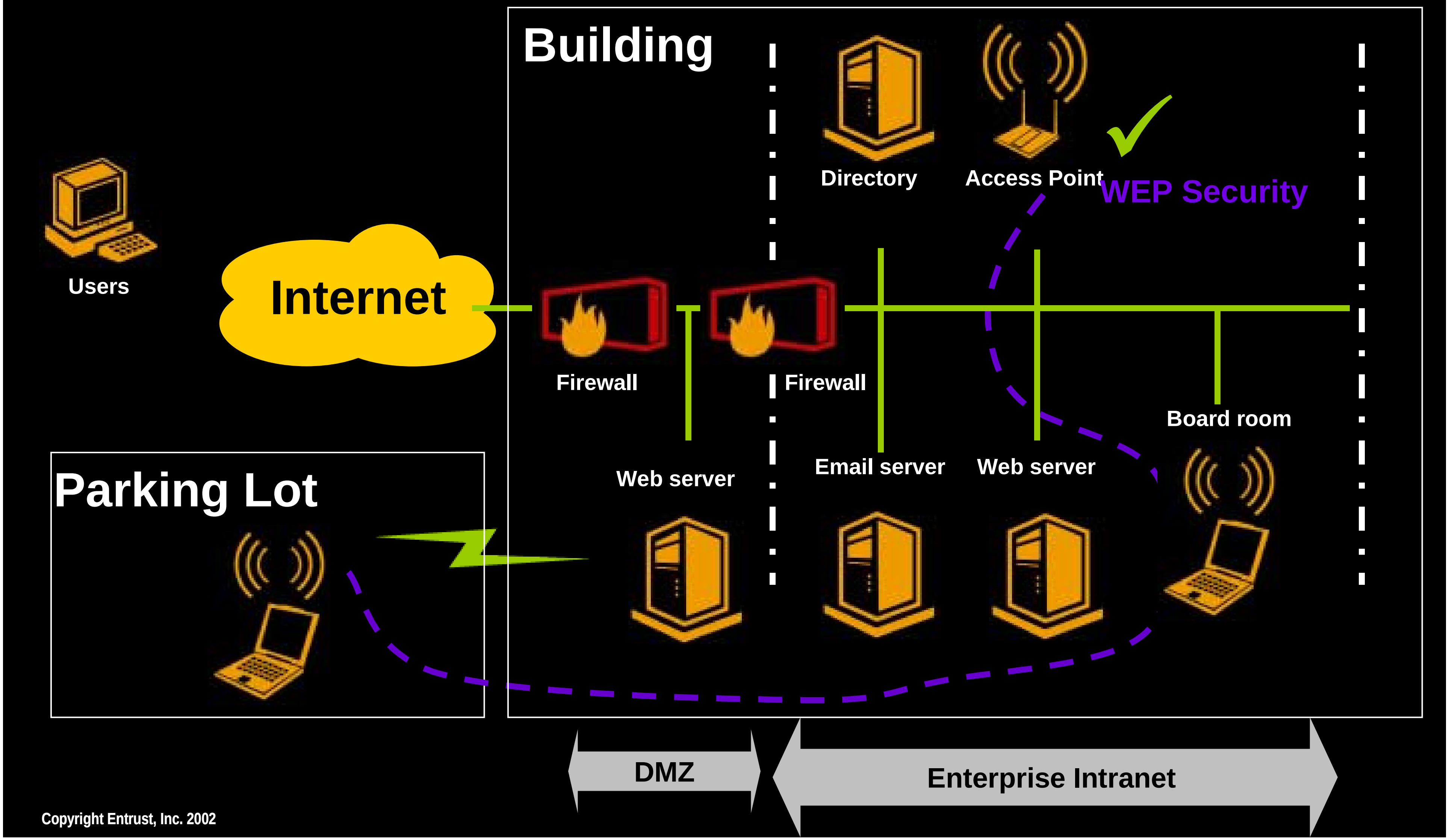
Security Issues

- AP Reception range further than advertised
- Poor crypto implementation in all devices
- Poor SNMP implementation in some APs
- Insecure default set-ups
- Rogue access points and stations

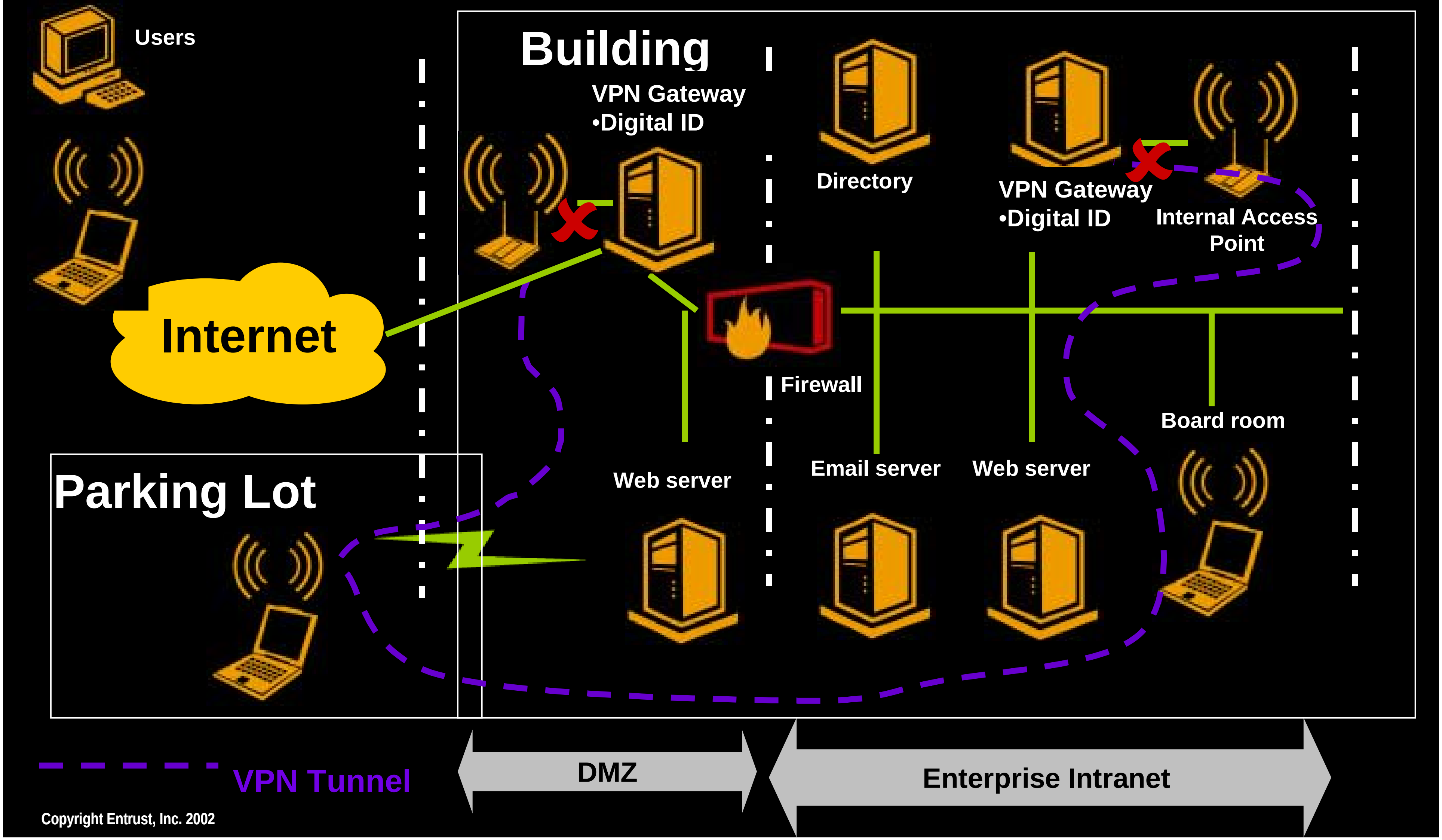
802.11 Security Alternatives


VPN
TLS Authentication
802.1X/EAP
IEEE 802.11
TCP/IP
WLAN Mobile Station
Access Point – Authentication Server
Application Server – Target System

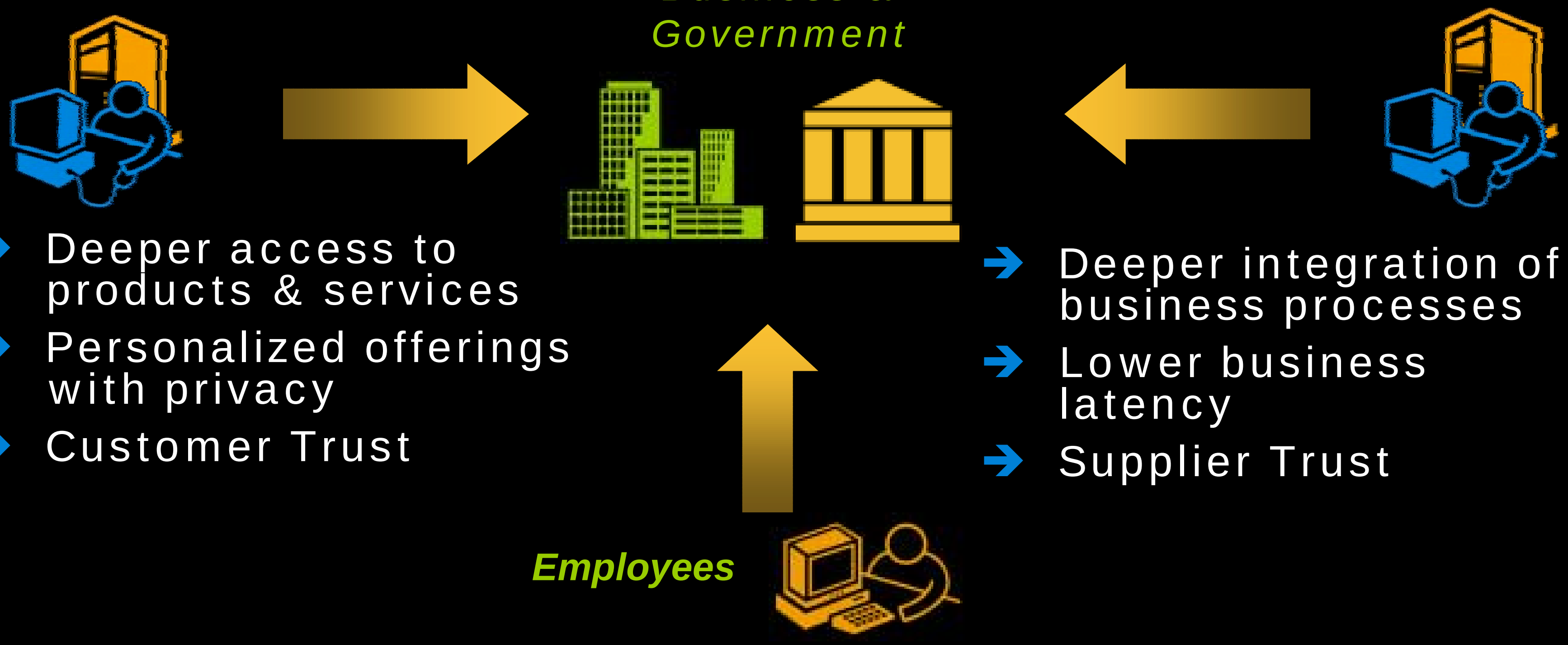
WLAN Enterprise Security- Weak Solution



WLAN Enterprise Security with VPN Tunnels- Strong Solution



Security Must Protect and Enable



Customers

- ➔ Deeper access to products & services
- ➔ Personalized offerings with privacy
- ➔ Customer Trust

Business & Government

Suppliers

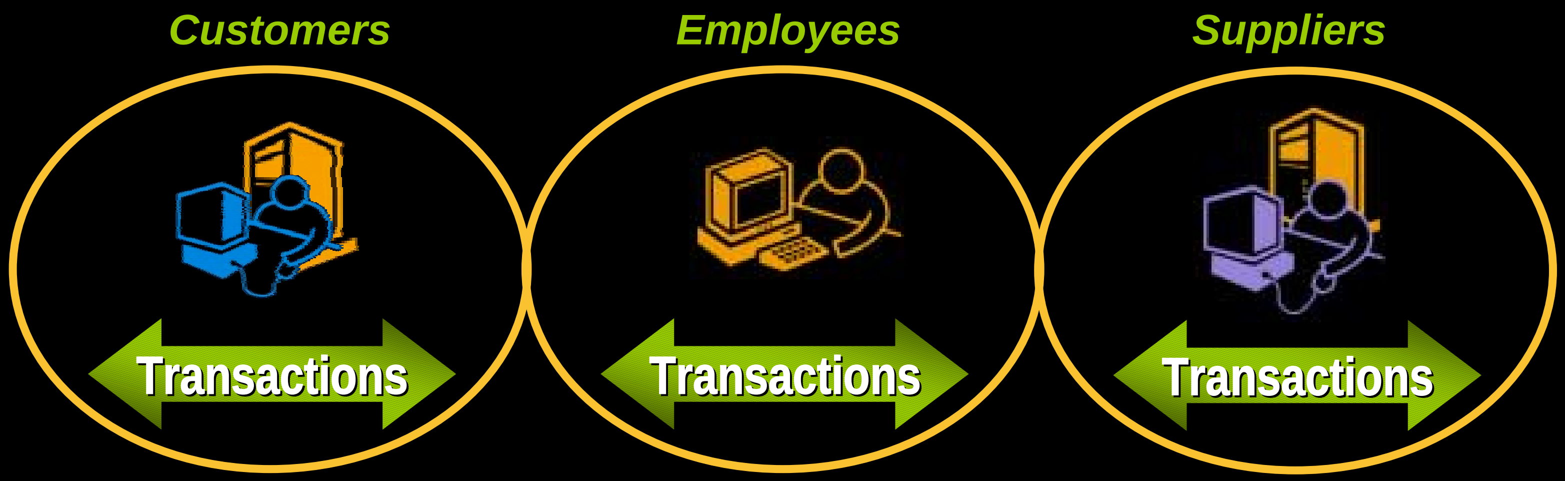
- ➔ Deeper integration of business processes
- ➔ Lower business latency
- ➔ Supplier Trust

Employees

- ➔ Faster business processes
- ➔ Anywhere, anytime access to business processes
- ➔ Employee Trust

Move from Isolated Enterprise & Government . . .

- Transactions are the vehicle for business processes
- To date, most transactions have been within the organization



Customers

Transactions

Employees

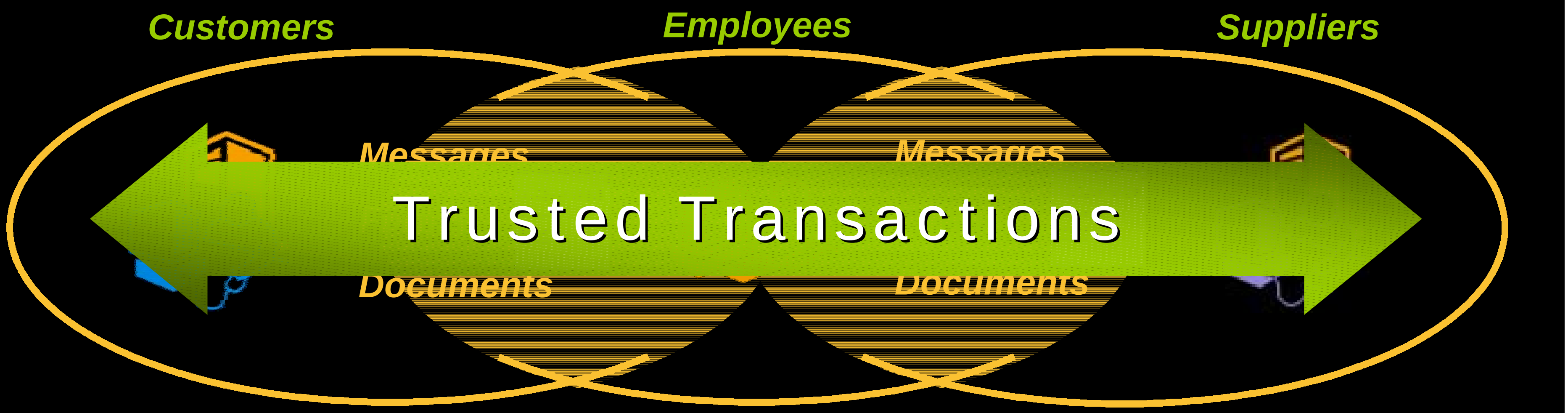
Transactions

Suppliers

Transactions

To Extended Enterprise & Government

- Deep business process integration requires trust
  - With trust, transactions can be conducted across the extended enterprise & government



Customers

Employees

Suppliers

Messages

Messages

Trusted Transactions

Documents

Documents

What is Required for Trusted Transactions?

Transactions

Enhanced Security +

Security Management +

Trusted Transactions

What is Enhanced Security?

Identification

Authenticating and **Protecting** Identity used in Transactions

Entitlements

Providing **Personalized** Access and Authorization to Transactions

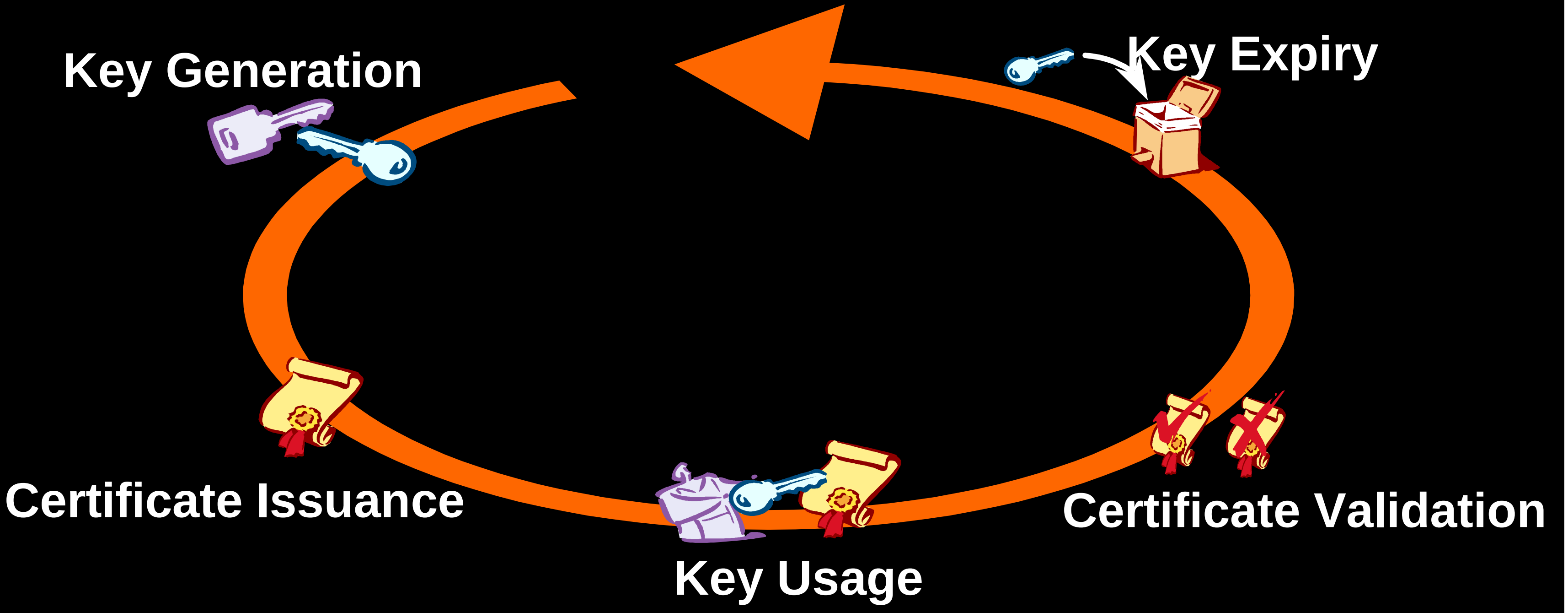
Privacy

Enforcing **Privacy** of Transaction Information

Verification

Ensuring Transactions are **Binding** and **Auditable**

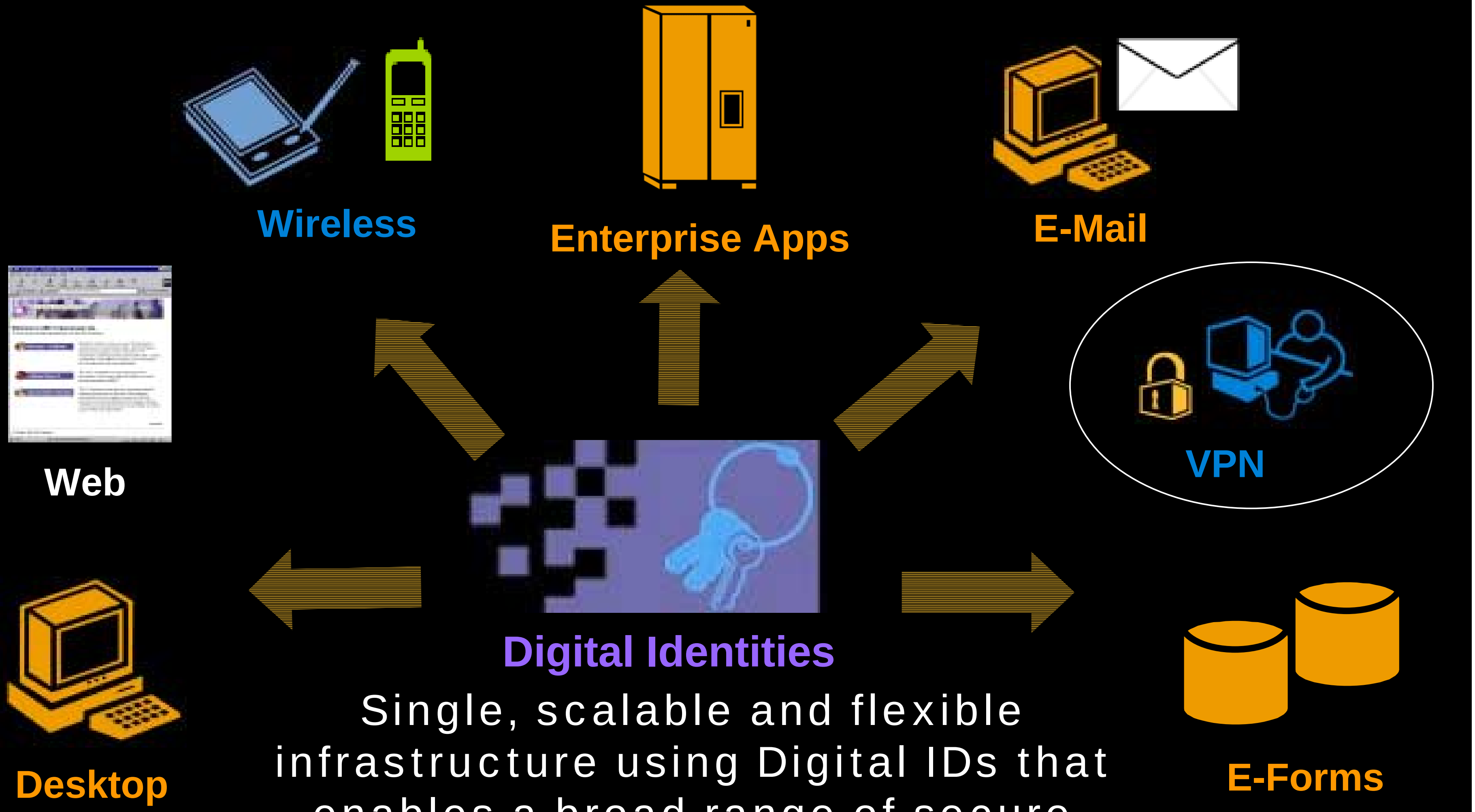
Enhanced Security Management Example for Certificates



Requirements:

- Automated key and certificate lifecycle management
- Self-service administration
- Support across a wide variety of applications and operating systems

“Enterprise-wide” Infrastructure



Wireless

Enterprise Apps

E-Mail

Web

VPN

Digital Identities

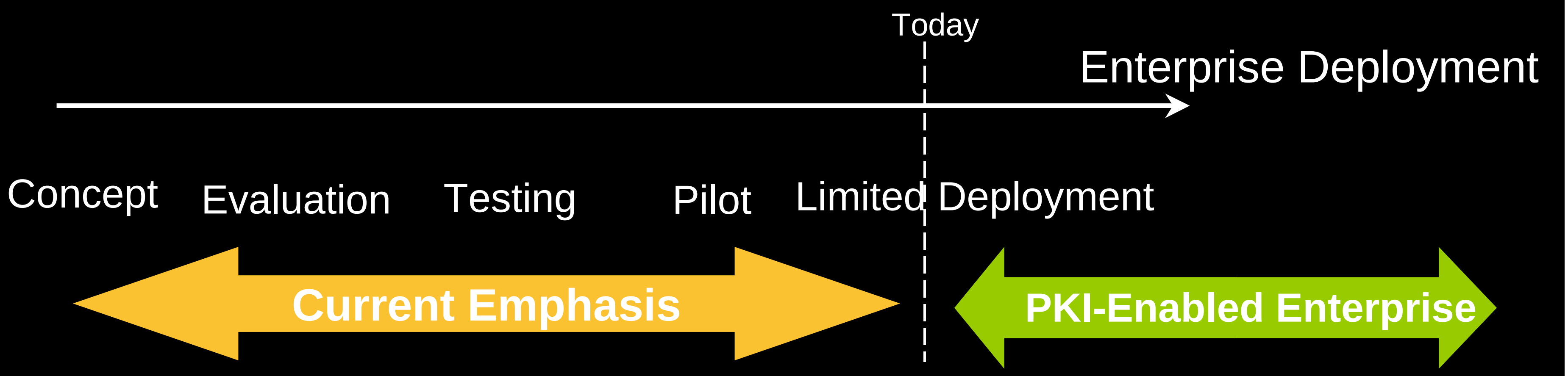
Desktop

E-Forms

Single, scalable and flexible infrastructure using Digital IDs that enables a broad range of secure transactions

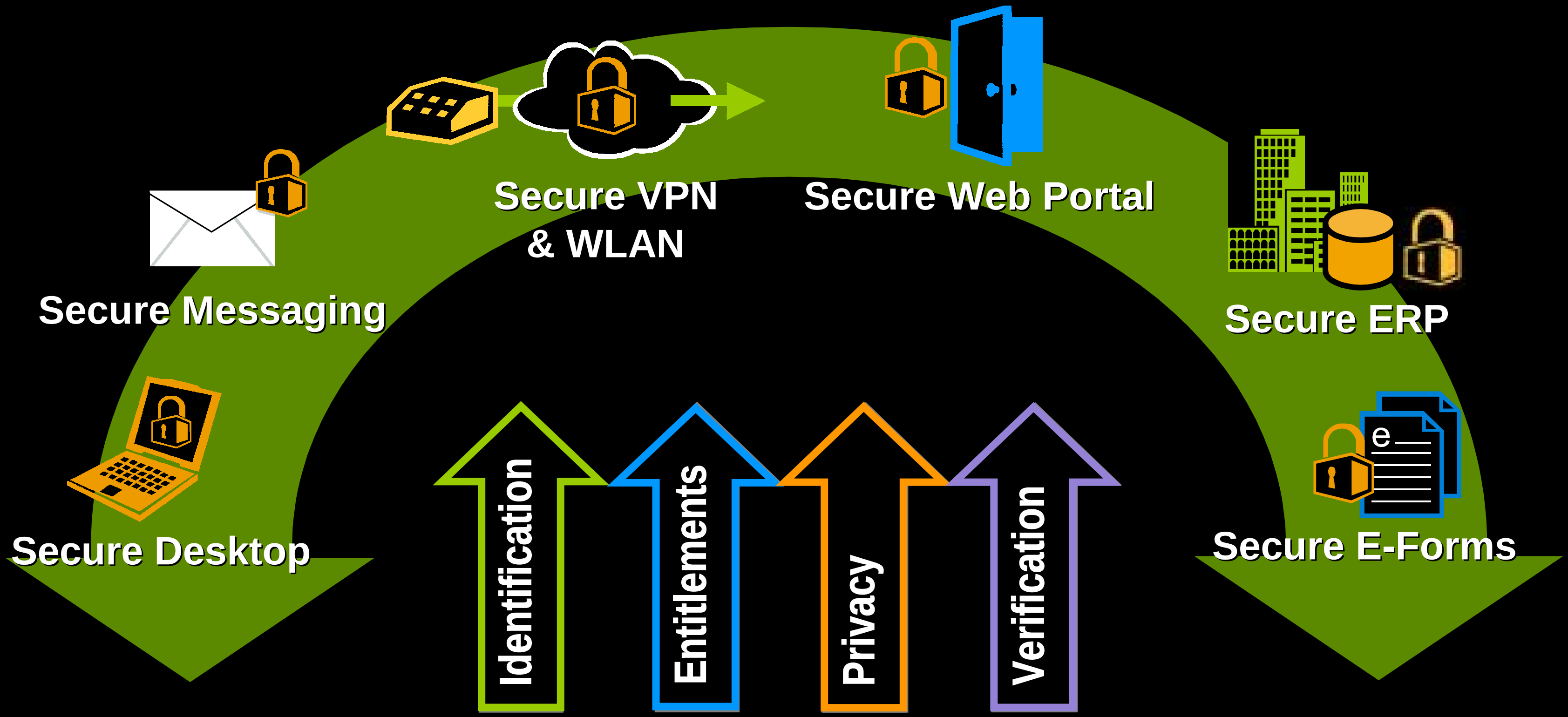
The Current PKI Landscape

- A lot of companies evaluating
- Many companies in pilot testing
- Some companies in production

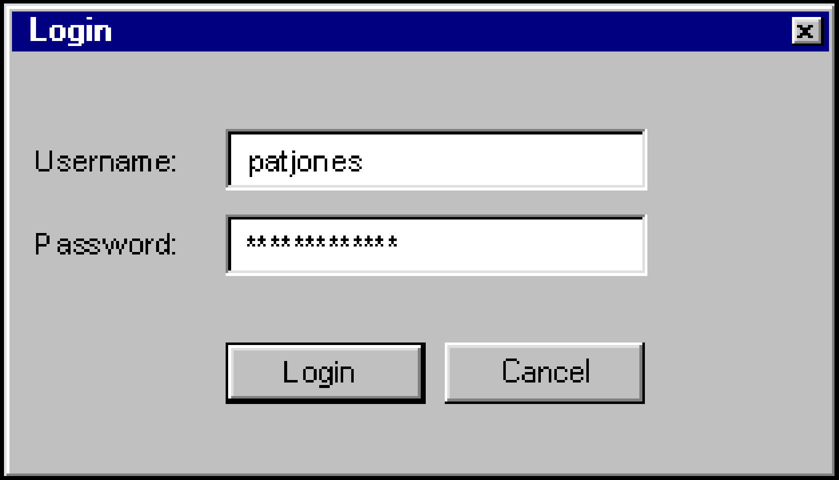


✓ Extensible Investment

. . and then leverage the investment



Username/Password



Login

Username: patjones

Password: *************

The ‘minimum’ authentication

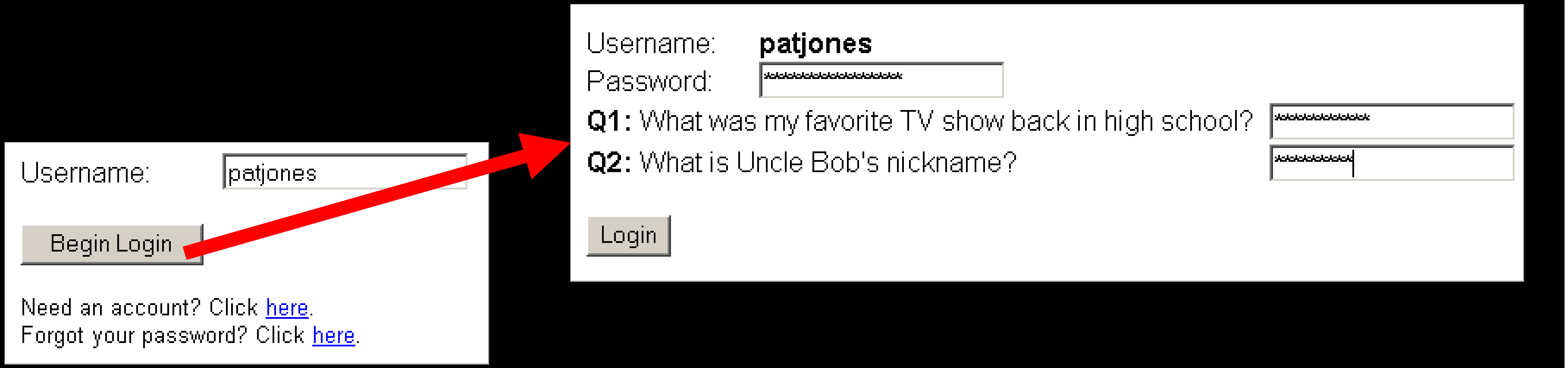
Even with username/password…

- PKI is stronger than regular username/password solutions
- The password does not travel over the network during login
- The server does not maintain a password list on the server
- Passwords alone do not do digital signature

Passwords with PKI provide stronger level of authentication

You can go further...

- User-selected Q&A
  - e.g. prompt for 2 of 10 pre-established questions
- Alternately, RSA SecurID or similar



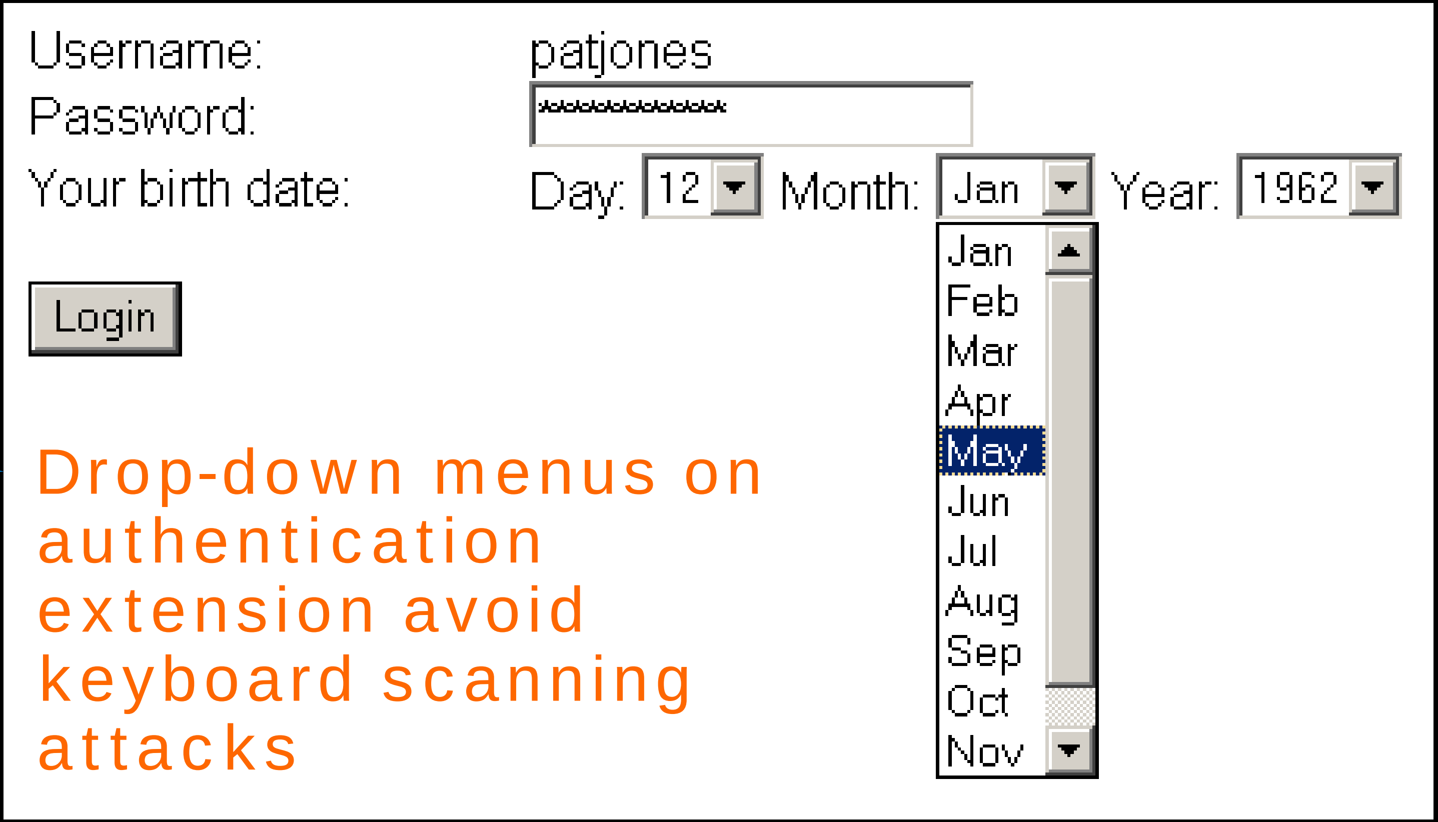
Username: patjones

Need an account? Click here.
Forgot your password? Click here.

Username: **patjones**
Password: ****************
Q1: What was my favorite TV show back in high school? ***********
Q2: What is Uncle Bob's nickname? *********

Enhanced Security: *Not All Transactions Are Created Equal*

... further ...



Username: patjones

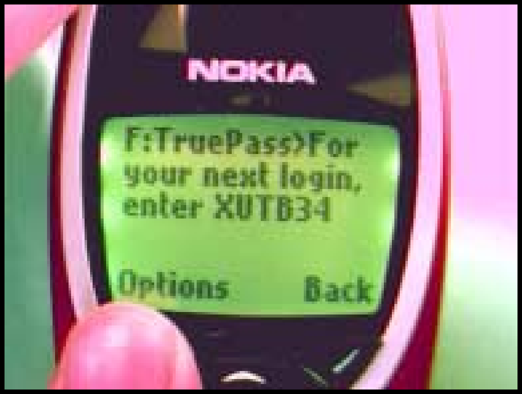
Password: ************

Your birth date: Day: 12 Month: Jan Year: 1962

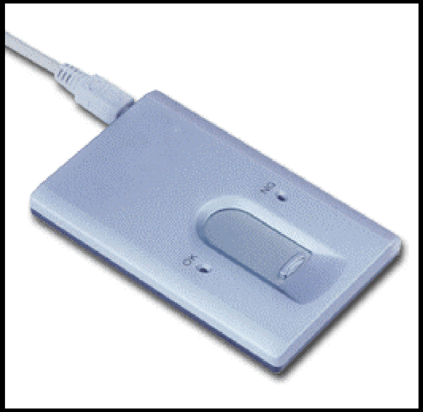
- Drop-down menus on authentication extension avoid keyboard scanning attacks

Complimentary 2-factor, 3-factor steps

- Physical cards, tokens
- Biometrics

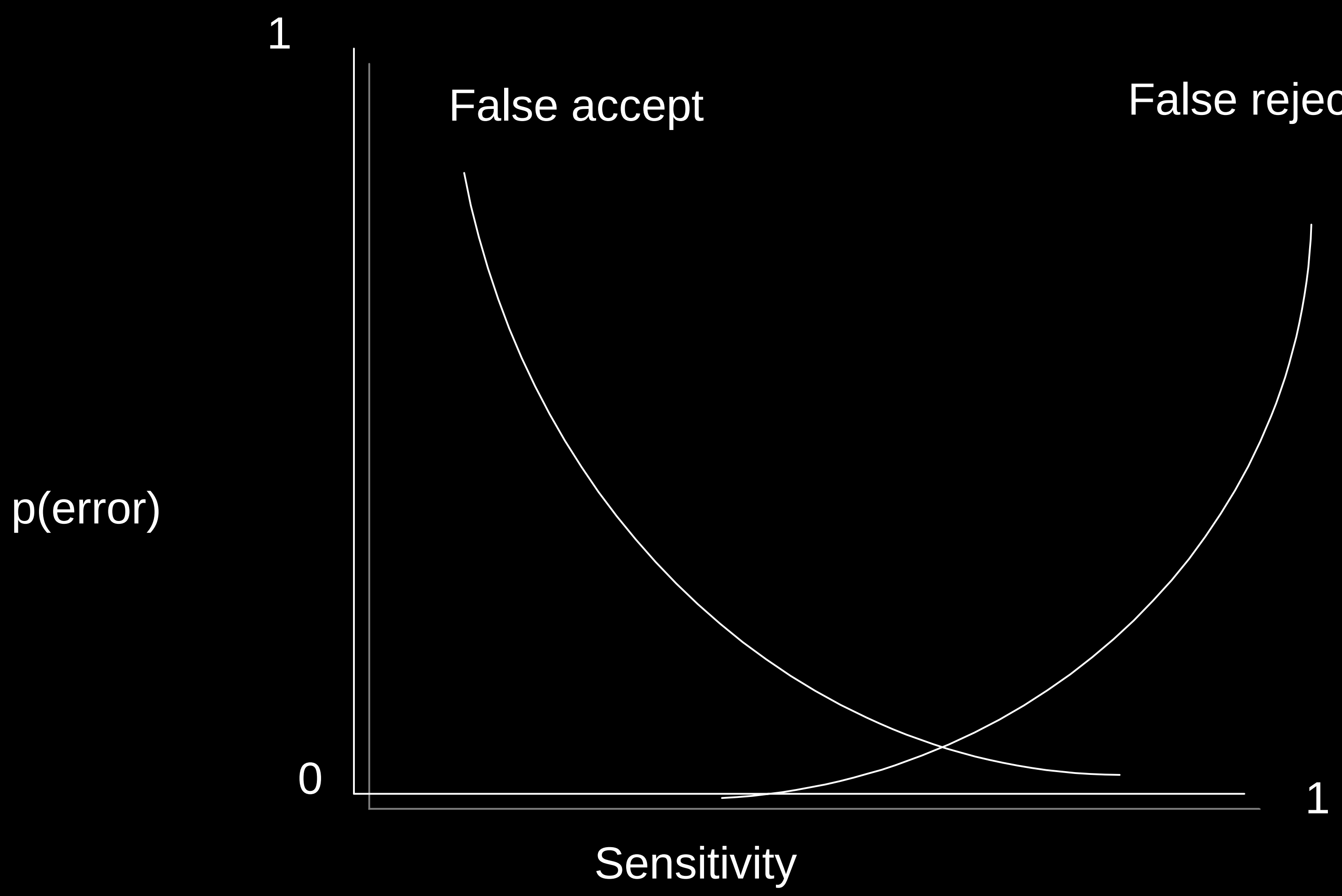


F:TruePass>For your next login, enter XUTB34

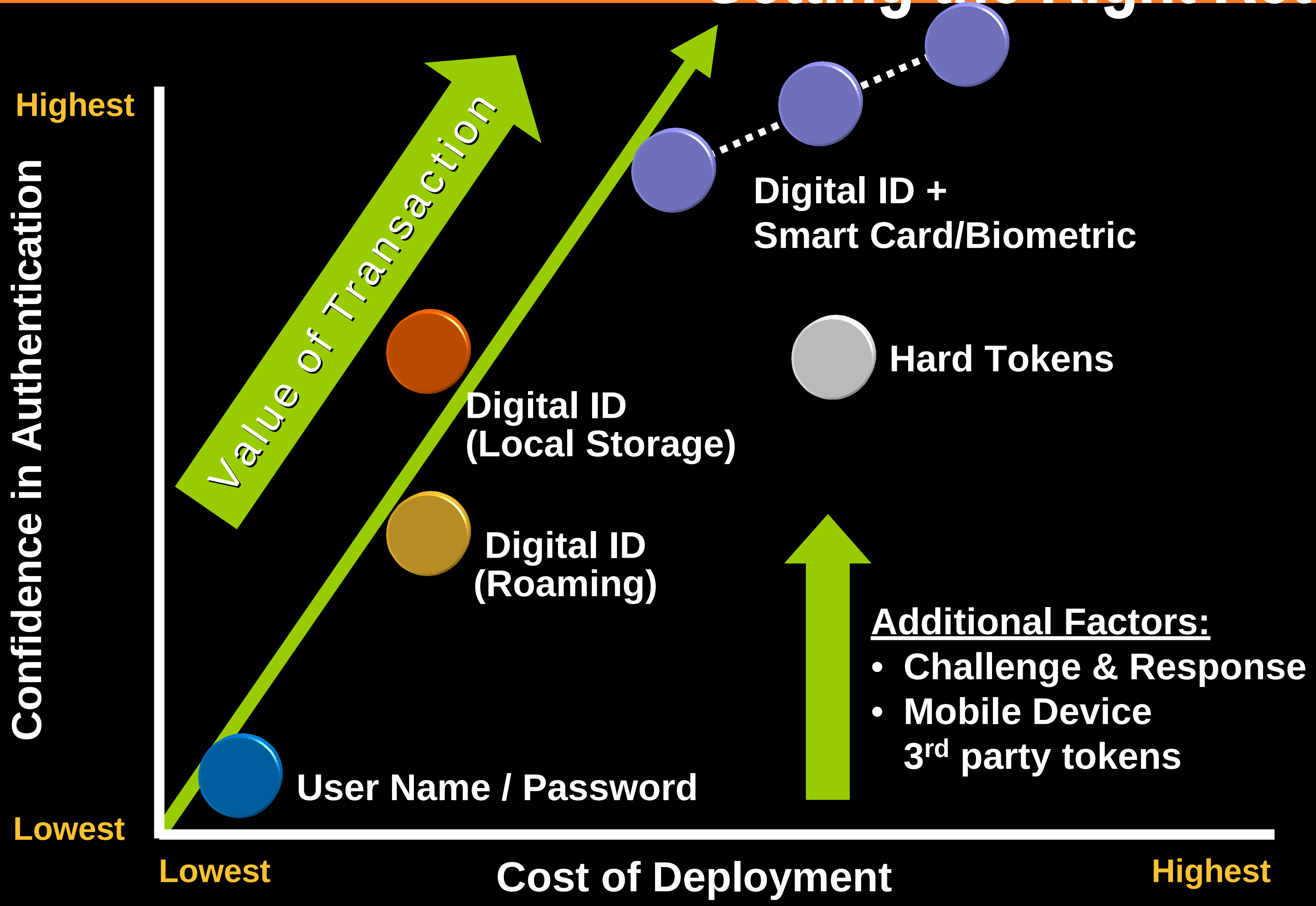


Complimentary technology provides greater certainty for identification

Biometric Accuracy Problem



Identification:
Getting the Right Return

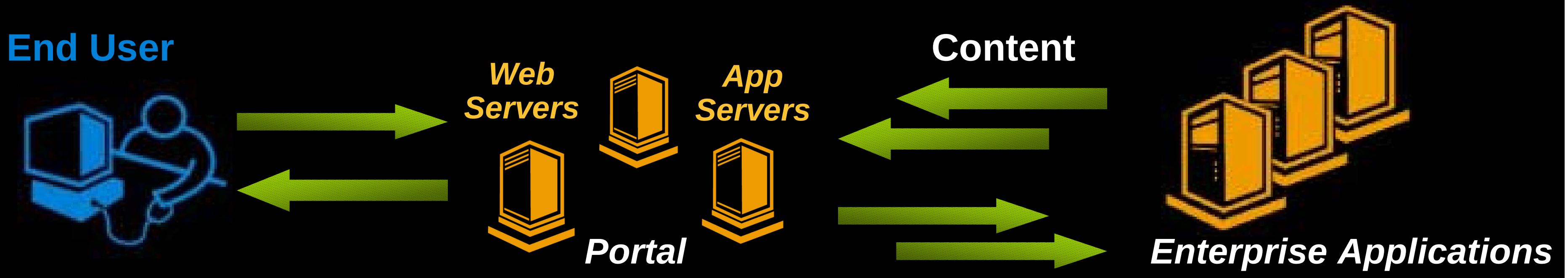


Additional Factors:

- Challenge & Response
- Mobile Device
  3rd party tokens

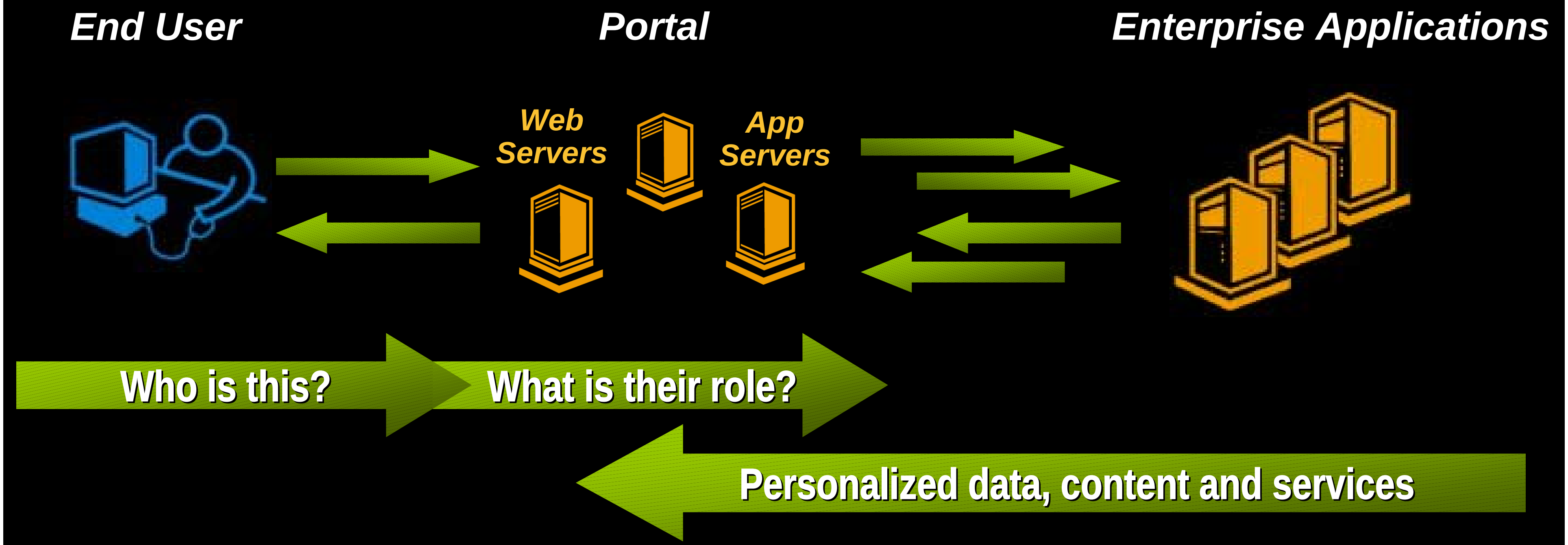
Web Portals Deliver

A single doorway for employees, customers/citizens and partners to access data, content and services



... and establish relationships over the Web

Trust Enables Personalization



End User

Portal

Enterprise Applications

Web Servers

App Servers

Who is this?

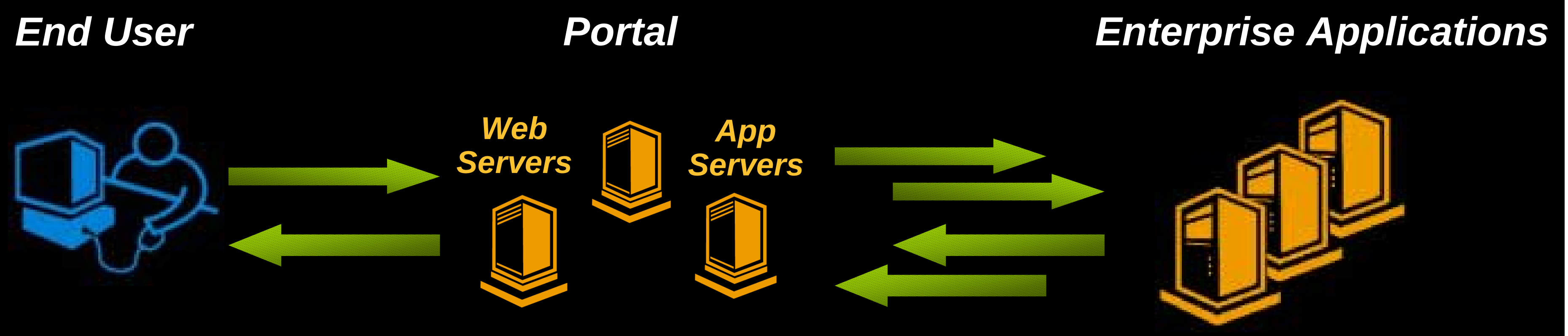
What is their role?

Personalized data, content and services

Personalization delivers:

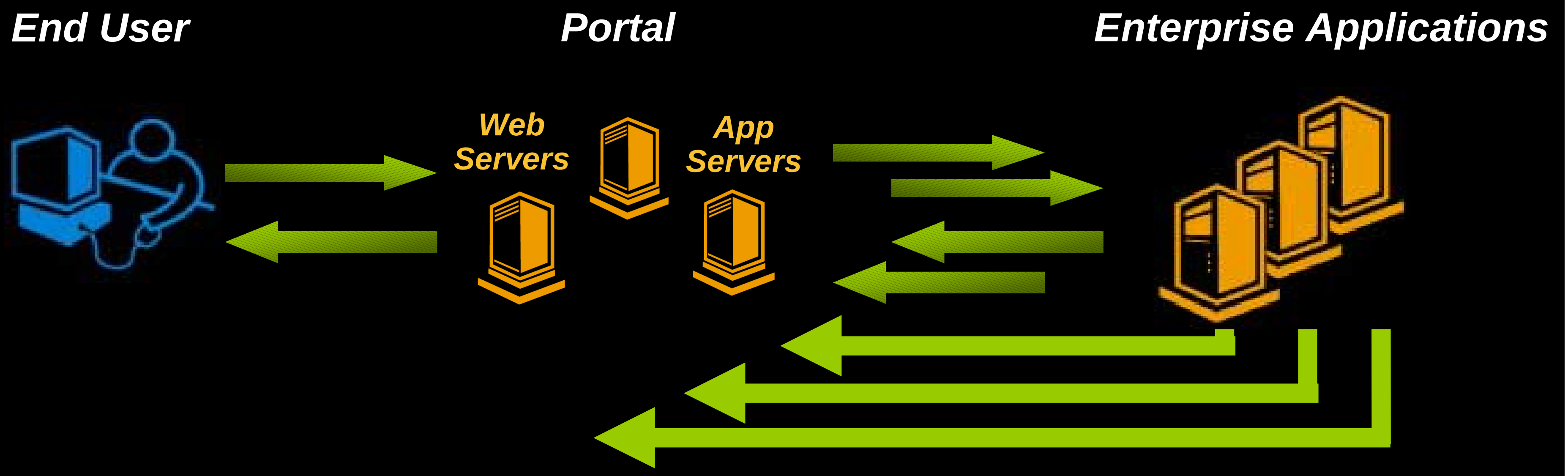
- Increased customer loyalty and retention
- Targeted delivery of new services for greater up-take
- Reduced administration costs

Trust Enables Personalization



Personalization Requires Identification and Entitlements

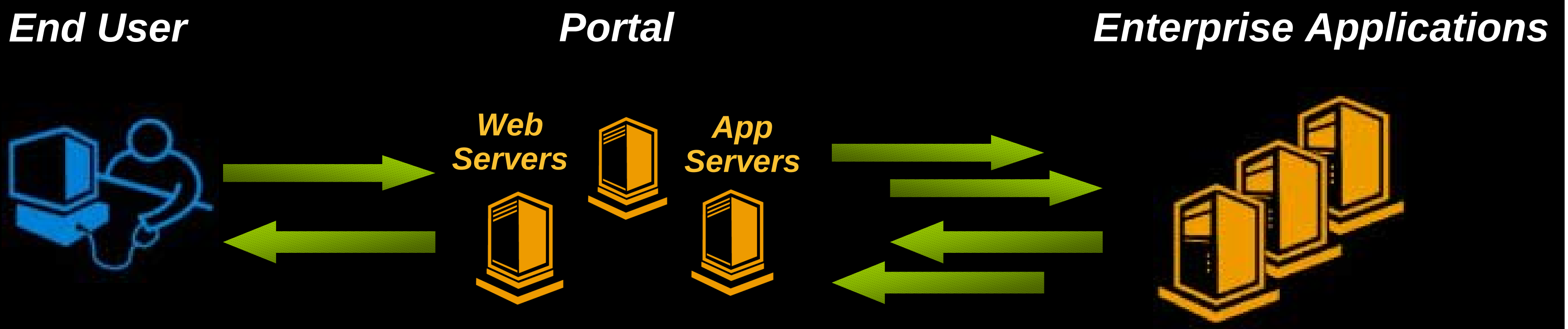
Trust Enables Application Integration



Application integration delivers:

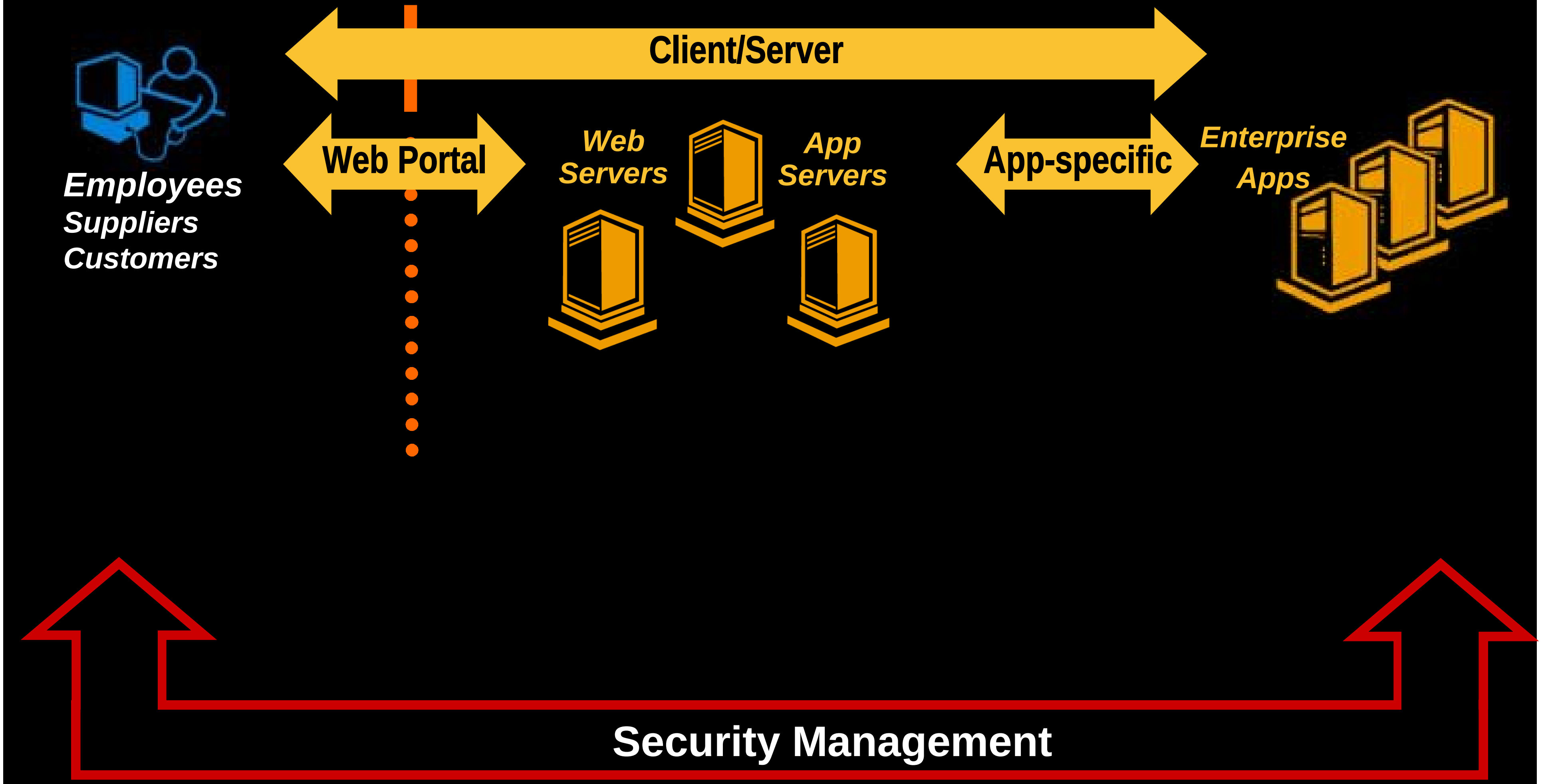
- Increased customer loyalty and retention
- Greater reach for new services
- Reduced delivery costs

Trust Enables Application Integration

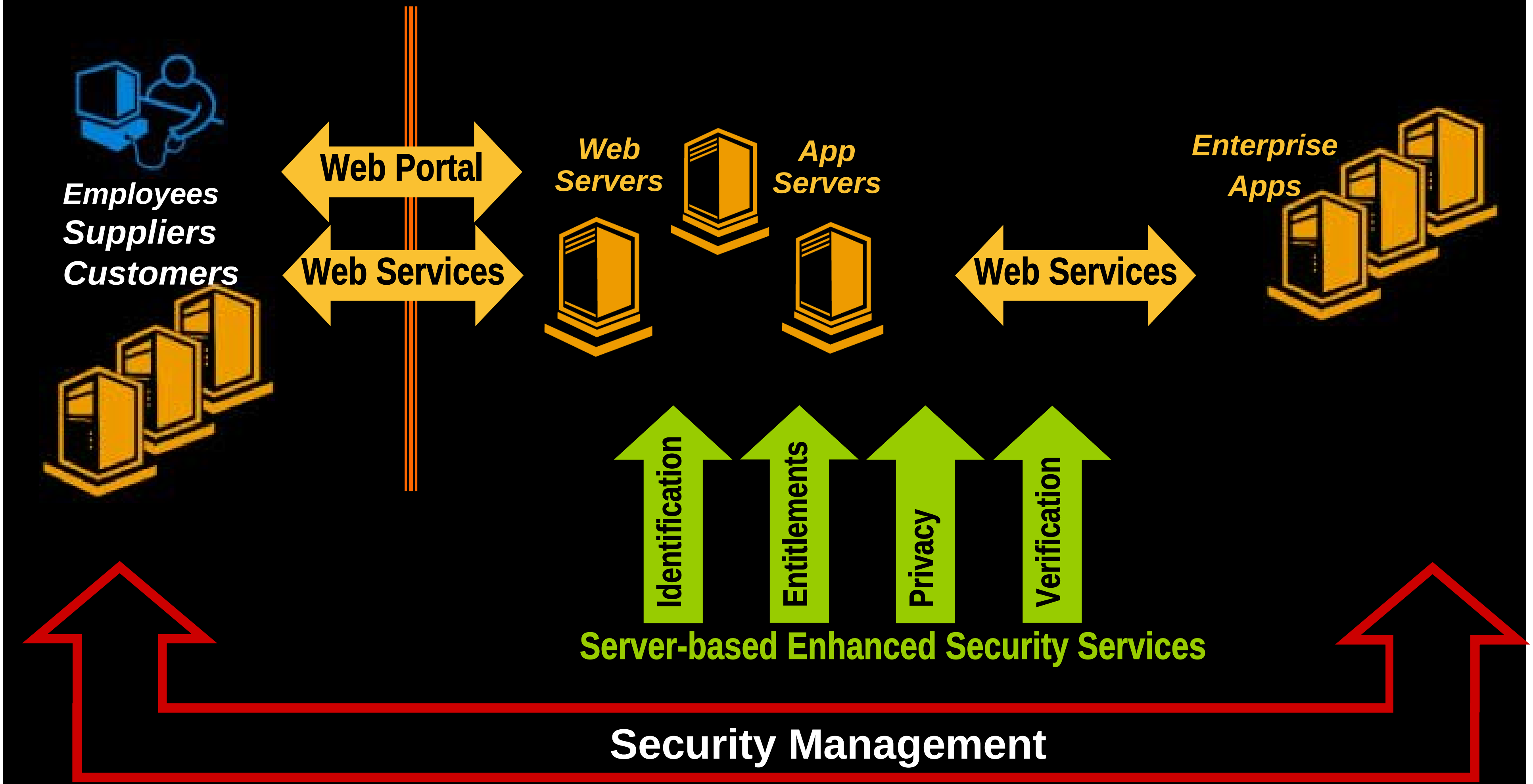


Application Integration Requires Identification, Privacy and Verification

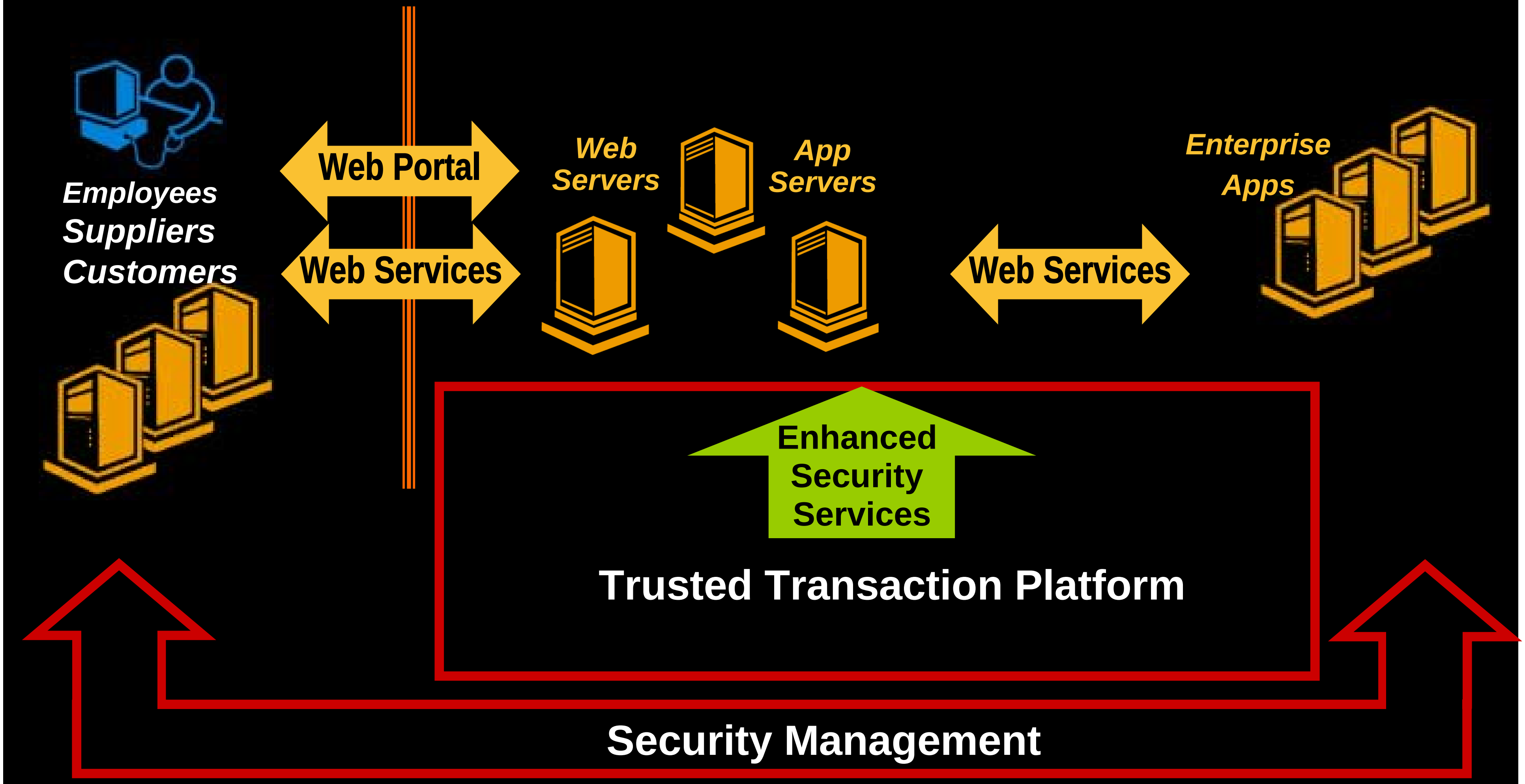
IT Landscape - Today



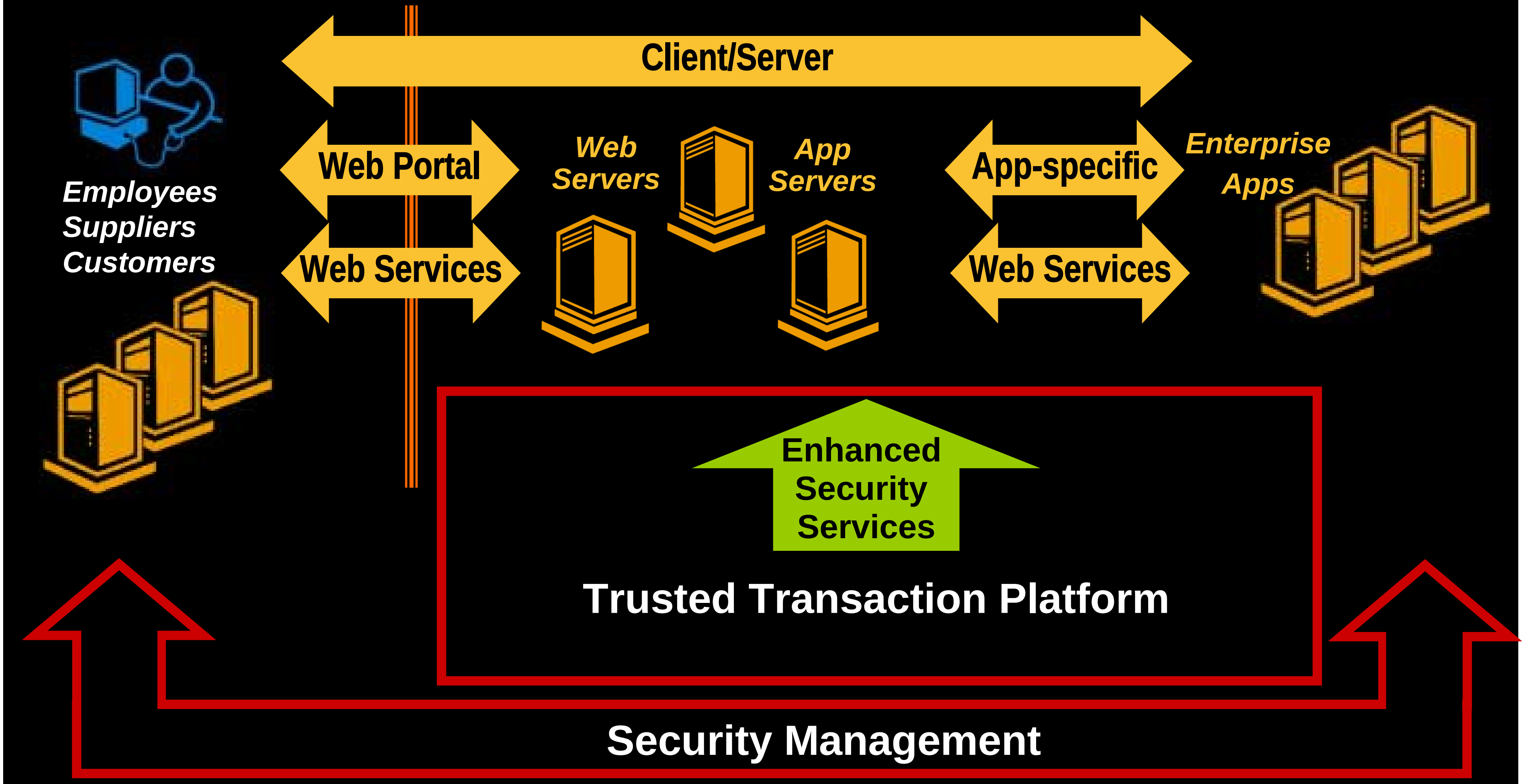
IT Landscape - Future



IT Landscape - Future



IT Landscape - Tomorrow



Enabling Interoperability

- Government, businesses and citizens need to communicate over a secure infrastructure
- Departmental projects are often technological stove pipes
- Identities and entitlements must be trusted by others
- Either common policy, or map different policy levels across departments
- Map entitlements across departments/companies

Mission of the Liberty Alliance

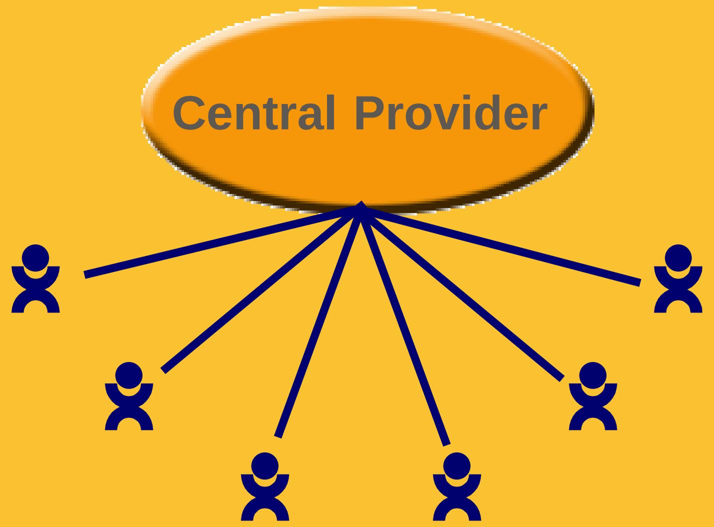
Establish an open standard for federated network identity through open technical specifications that will:

- Support a broad range of identity-based products and services
- Allow for consumer choice of identity provider(s), the ability to link accounts through account federation, and the convenience of single sign-on, when using any network of connected services and devices
- Enable commercial and non-commercial organizations to realize new revenue and cost saving opportunities that economically leverage their relationships with customers, business partners, and employees
- Improve ease of use for e-commerce consumers

Why is Federated Important?

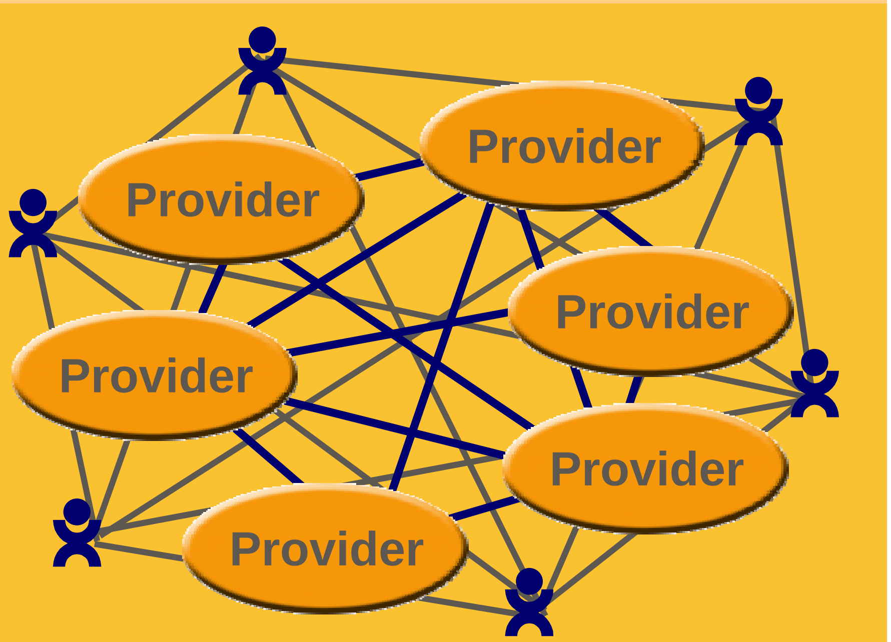
Centralized Model

- Network identity and user information in single repository
- Centralized control
- Single point of failure
- Links similar systems



Open Federated Model

- Network identity and user information in various locations
- No centralized control
- No single point of failure
- Links similar and disparate systems



Key Objectives of the Liberty Alliance

- **Simplified Sign-On:** Provide an open simplified sign-on specification that includes federated authentication from multiple providers operating independently, simplified access across multiple accounts within a trust community, and portable on-line identity

- **Enhance Constituent Relationships:** Enable commercial and non-commercial organizations to control, maintain and enhance relationships with constituents

- **Support All Devices:** Create a network identity infrastructure that supports all current and emerging network access devices

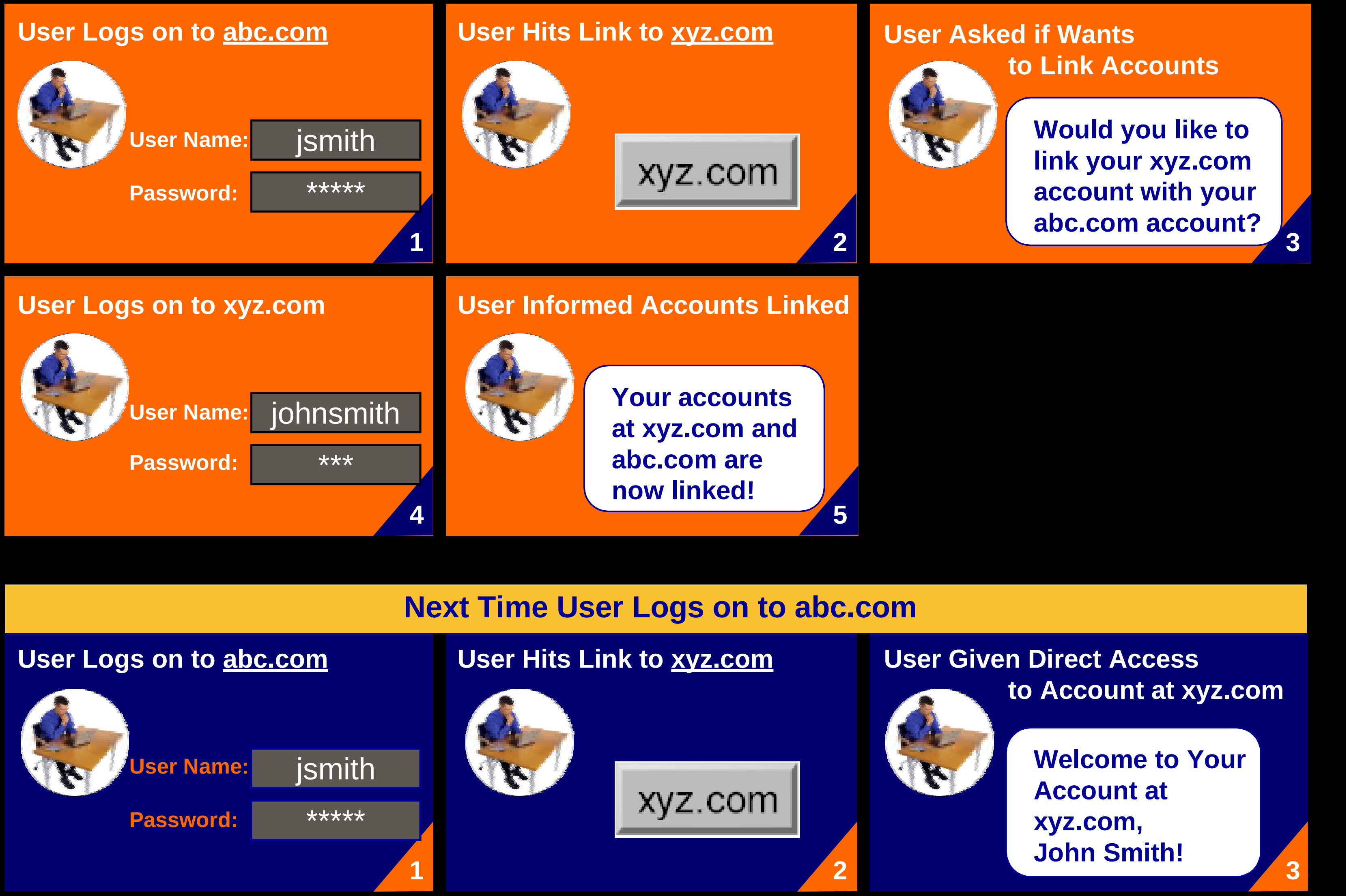
- **Enable Consumer Privacy:** Enable commercial and non-commercial organizations to protect consumer privacy

- **Support Interoperability:** Provide a mechanism supporting interoperability with existing systems, standards, and protocols

Version 1.0 Specifications Functionality

- **Opt-in account linking** – Users can link their accounts with different service providers within "circles of trust"
- **Simplified sign-on for linked accounts** – Once users' accounts are federated, they log-in, authenticate at one linked account and navigate to another linked account, without having to log-in again
- **Authentication context** – Companies linking accounts communicate the type of authentication that should be used when the user logs-in
- **Global log-out** – Once users log-out of the site where they initially logged in, the users can be automatically logged-out of all of the other sites to which they were linked
- **Liberty Alliance client feature** – Implemented on client solutions in fixed and wireless devices to facilitate use of Liberty version 1.0 specification

Sample Version 1.0 User Experience



Account Federation

1. User Logs on to abc.com

User Name: jsmith

Password: *****

2. User Hits Link to xyz.com

xyz.com

3. User Asked if Wants to Link Accounts

Would you like to link your xyz.com account with your abc.com account?

4. User Logs on to xyz.com

User Name: johnsmith

Password: ***

5. User Informed Accounts Linked

Your accounts at xyz.com and abc.com are now linked!

Next Time User Logs on to abc.com

Federated Simplified Sign-On

1. User Logs on to abc.com

User Name: jsmith

Password: *****

2. User Hits Link to xyz.com

xyz.com

3. User Given Direct Access to Account at xyz.com

Welcome to Your Account at xyz.com, John Smith!

Specifications: A Phased Approach

Version 1.0

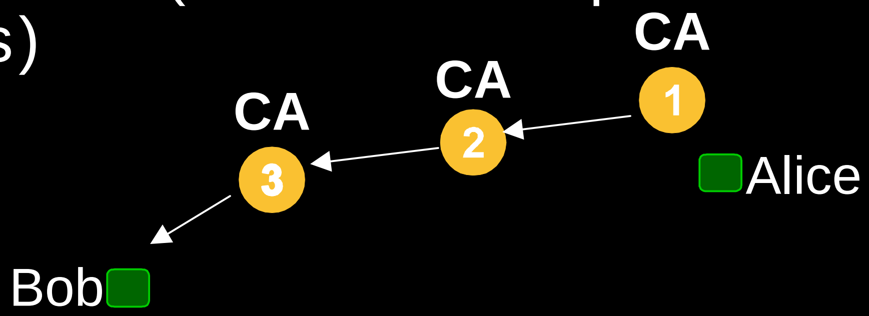
- Federated network identity
- Opt-in account linking and simplified sign-on within an authentication domain created by business agreements
- Security built across all the features and specifications

Future Versions

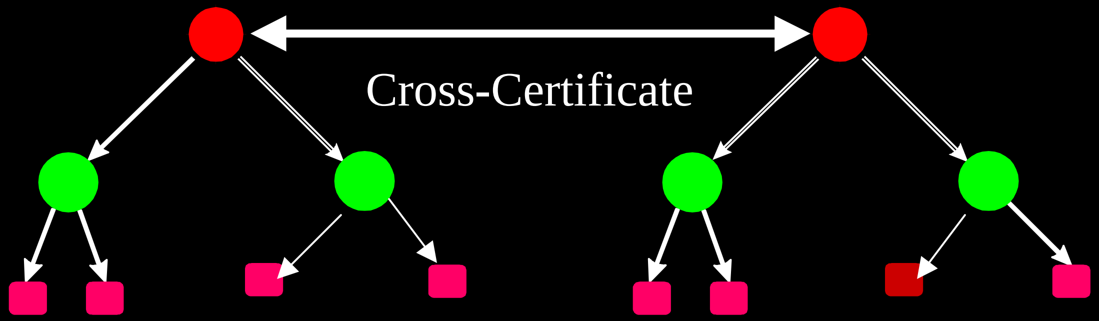
- Permissions-based attribute sharing
- Schema/protocols for core identity profile service
- Simplified sign-on across authentication domains created in version 1.0 by business agreements
- Delegation of authority to federate identities/accounts

Developing Trust

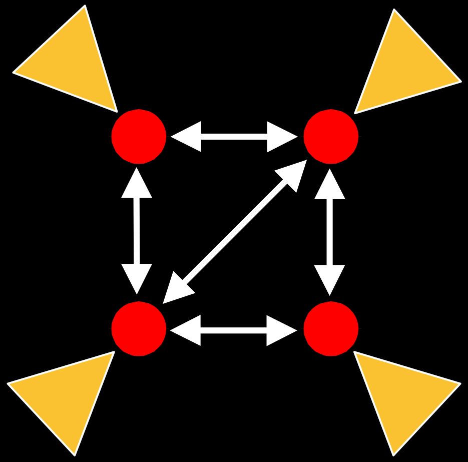
- Bob sends Alice an e-mail
- How does Alice know to trust it?
- Alice can verify Bob’s certificate by verifying a chain of certificates ending in one issued by a Certification Authority (CA) she trusts (and whose public key she knows)



Extending the idea

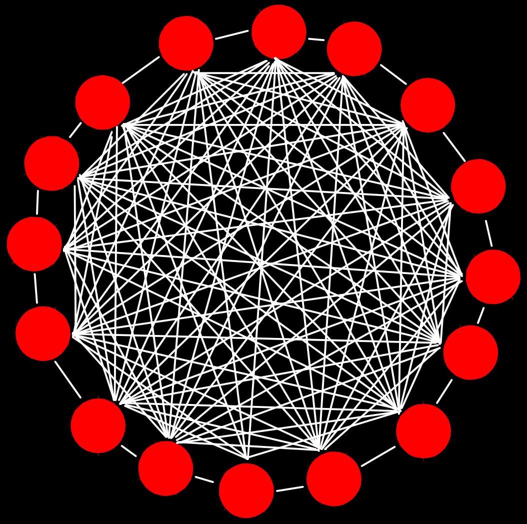


Allows PKIs to establish peer relationships



Can be managed when there are not many infrastructures

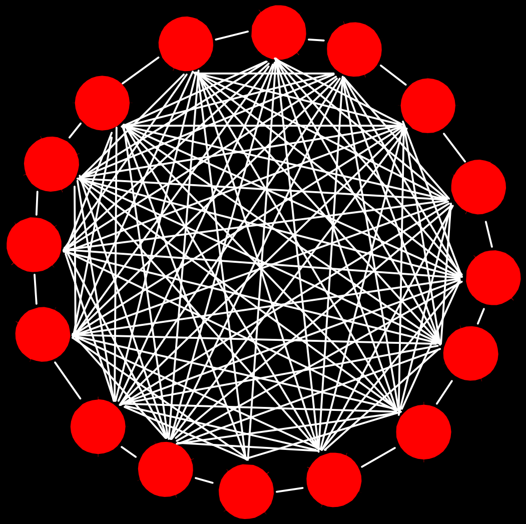
Management difficulty increases exponentially as more infrastructures are added



Copyright Entrust, Inc. 2002

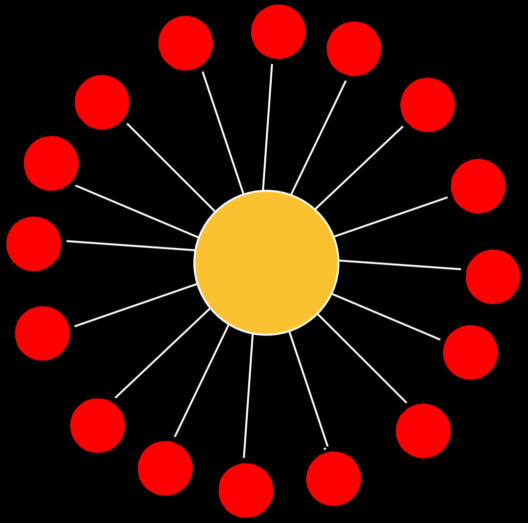
Extending the idea

We need to …



go from this unmanageable
environment

TO



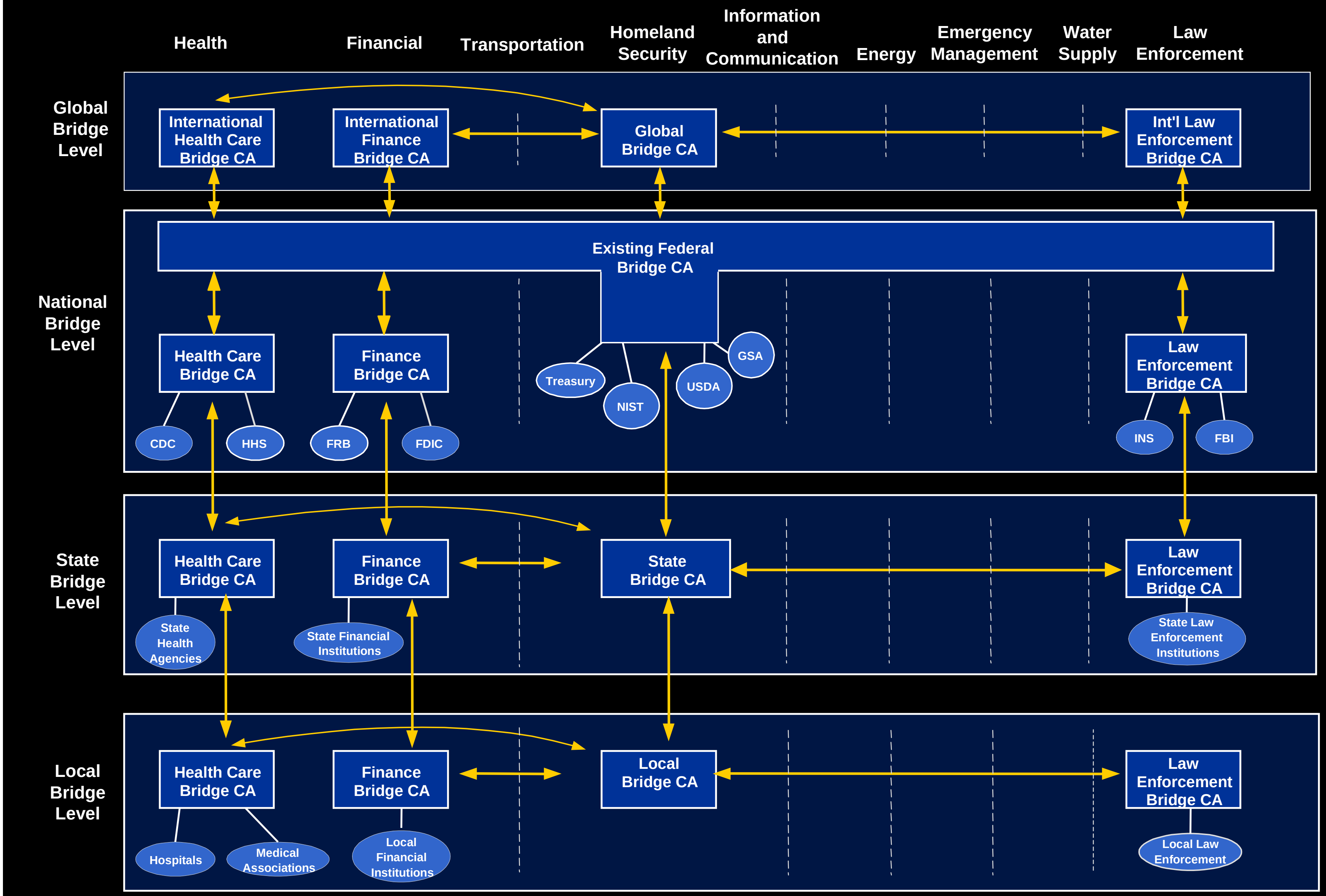
An easily MANAGED
environment

The Bridge CA

- A Bridge CA is a conduit for TRUST
- It is NOT a TRUST ROOT
  - There is no assertion of trust
- It is built upon the X.509 framework
- It is open and standards based

Linking up trusted environments

U.S. Example: National Cybersecurity Architecture



The security ‘flip’

- Change from deny first, open permissions selectively, to…
  - open everything, deny selectively
- Identify users, determine what they can see
- Protect the data and the transactions
- Audit for compliance to security policy

Summary

- Framework, interoperability, viability are no longer hurdles!
- PKI has evolved beyond the enterprise, large scale deployment now underway
- ROI: Leverage Metcalfe's law and get started