Session 027

Windows Server 2003: Under The Hood

Robert G. Nottoli, Principal Infrastructure System Architect

IBM @server xSeries Technical Conference

Aug. 9 - 13, 2004

Chicago, IL

RETURN TO INDEX

Agenda

- Vision and Value
- Under the Hood
  - IT Infrastructure
  - Application Platform
  - Information Worker Infrastructure
- Summary

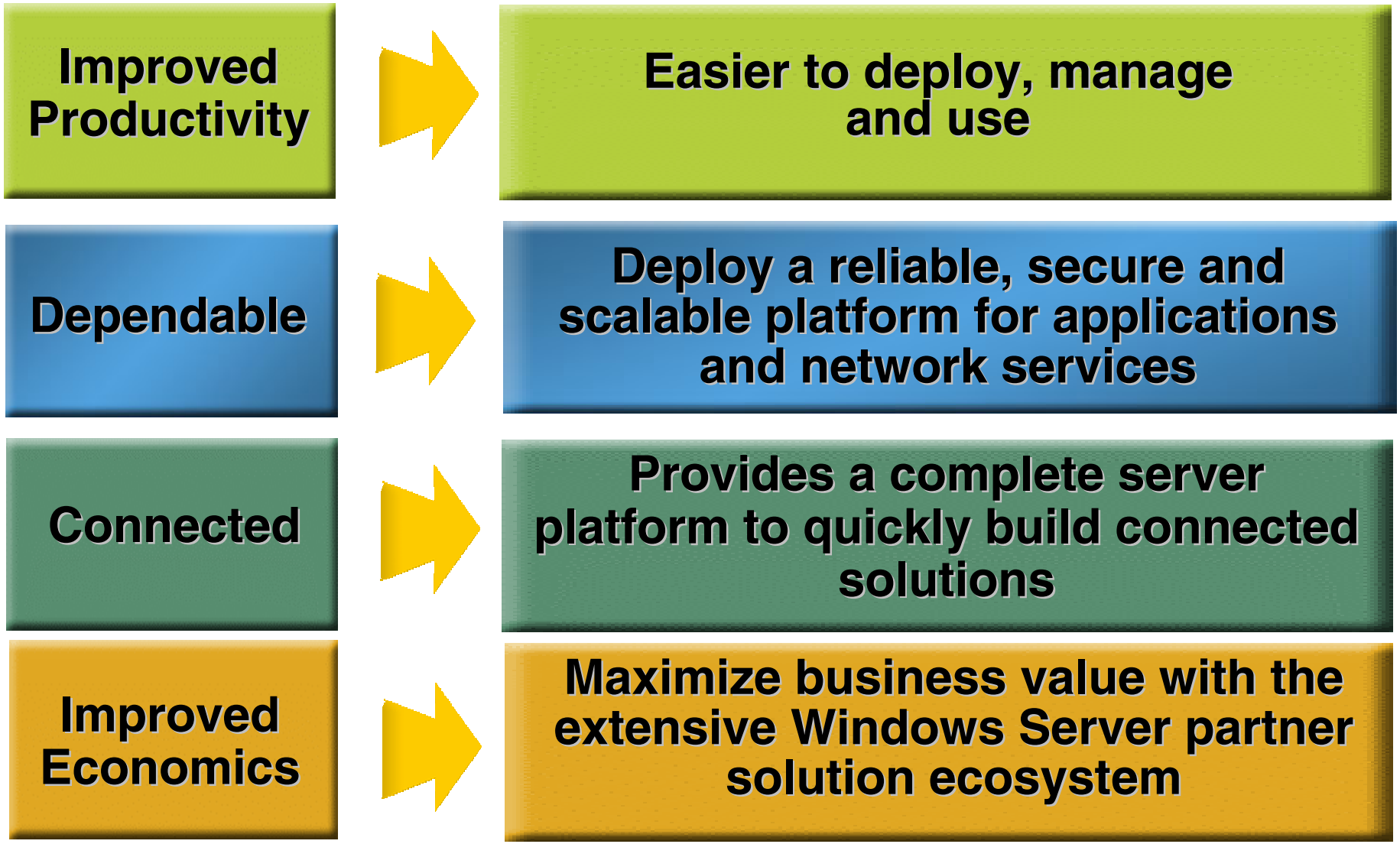
Windows Server Design Philosophy

Windows Servers designed for connecting people, technologies and businesses

A platform designed for developing, deploying and operating applications and services that federate seamlessly and scale extensively in every direction

Windows Server 2003

Designed with every end-user type in mind



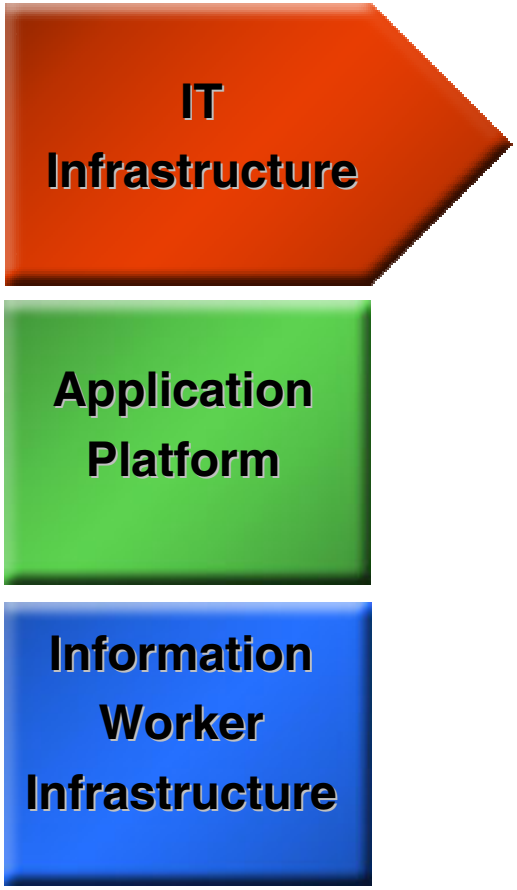
Under The Hood

Windows Server

Customer Driven Release

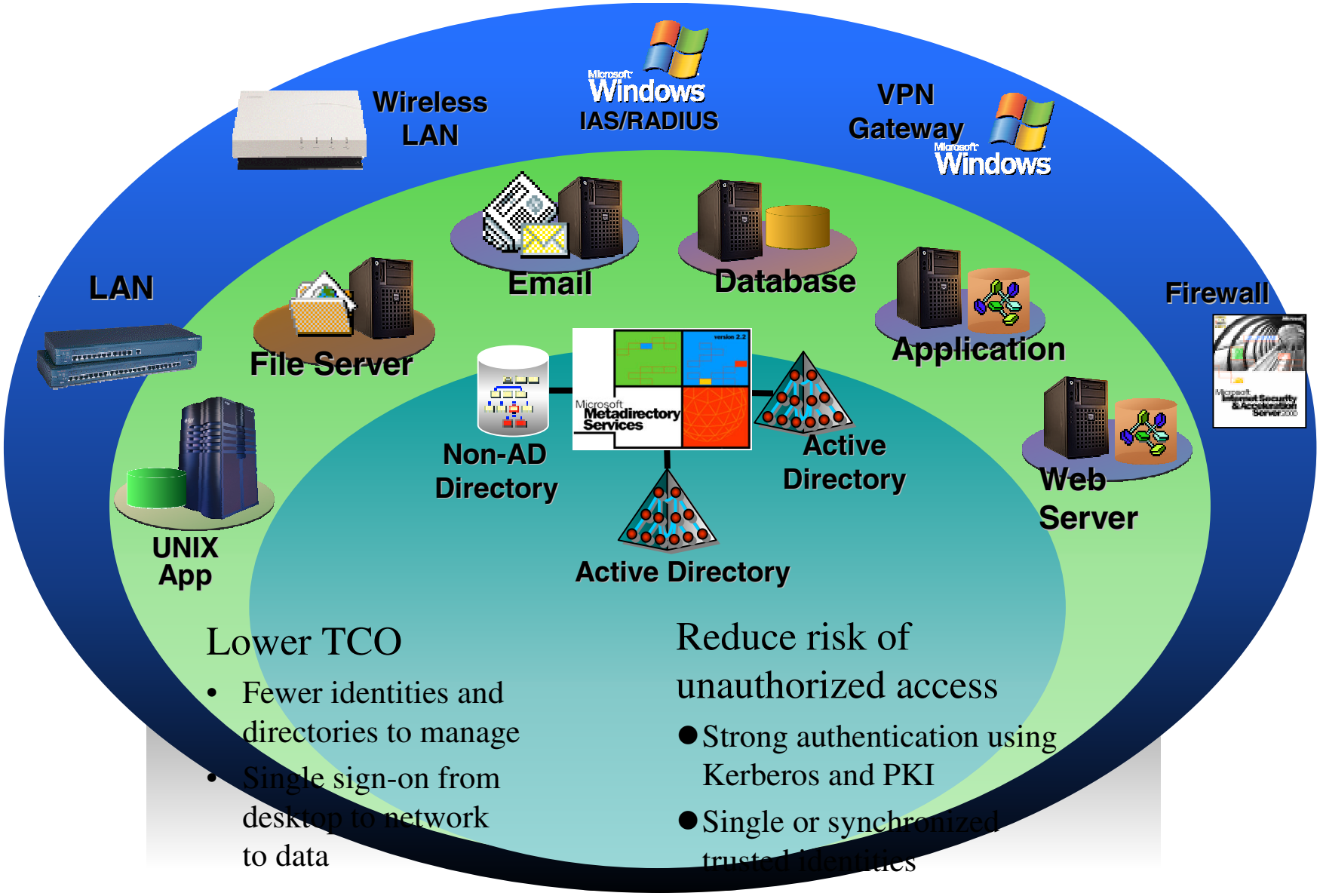
IT Infrastructure	■ Focus on Security, Reliability, Availability & Scalability ■ Flexible tools for identity management, deployment and use ■ Simplified and proactive management
Application Platform	■ Integrated Web Server platform ■ Develop, deploy and manage Web services ■ Standards-based integration
Information Worker Infrastructure	■ Protect/insulate end-users ■ Integrated Media Services ■ Infrastructure for managed Instant Messaging, User portals

IT Infrastructure Dependability Improvements



- **Improved Dependability**
  - Secure Connected Infrastructure
  - Patch Management
  - Server Consolidation
  - WSRM
- **Improved Productivity**
  - Active Directory enhancements
  - Policy and Automation
  - Guided Configuration
  - Intelligent File and Storage Services
- **Improved Connectivity**
  - Remote Access, VPN
  - Secure Mobile Access

Secure Connected Infrastructure



Lower TCO

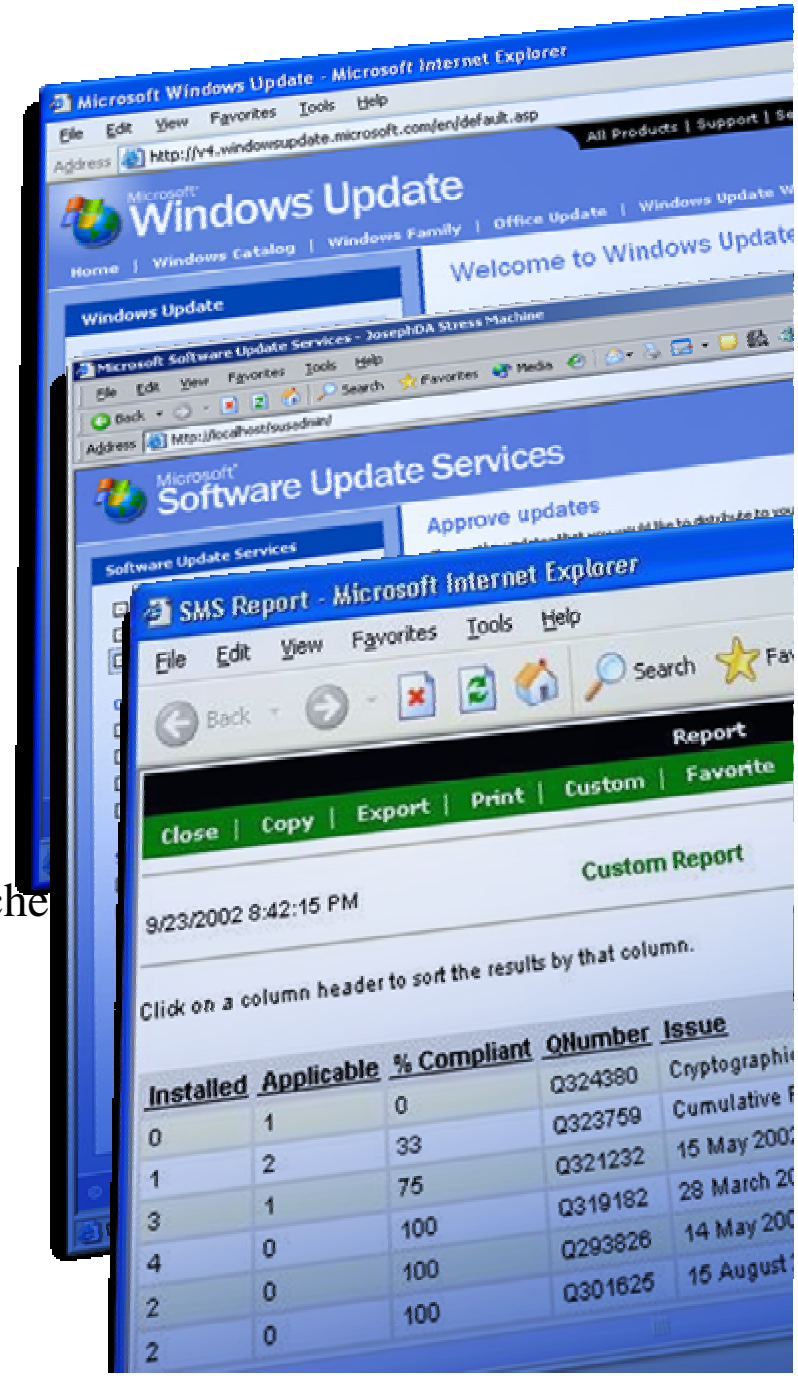
- Fewer identities and directories to manage
- Single sign-on from desktop to network to data

Reduce risk of unauthorized access

- Strong authentication using Kerberos and PKI
- Single or synchronized trusted identities

Patch Management And Software Distribution

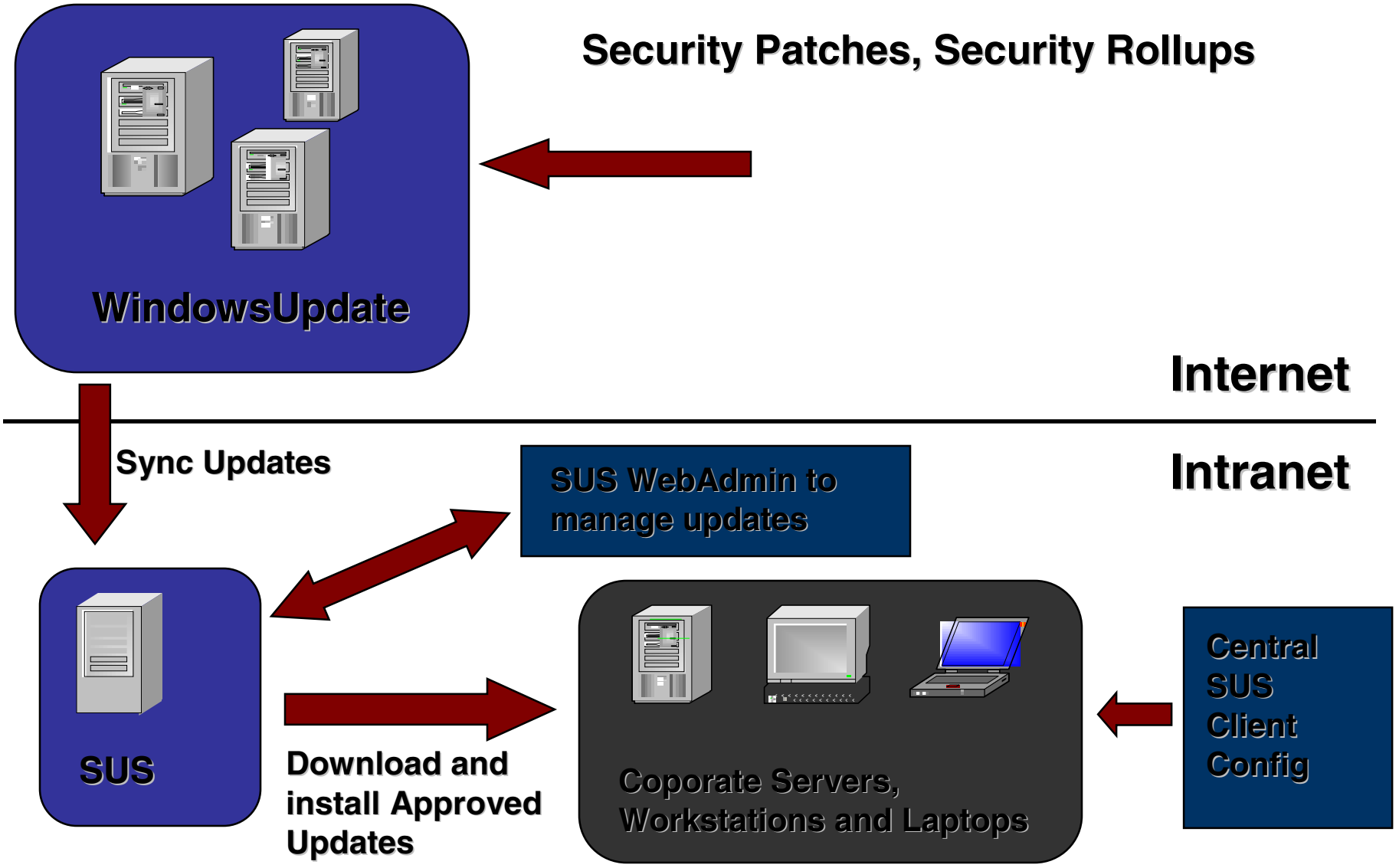
- Consumer and Small Business:
  Windows Update
  - User Initiated or Automated Updates
  - Access to all available updates
  - Deployment from Microsoft.com
- Medium Business:
  Software Update Services
  - Windows Update inside your firewall
  - Admin control over approval
  - Fire and forget for W2k/XP/WS03 security patche
  - Win2k/XP/WS03
- Enterprises:
  SMS 2003
  - Tailored already for large enterprises
  - Greater platform, content, and control



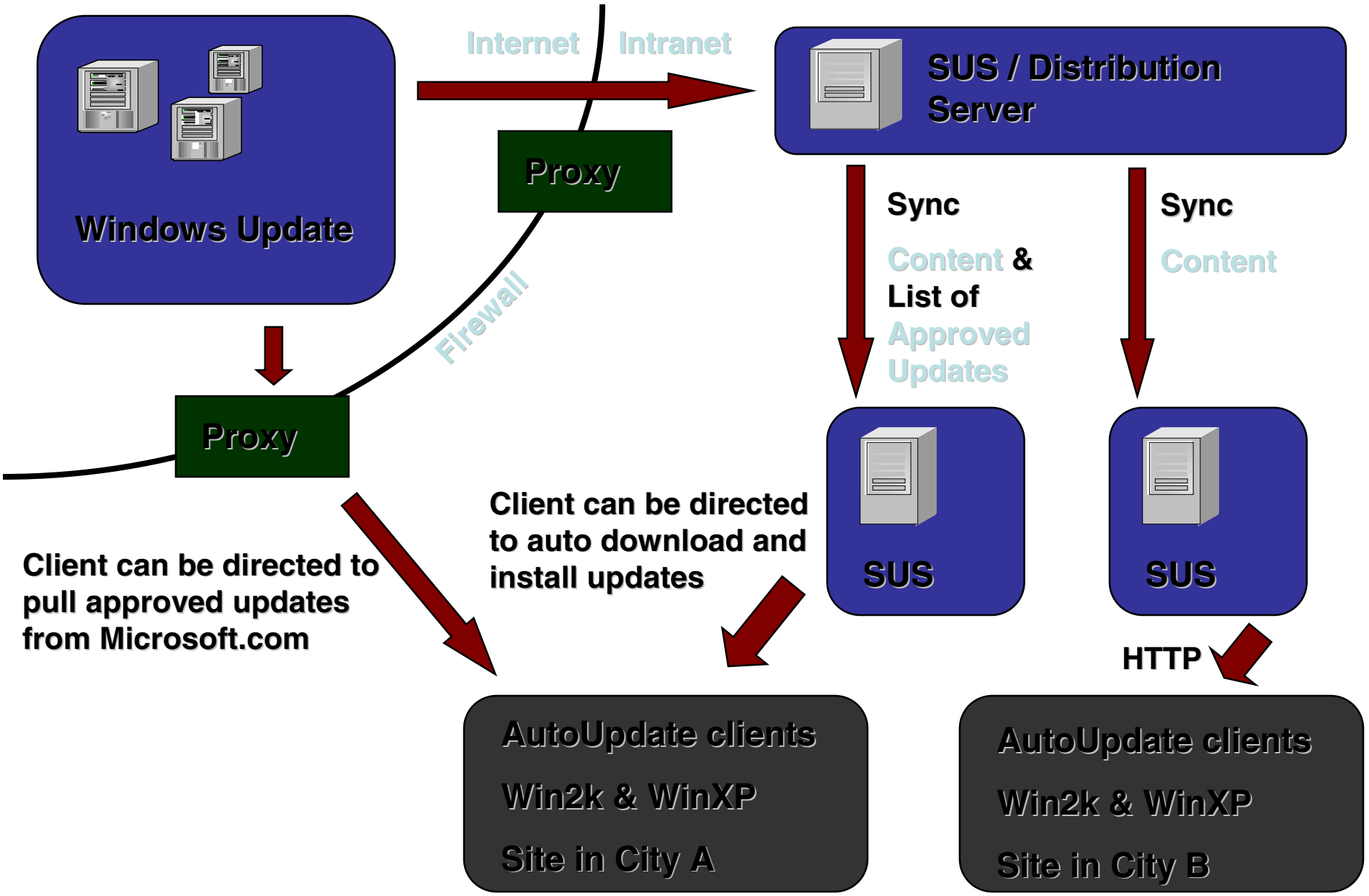
SUS 1.0 Details

- Support for:
  - Windows Update inside your firewall
  - Support for Windows 2K/XP/03 critical updates only
  - Basic Admin control
    - Which patches get distributed
    - Scheduling/reporting
    - Client configuration using Group Policy
- Not Supported:
  - Non-Windows updates (e.g. SQL, Exchange, Office)
  - 3rd party update publishing
  - Full app distribution
  - Driver deployments
  - Public API's for programmatic access
- Client (based on WinXP AutoUpdate)
  - Check corporate or public WU for updates
  - Can be configured centrally by Administrator
  - Can auto-download and install updates under admin control
- Server (SUS Server)
  - Hosted on the corporate intranet
  - Synchronization service with public WU
  - Administrator control over updates that can be deployed

Architecture:

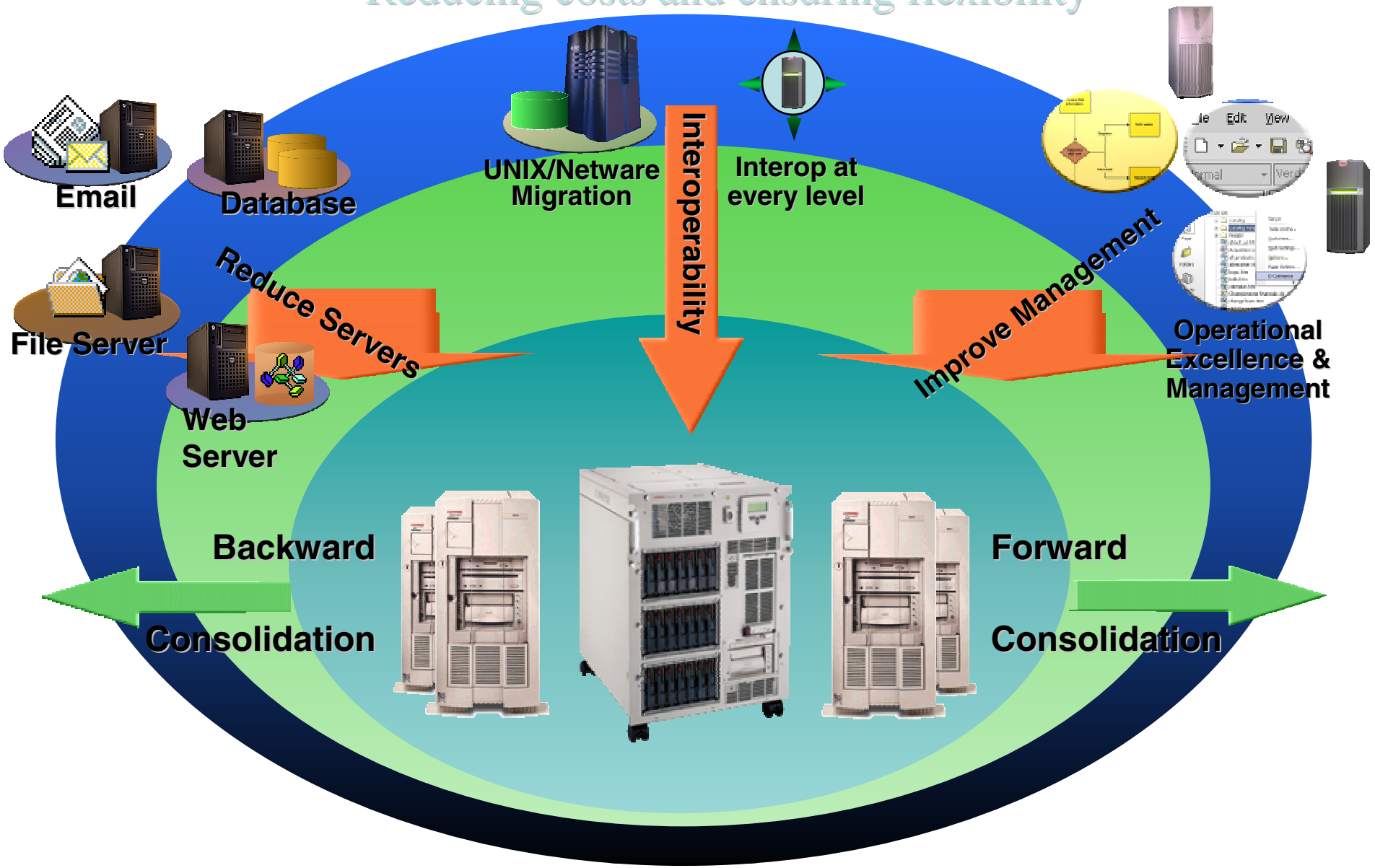


SUS Server Scale-out



Server Consolidation

Reducing costs and ensuring flexibility



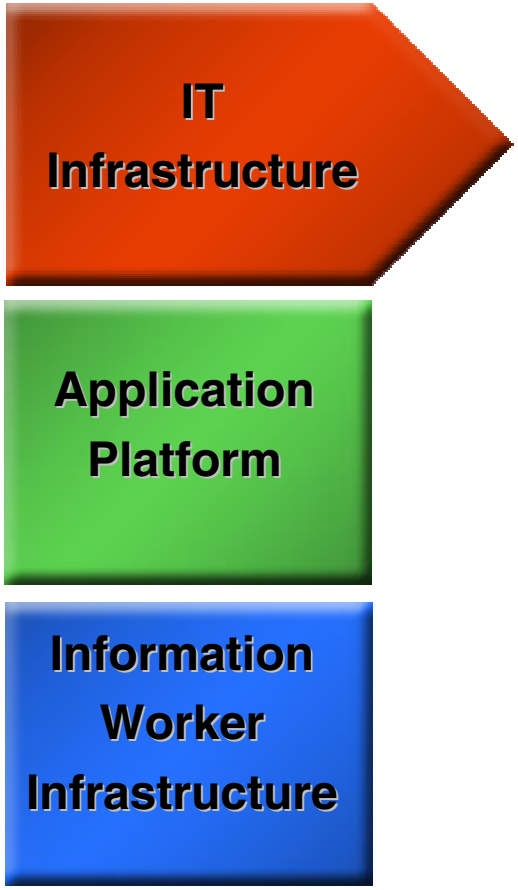
Server Consolidation Enhancements

- Server can be virtualized by CPU and memory boundaries
  - Windows Resource Manager (WRM) add-on
- Multiple applications co-exist easily
  - Side by Side DLLs
  - Web server process isolation
- Availability features
  - Hot Add memory, memory mirroring
- Scalability Features
  - Multi-path I/O
  - NUMA Support, Hyperthreading
  - Significant TPC-C progress
- Support for new, large server machines

demo

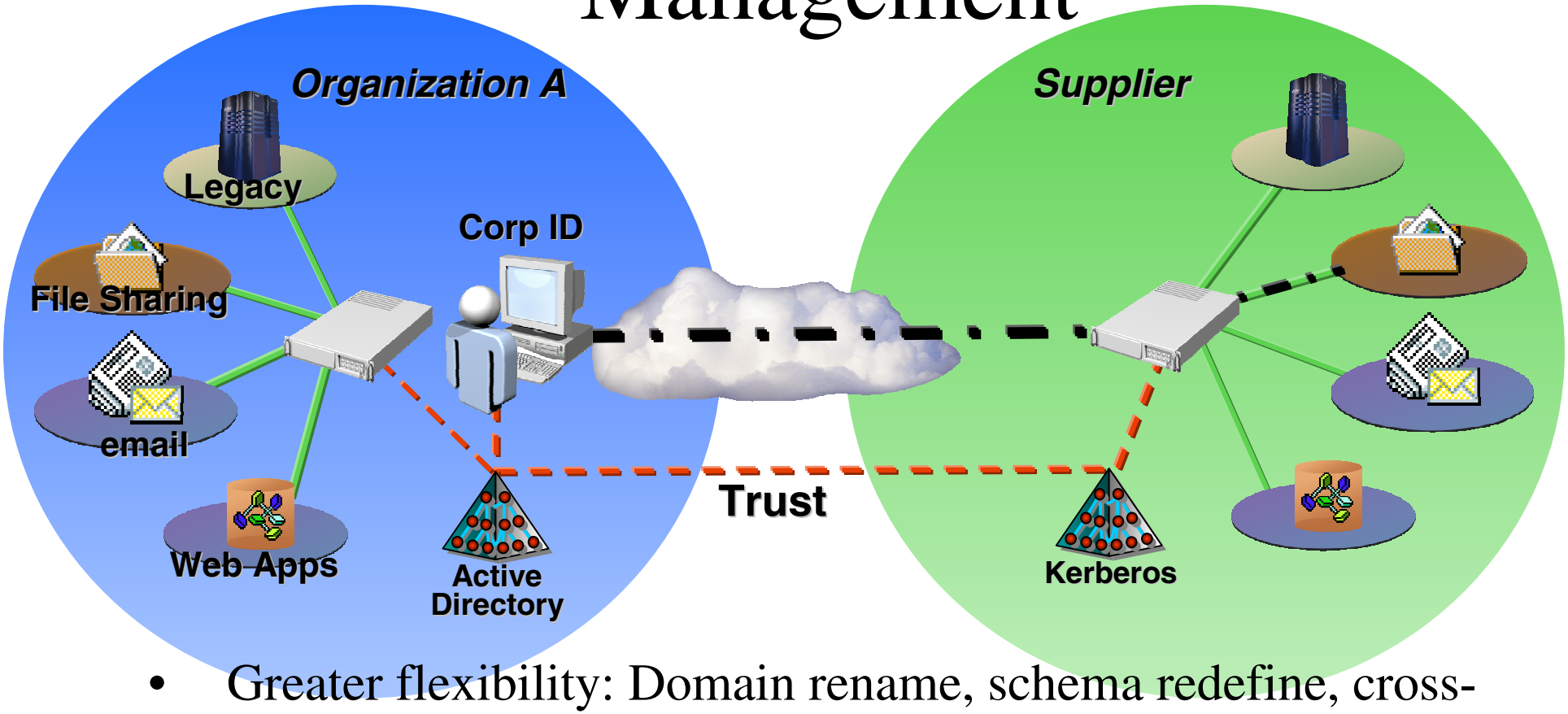
WSRM

IT Infrastructure Productivity Improvements



- **Improved Dependability**
  - Secure Connected Infrastructure
  - Reliability and Availability
  - Scalability
  - Server Consolidation
- **Improved Productivity**
  - Active Directory enhancements
  - Group Policy
  - Automated Management
  - Intelligent File and Storage Services
- **Improved Connectivity**
  - Remote Access, VPN
  - Secure Mobile Access

Improved Active Directory Identity Management



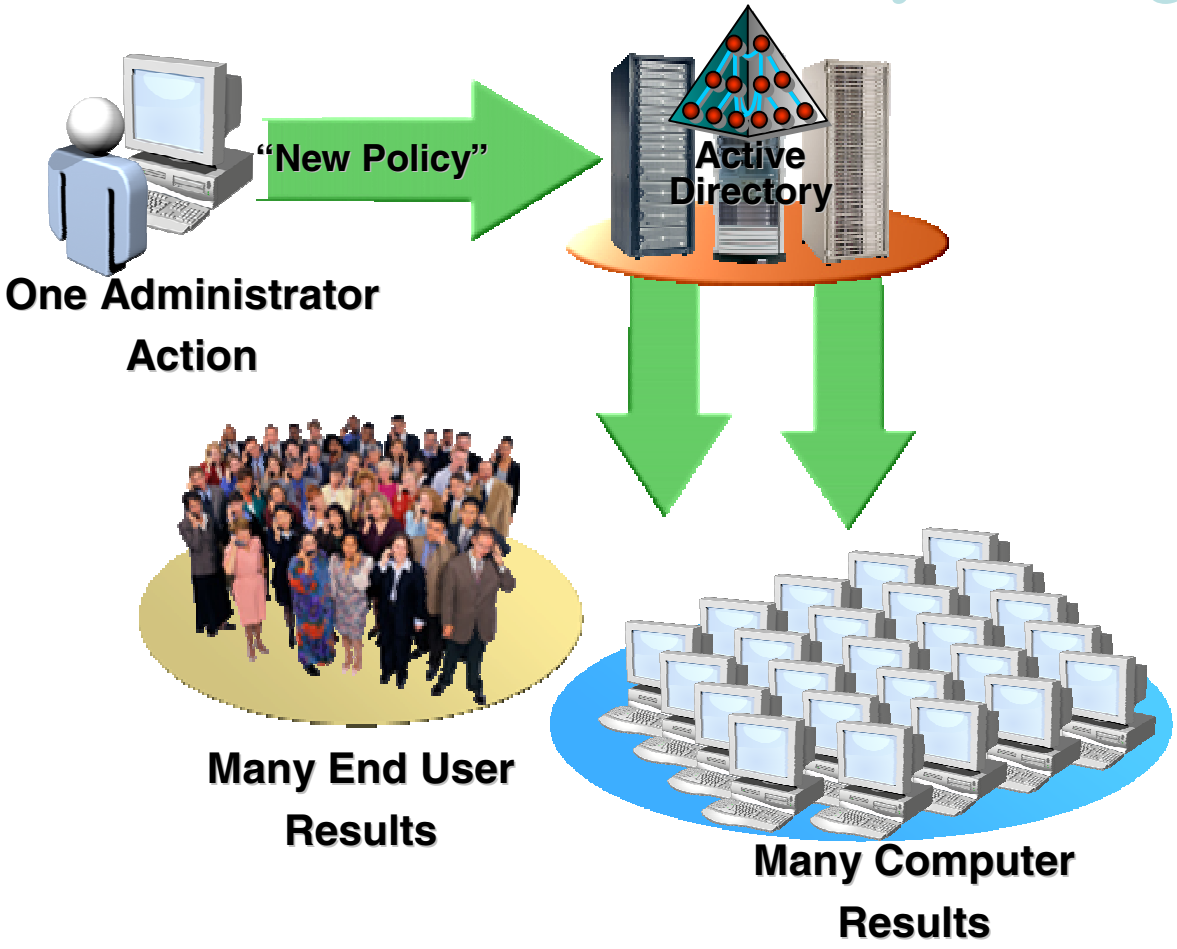
- Greater flexibility: Domain rename, schema redefine, cross-forest trust
- Increased performance and scale
- Enhanced LDAP support

Active Directory Enhancements

- Flexibility
  - Domain rename
  - Design easier via cross-forest trust
  - New migration tool (including passwords)
  - Can now redefine schema
- Management
  - Credential management
  - Better health monitoring
  - Improved interfaces
- Scale and Performance
  - Faster login for branch offices
  - Improved replication
  - LDAP performance enhancements

Group Policy

One-to-Many Management



Solution: Group Policy

- **Policy work for the admin to mass-customize the desktop experience**
- **New Group Policy Management Console (GPMC) makes it much easier to do**

Key Benefits:

- **Reduces admin, support, training requirements**
- **Increased user productivity**
- **Allows for mass-customization – scalability without sacrificing flexibility to customize**

Group Policy Enhancements

- Scope
  - More pre-defined policies
  - Cross-forest support
  - Deploy more effectively
- Machine Independence
  - Enhanced folder redirection
  - Improved roaming
- Management
  - New management console (GPMC)
  - Better visibility into policy results

Group Policy Management Console

Group Policy is a powerful application of Active Directory

- New admin tool with Windows Server
- Key improvements for administrators:
  - Improved User Interface
    - Based on how customers use Group Policy
  - New capabilities for rapid deployment of policy
    - backup/restore
    - import/export, copy/paste GPO
  - Scripting of GPO operations (Note: not settings within GPO)
    - Enables customization and automation
  - Support for Staging
    - First create in sandbox test environment
    - Replicate to production

demo

GPMC

Automated Management Enhancements

- Automation
  - Command line and scripting
  - Intelligent control through WMI
- Install and Updates
  - Guided configuration wizards
  - Remote Installation Services
  - Automated updating
- Flexibility
  - Lights out support
  - Emergency management
  - Better server event tracking and reporting

Automated Deployment Services

A fast, flexible platform for large scale server deployment and administration

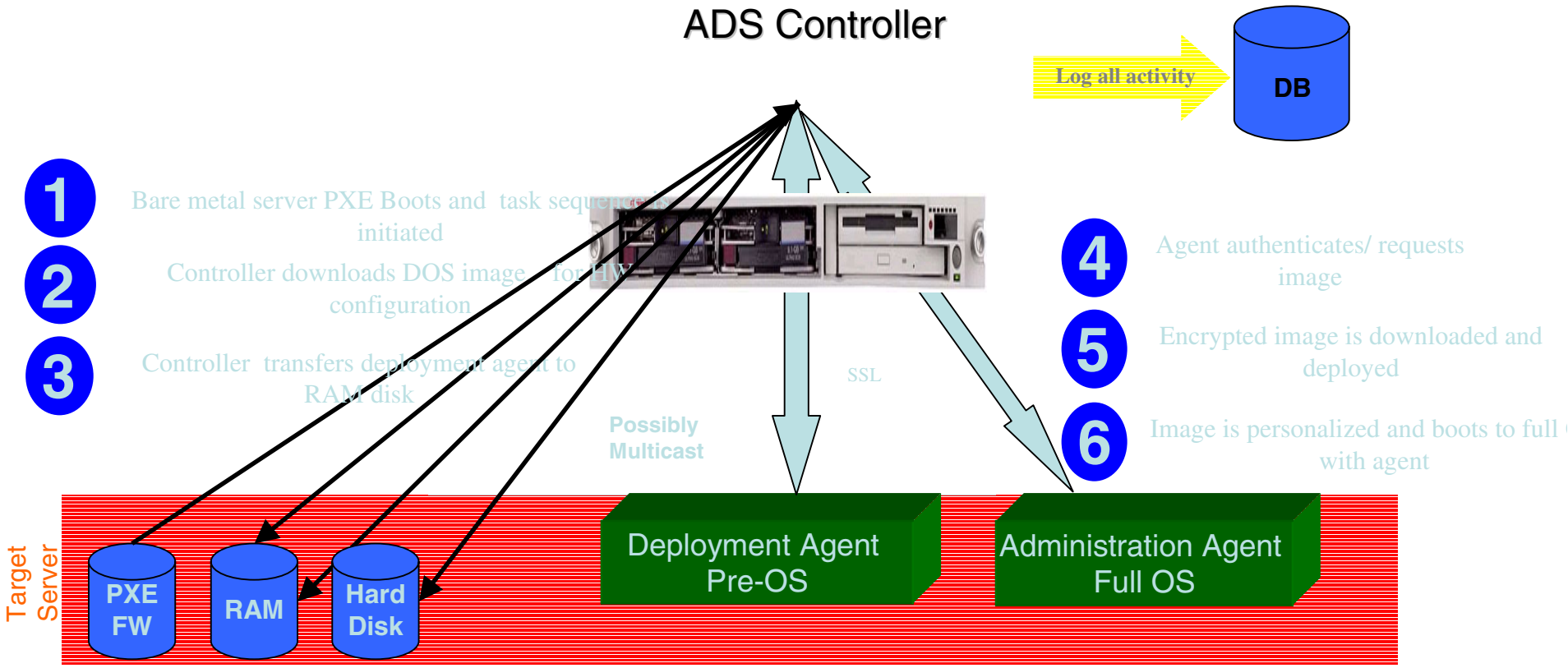
- Imaging and Deployment Engine
  - Speed of traditional imaging with added flexibility
  - Microsoft developed Imaging tools and format
    - Intelligent compression → smaller image size
    - Increased flexibility with on-the-fly image editing
    - Supports imaging of W2K and WS03 servers
  - Secure, remote deployment framework
    - Headless PXE support
    - Lightweight Pre-OS deployment agent
    - Extensible framework for customization
- Reliable Remote Execution
  - Centralized scripting of an entire server farm
  - A persistent log of all administrative activities
- Versatile set of User Interfaces
  - MMC UI for point and click operation
  - Rich programmatic interface for automation

Key Benefits Of ADS

1. **Lower the TCO associated with bare metal server builds and script-based administration**
   - **Enable zero-touch server builds from bare metal**
   - **Secure script based administration of 1000 servers as easily as 1**
2. **Improve the consistency, security and scalability of your Windows Server datacenter**
   - **Encode operational best practices and eliminate human error**
   - **Maintain a persistent store of all administrative activities**
   - **Centrally perform secure, script-based administration of your entire Windows datacenter**
   - **Rapidly change server role in response to changes in workload requirements**
3. **Leverage your existing server administration investments**
   - **Extend and enhance your existing script-based automation methodologies**

ADS Secure, Remote Imaging

'Zero Touch Server Builds from Bare Metal'

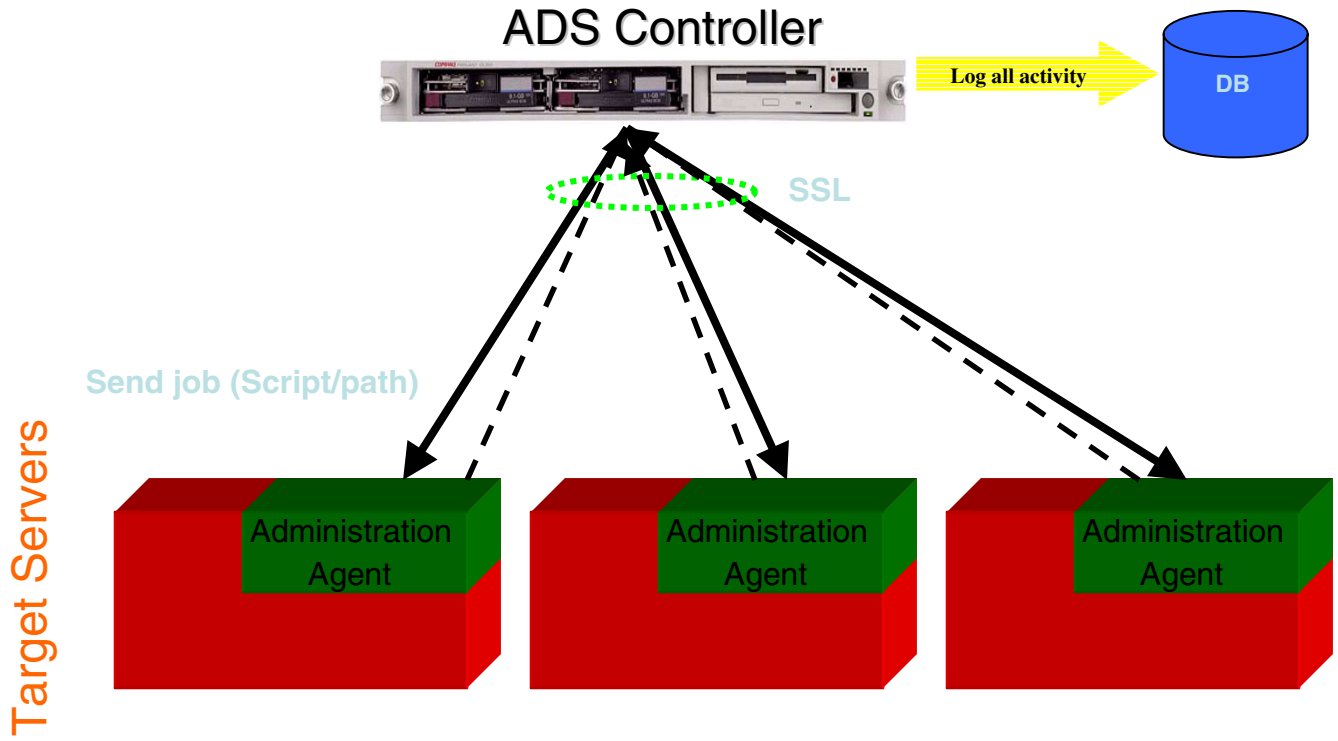


ADS Administration

'Secure script-based administration on 1000 servers as easily as 1'

1. Initiate script-based administration on thousands of servers from the central controller

2. Gather all output from task and store in database



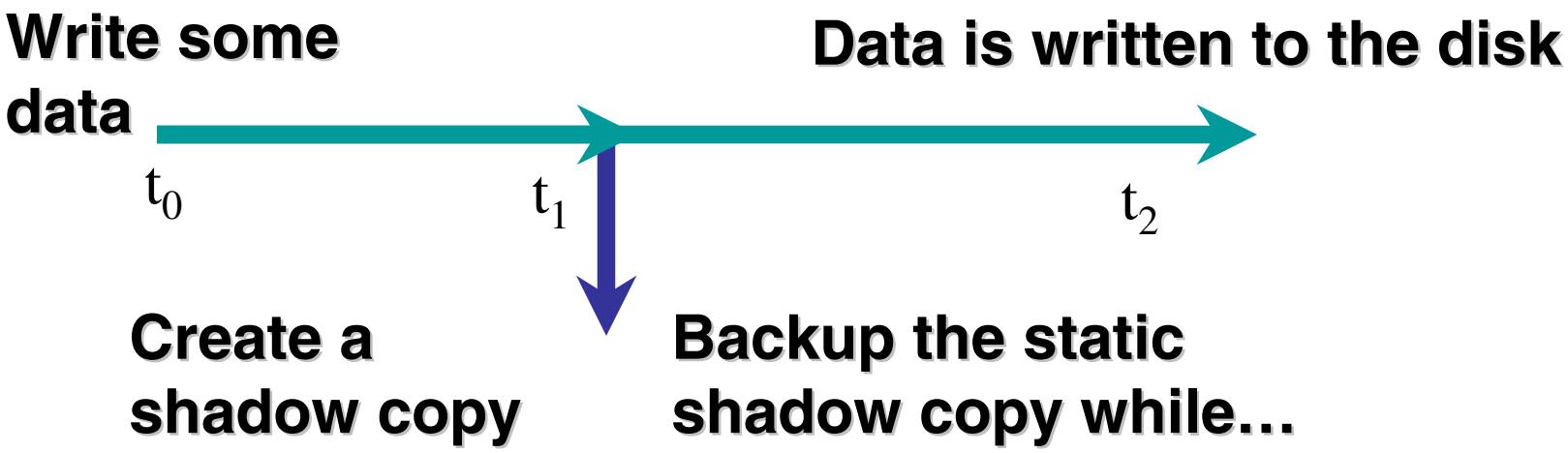
Intelligent File And Storage

Enhancements

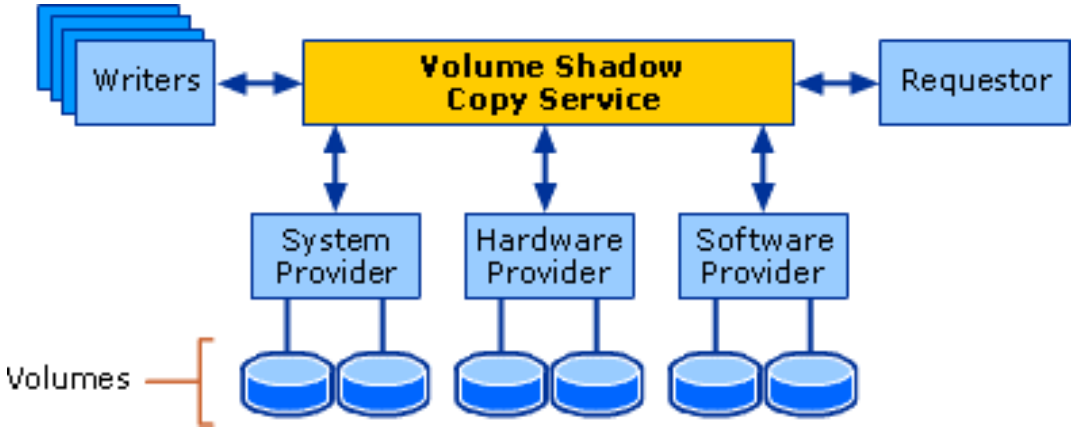
- Access
  - Distributed File System flexibility
  - SAN enhancements
  - iSCSI support
- Performance
  - 100-139% performance gains over Windows 2000
  - Multi-path I/O
- Administration
  - Versioning via Volume Shadowcopy Services
  - End user file recovery via Previous Versions
  - Automated System Recovery

What Is A Shadow Copy?

- Data “Snapshot”
- Infrastructure for creating a point-in-time copy of a single volume or multiple volumes
- Appears static, even though the original data is changing



Volume Shadow Copy Service Architecture



Component	Description
Volume Shadow Copy service	A service that coordinates various components to create consistent shadow copies of a volume.
Requestors	A process that requests that a volume shadow copy be taken. A backup application is an example.
Writers	A component of an application that stores persistent information on one or more volumes that participates in shadow copy synchronization. Typically, this is a database application like SQL Server or system service like Certificate Services.
Providers	An interface that creates and maintains the shadow copies.
Source volume	The volume that contains the data to be shadow copied.
Storage volume	The volume that holds the shadow copy storage files for a copy-on-write software provider.

demo

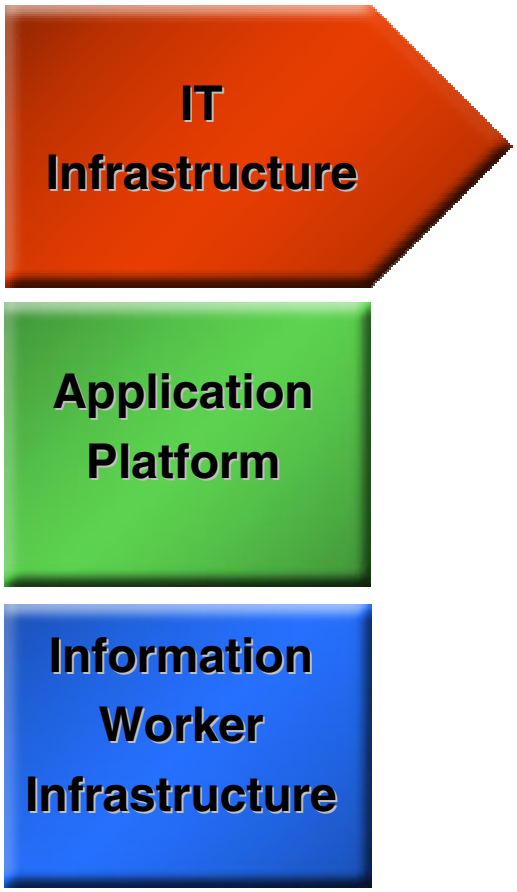
VSS

Intelligent File And Storage

Volume Shadowcopy Benefits

- Fewer help desk calls due to user self-service recovery
- Open File Backup
- No more “Backup Window”
  - Applications continue to run while backup runs against snapshot
- Applications register “how to be backed up and restored”
- “Data Freighting:” Clone volumes and move them to other hosts on a SAN

IT Infrastructure Connectivity Improvements

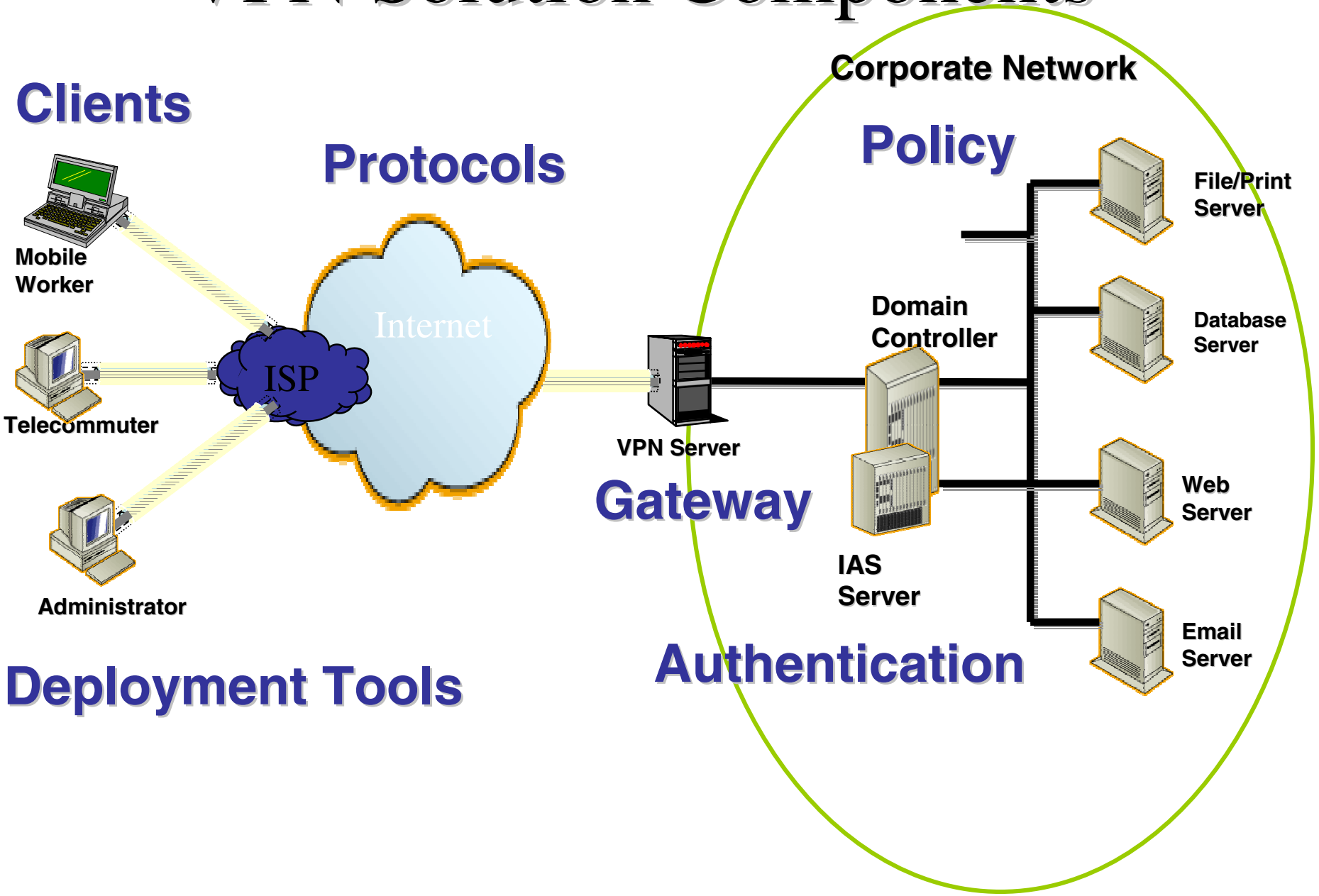


- **Improved Dependability**
  - Secure Connected Infrastructure
  - Reliability and Availability
  - Scalability
  - Server Consolidation
- **Improved Productivity**
  - Active Directory enhancements
  - Policy and Automation
  - Guided Configuration
  - Intelligent File and Storage Services
- **Improved Connectivity**
  - Remote Access, VPN
  - Secure Mobile Access

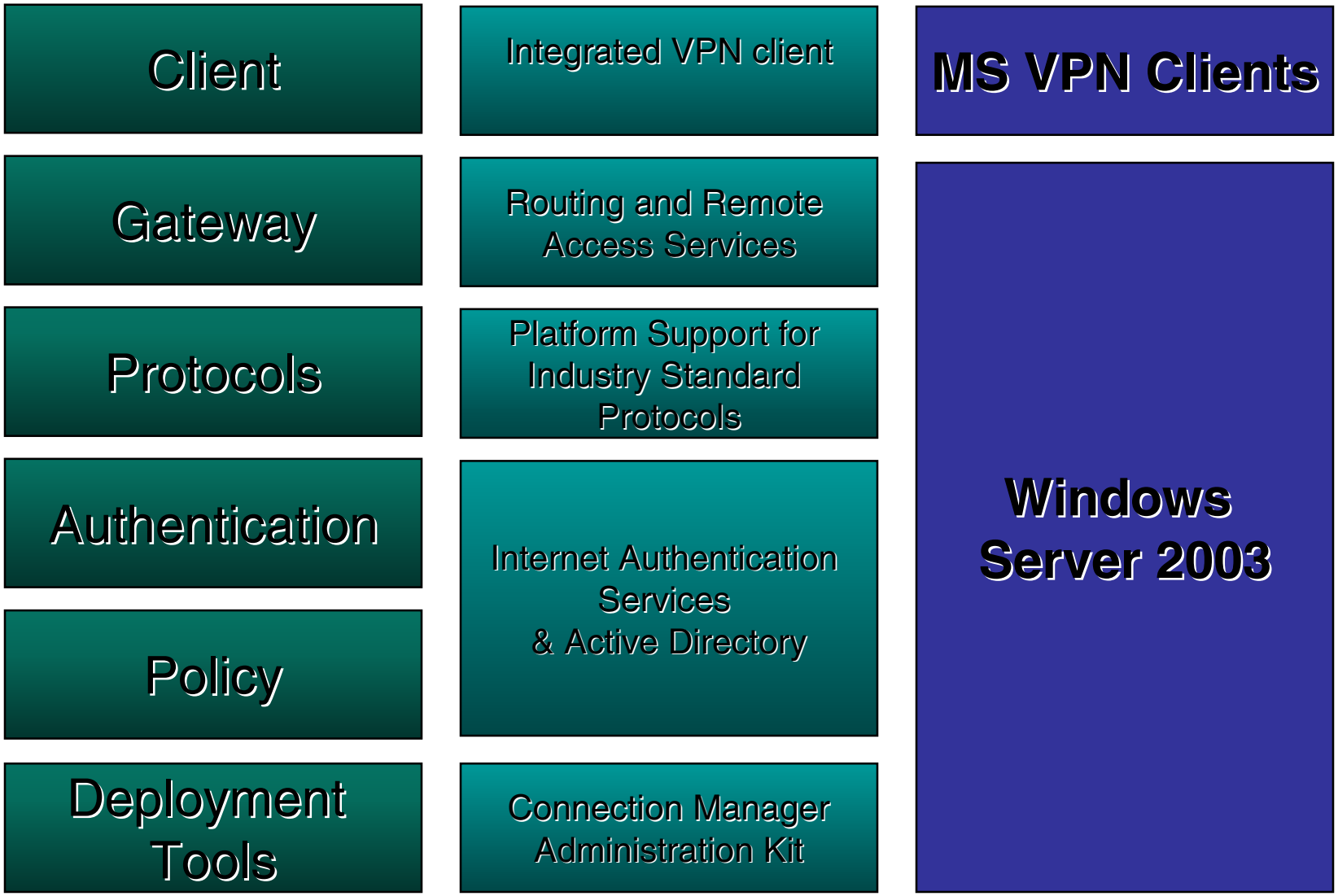
Connectivity Improvements

- Remote Access
  - RADIUS failover, proxy and load balancing
- VPN
  - Quarantine
  - Over Network Address Translation (NAT)
  - Load balancing enabled
- Wireless
  - Passwords over 802.1x
  - Faster roaming and re-authentication

VPN Solution Components



Windows VPN Solution



VPN Solution Components

Microsoft VPN Clients

- Client
- Gateway
- Protocols
- Authentication
- Policy
- Deployment Tools

Integrated VPN Clients

- **L2TP/IPSEC with NAT-T**
  - **Windows Server 2003**
  - **Windows XP**
  - **Windows 2000 (all flavors)**
- **PPTP**
  - **Windows Server 2003/Windows XP**
  - **Windows 2000**
  - **Windows NT 4.0**
  - **Windows ME, 98**

Add on Client

- **L2TP/IPSEC client for Win9x, NT4.0**
  - **Available on the Web**
  - **Includes NAT-T support**

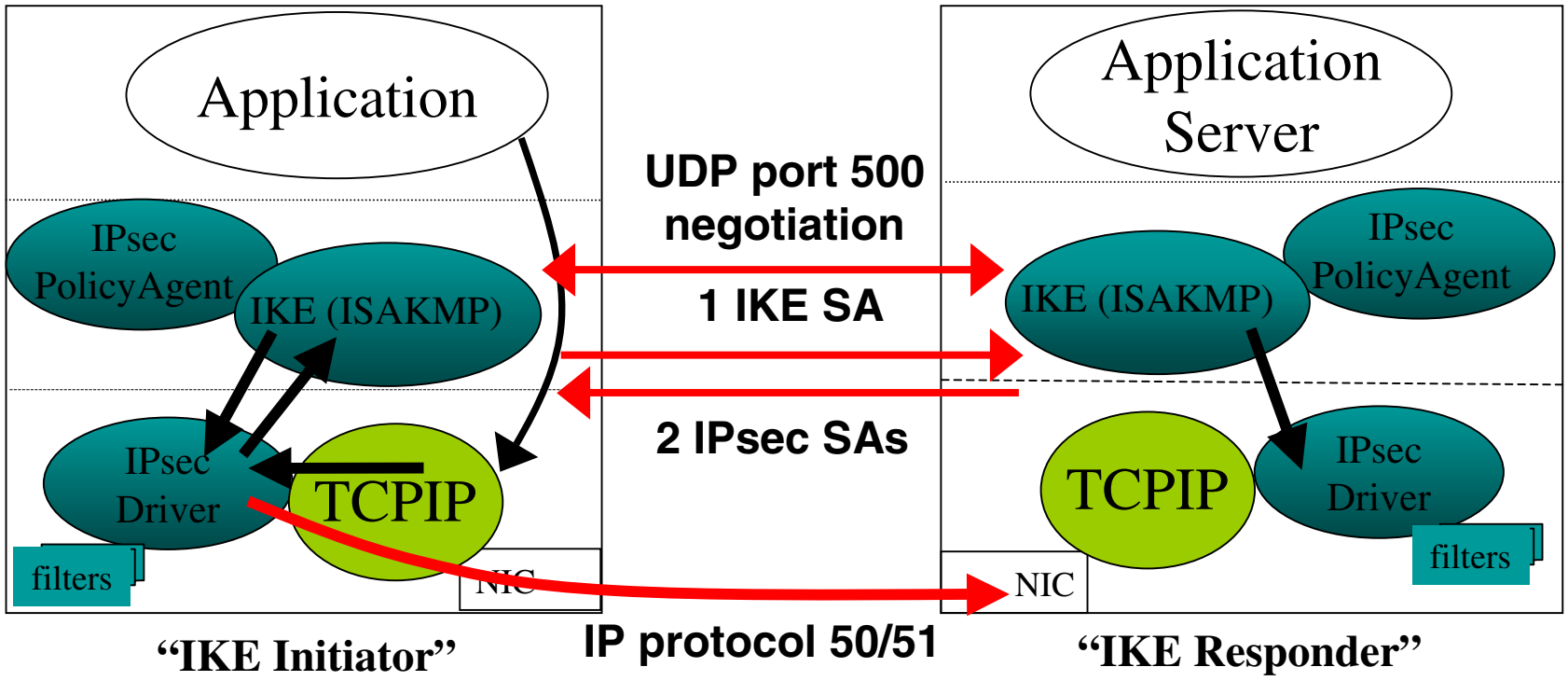
IPsec Overview

- Network security problems
  - Inside vs outside
  - Sensitive data protection
- Privacy, Integrity & Authenticity
- Four good reasons
  1. Encryption
  2. Hashes prevent modification
  3. Transport level machine authentication
  4. Fewer firewall holes
- IETF standard implementation
  - AH/ESP, IKE

IPSec Deployment Guidance

- Recommended Scenarios
  - Packet filtering
  - Securing host-to-host traffic on specific paths
  - Securing traffic to specific servers
  - L2TP/IPsec tunneling for VPN connections
  - Tunnel mode supported for site-to-site
    - Prefer L2TP/IPSec Tunnel
- Scenarios not recommended
  - Domain member to DC
  - IPSec for the entire network

How IPsec works



- Internet Key Exchange (IKE) - Identity Protect Mode – defined in RFC 2409
  - Phase 1 "Main Mode" establishes IKE SA – trusted channel between systems, negotiation establishes encrypted channel, mutual trust, and dynamically generates shared secret key ("master" key)
  - Phase 2 "Quick Mode" establishes IPsec SAs – for data protection, one SA for each direction identified by packet label (SPI), algorithms and packet formats agreed, generates shared "session" secret keys derived from "master" key

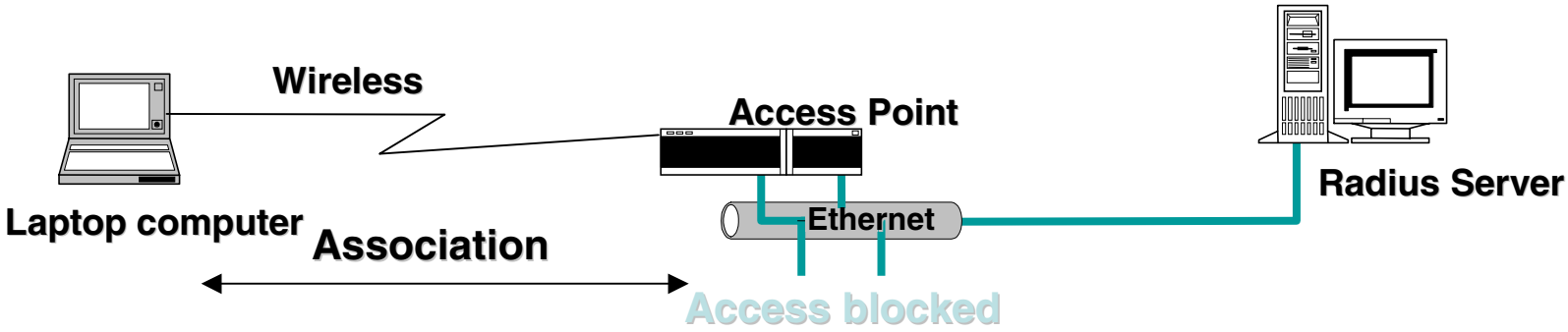
IPsec In Windows Server 2003

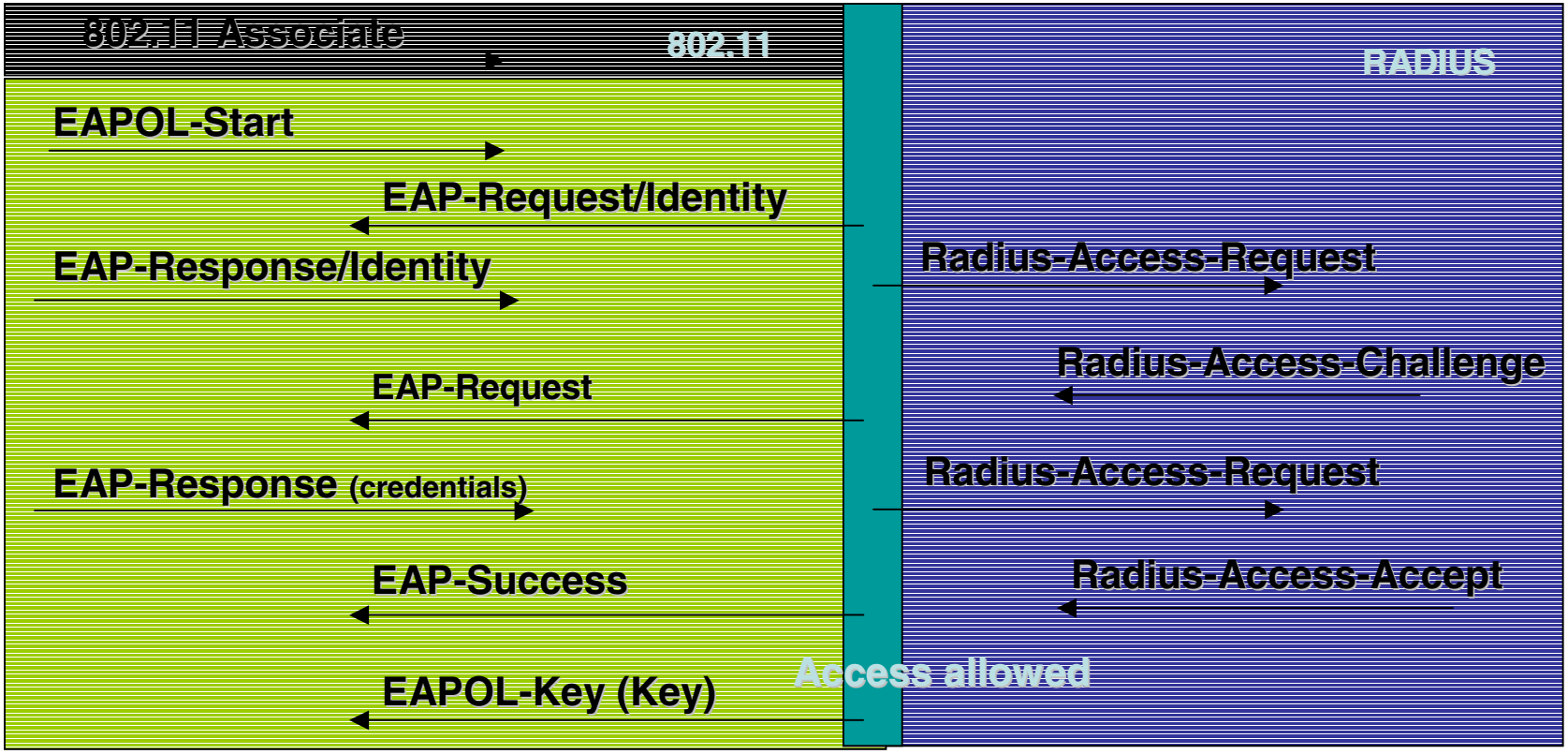
- NAT traversal
- NLB + IPSec Support (Load-Balancing)
- Cluster (MSCS) + IPSec Support (Failover)
- Full command line support (netsh)
- RSOP Support for group policy
- Faster and Improved Filtering
- “Access this Computer from Network” Authorization
- Security enhancements
  - DH-2048 in IKE
  - Boot time security
  - Failsafe Policy Processing
  - No Default Exemptions for Kerberos

IEEE 802.1X

- Standard protocol for authenticated network access
- Supported on Ethernet and 802.11
- User and machine authentication using Radius
  - Same as used for dial-up and VPN authentication
  - Windows 2000 Internet Authentication Server can be integrated with Active Directory user database
- Level of network access is under admin control (RAP)
  - No access (don't even get an IP address)
  - Complete access
  - Guest access
- Supports distribution and refresh of encryption keys to clients to defeat well known attacks
- Supports Certificates (TLS) and Password (PEAP)

802.1X On 802.11





VPN Solution Components

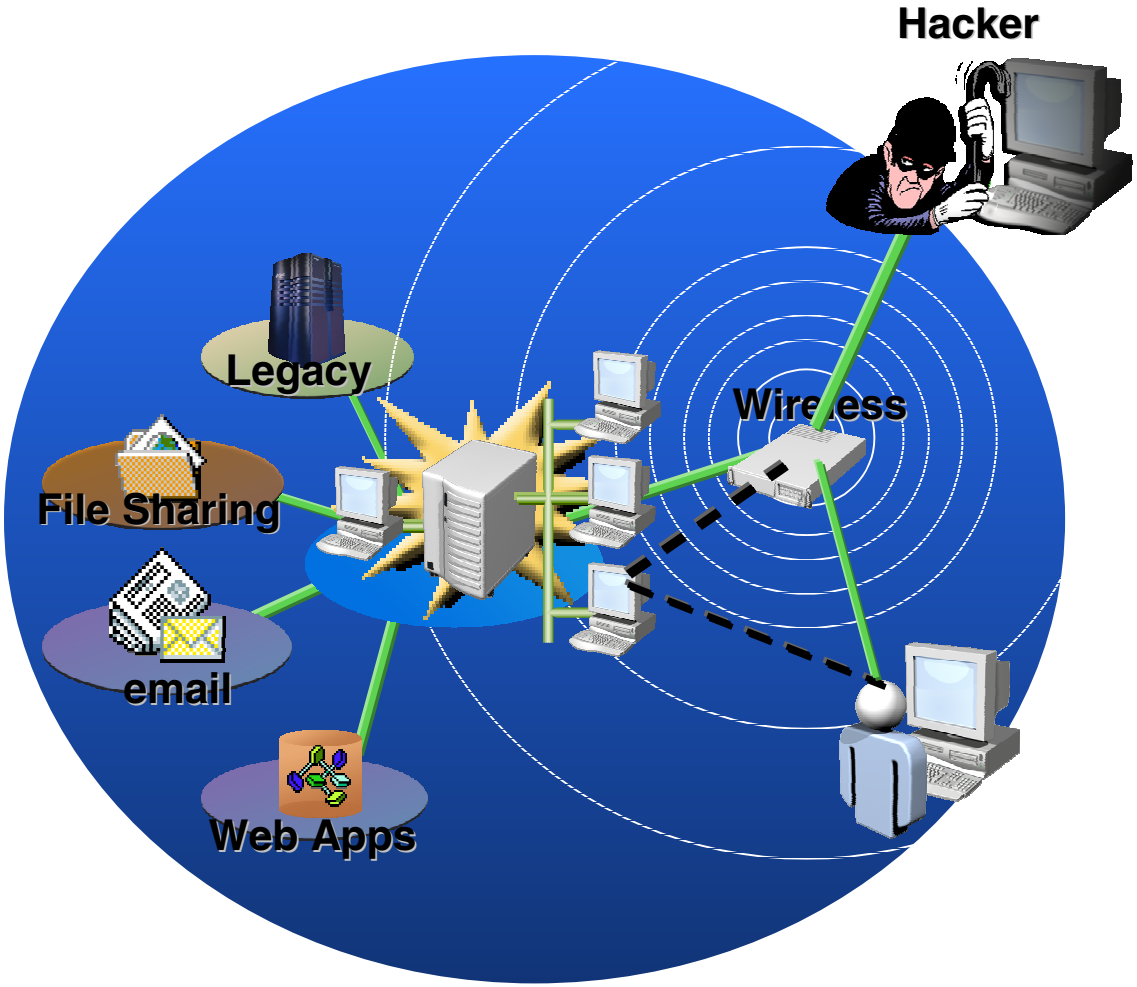
Windows Server 2003

- Client
- Gateway
- Protocols
- Authentication
- Policy
- Deployment Tools

Routing and Remote Access Services
Link clients to private networks

- Security
  - Secure remote access connection technology
  - Per session VPN packet filters
- Performance
  - Offload hardware encryption supported
  - Load Balance support for VPN
- Manageability
  - Integrated Active Directory authentication
  - Supports standards based Authentication Servers (RADIUS)

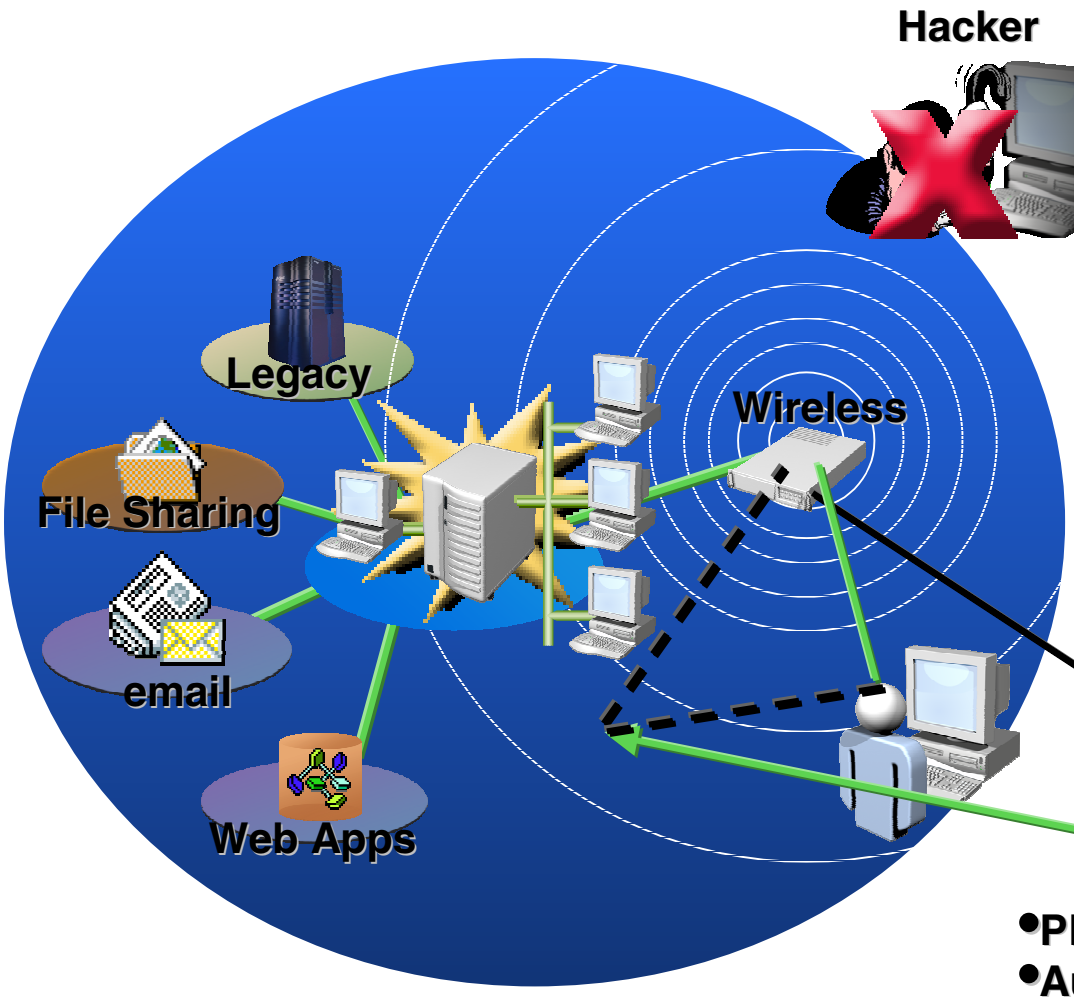
Secure Mobile Access



HACKER can attack Wireless with Brute Force tools

Airopeek, Net Stumbler, etc… Breaking standard WEP and gaining access to the corporate network

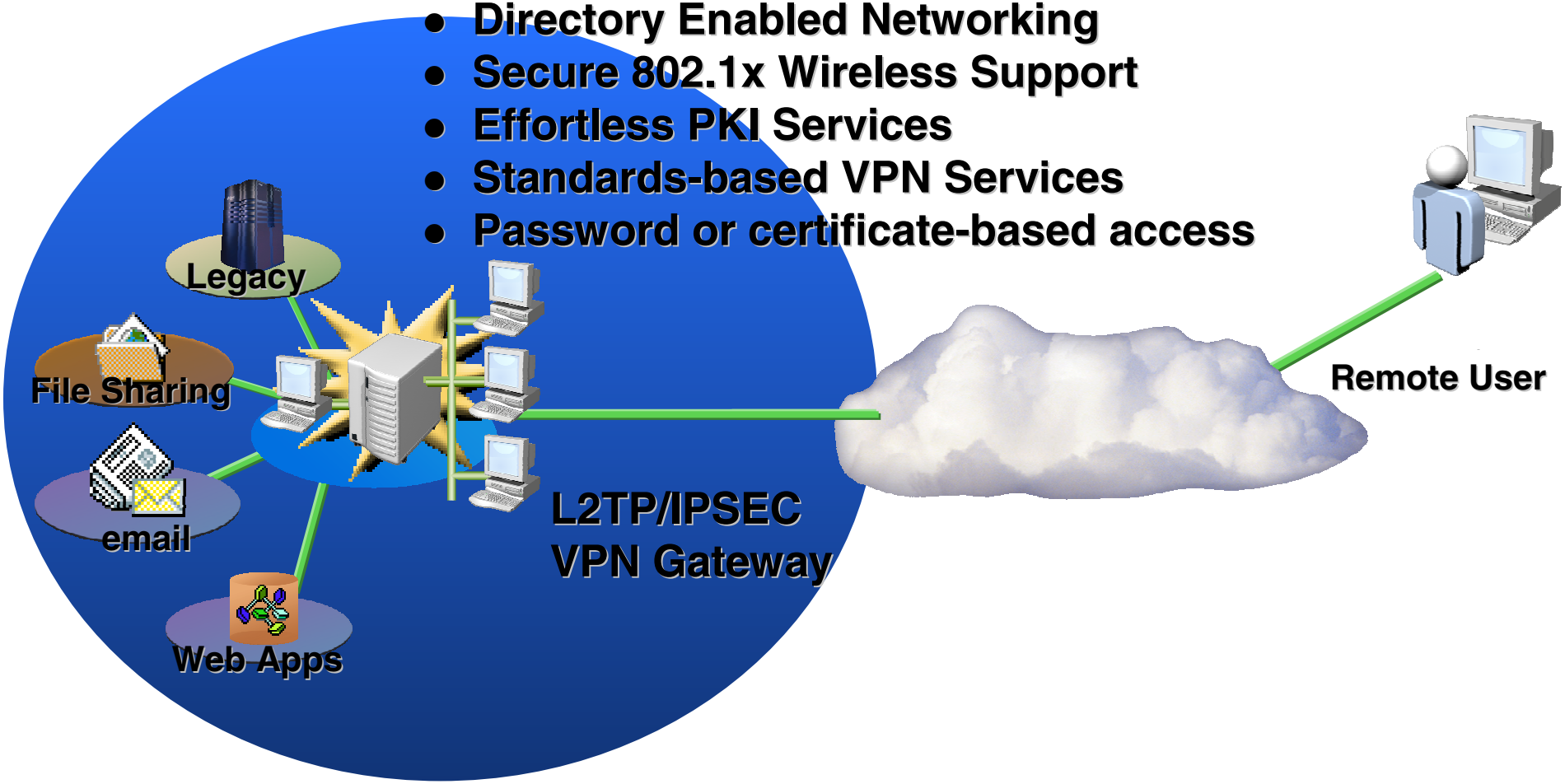
Secure Mobile Access



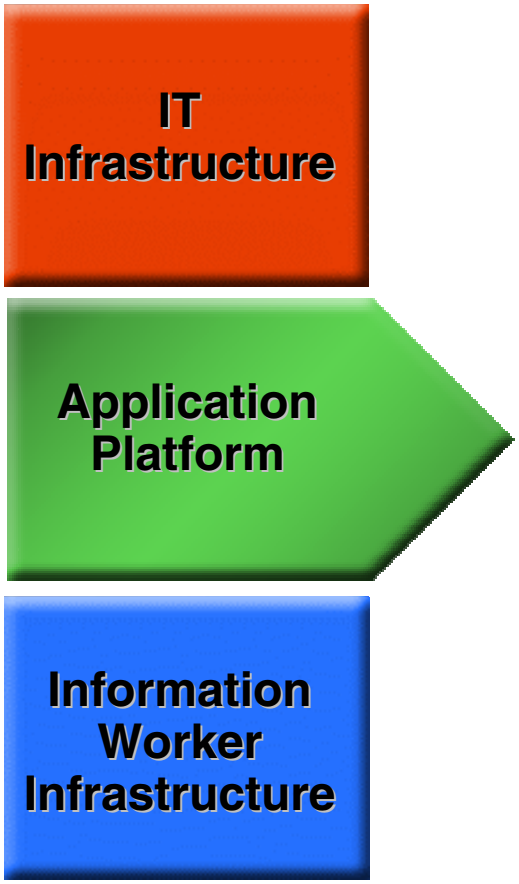
- PKI integrated with Active Directory
- Auto enrollment of certificates
- Integrated 802.1x Support
- Integrated EAP Security

Secure Mobile Access

- Directory Enabled Networking
- Secure 802.1x Wireless Support
- Effortless PKI Services
- Standards-based VPN Services
- Password or certificate-based access

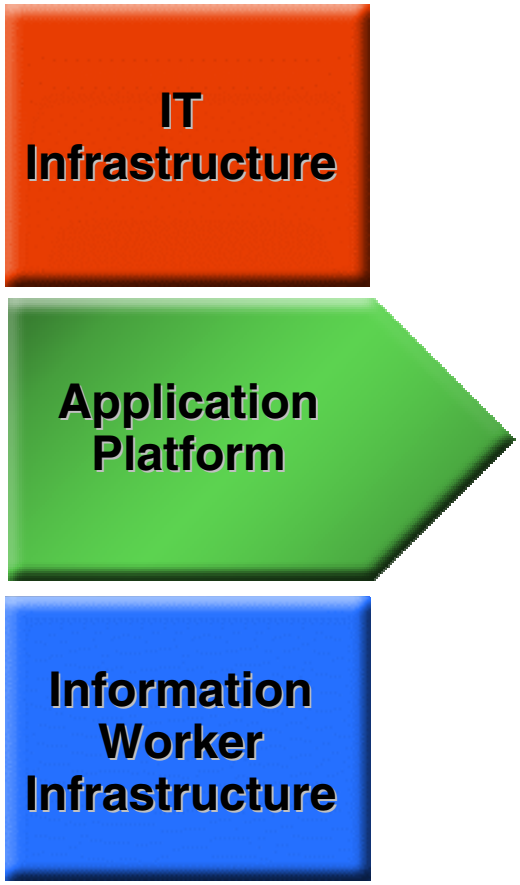


Application Platform Enhancements



- **Improved Dependability**
  - IIS Enhancements
  - IIS Security, Reliability, Availability, Scalability and Manageability
  - IIS Performance
- **Improved Productivity**
  - Comprehensive Application Platform
  - Simple Web service creation with ASP .NET
- **Improved Connectivity**
  - Secure Web Services Registry and Discovery
  - SOAP-enable COM apps
  - Mobile development

Application Platform Dependability Enhancements

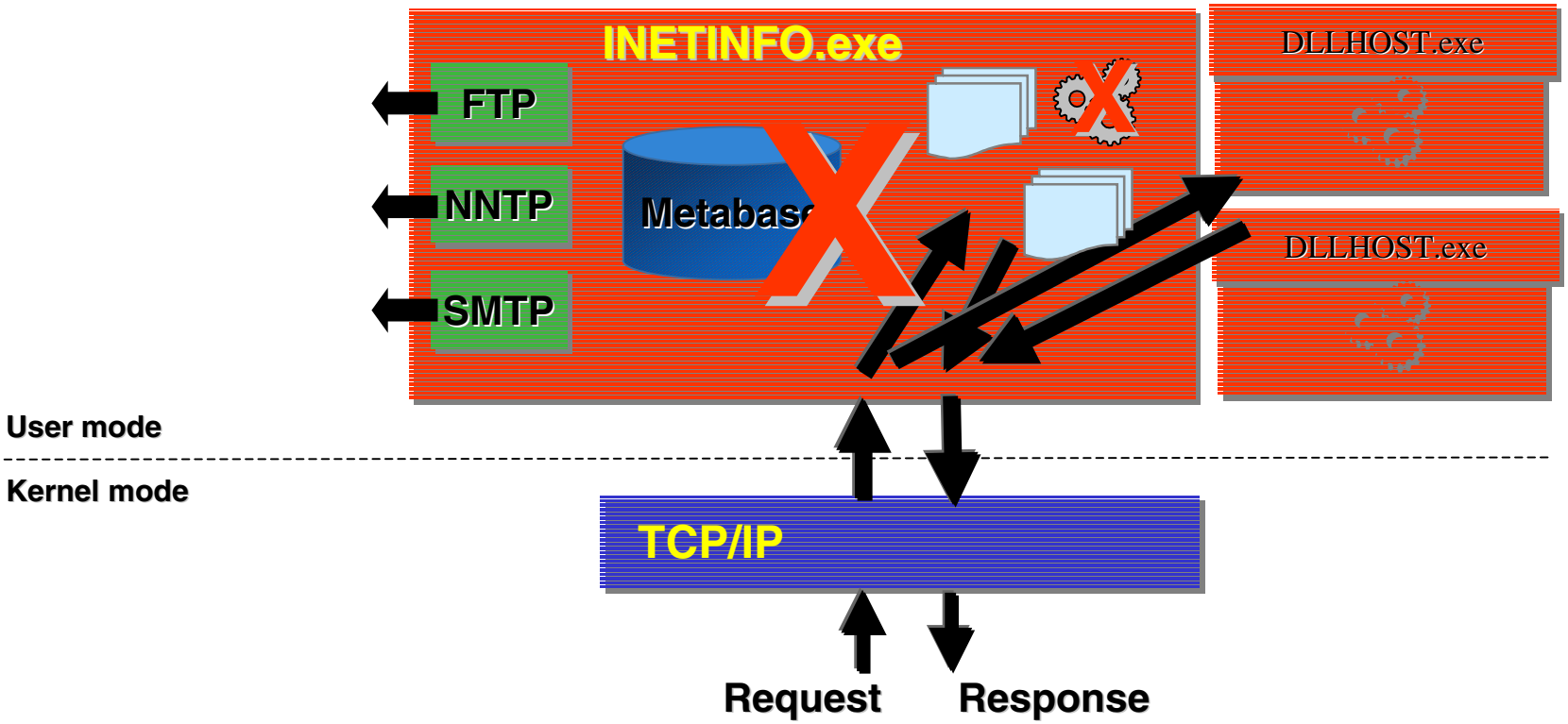


- **Improved Dependability**
  - IIS Security, Reliability, Availability and Scalability
  - Manageability
  - IIS Performance
- **Improved Productivity**
  - Comprehensive Application Platform
  - Simple Web service creation with ASP .NET
- **Improved Connectivity**
  - Secure Web Services Registry and Discovery
  - SOAP-enable COM apps
  - Mobile development

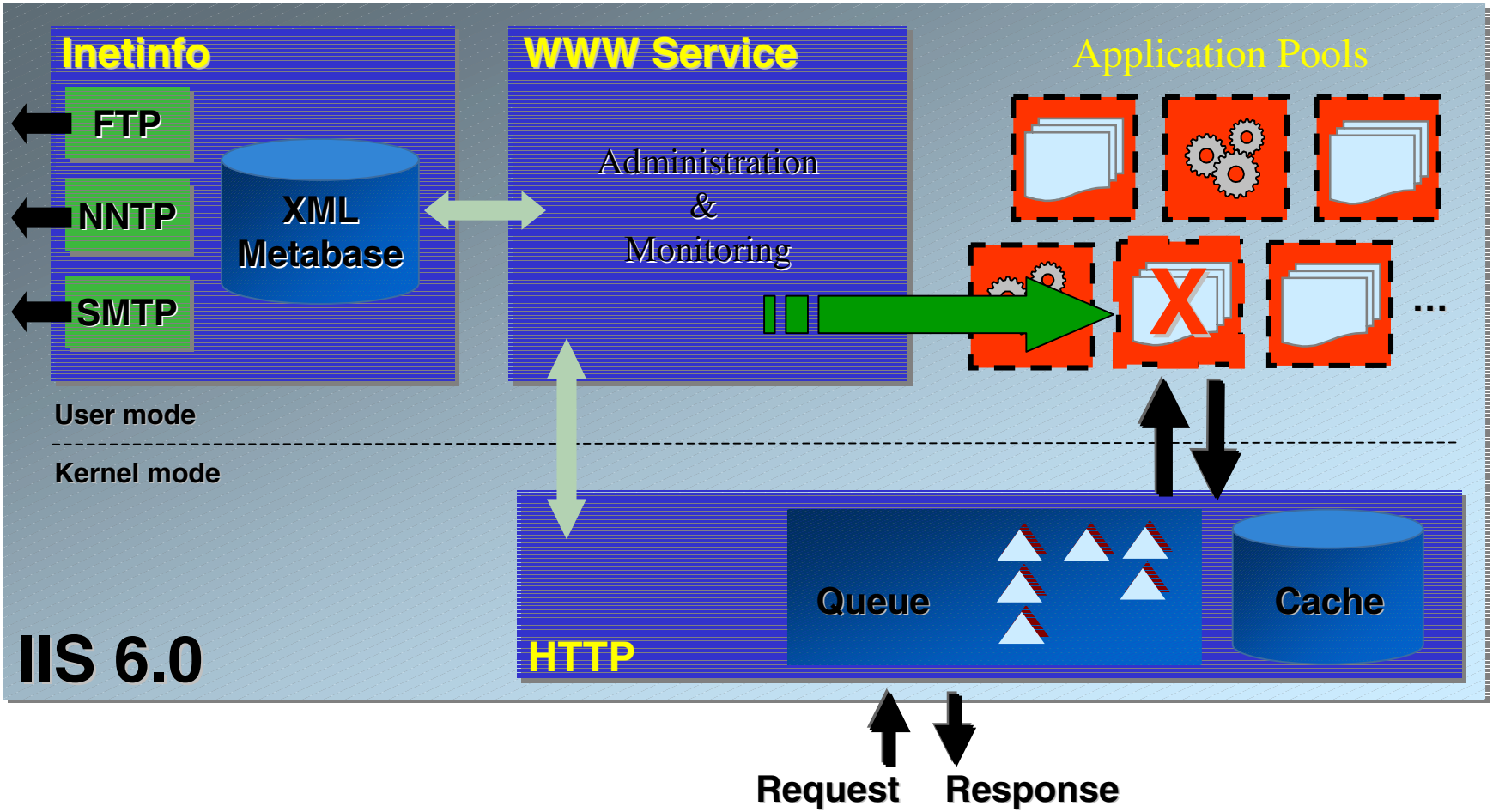
IIS 6 Security, Reliability Availability and Scalability

- Security enhancements
  - Run as least privileged account
  - Secure defaults
- Reliability
  - Worker process isolation mode
- Availability
  - Process recycling
- Scalability
  - 20,000 pooled applications
    - Compare: Fewer than 3000 with IIS5
  - 1000 isolated apps on 1 box each with its own security identity
    - Compare: Maximum of 100 with IIS5
  - Web Gardens support

IIS 5 Request Processing



IIS 6.0 Request Processing

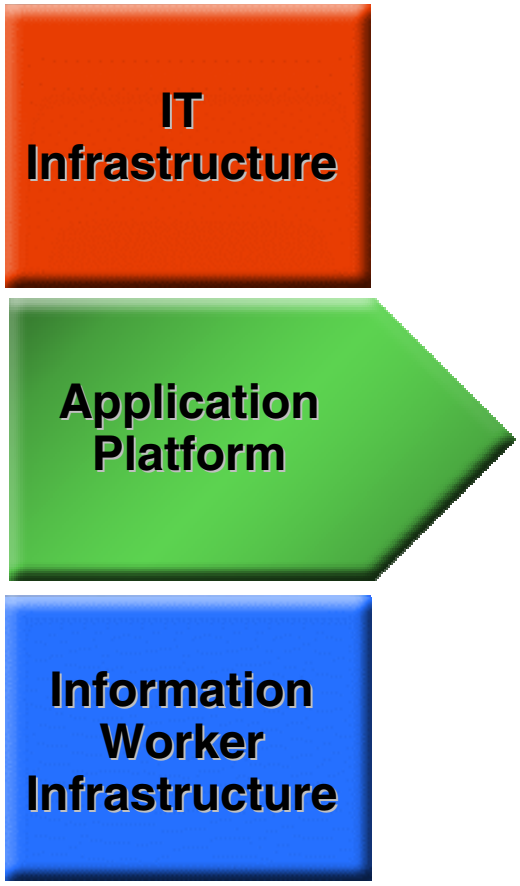


Security conscious architecture

Security = Reliability

- IIS processes run with the lowest possible privilege
- New Architecture Reduces Denial-of-Service Potential Through:
  - Advanced Health Monitoring
    - Pinging
    - Rapid Fail Protection
  - Recycling
    - Based on #requests
    - Time of Day
    - Memory Consumption
  - CPU Accounting

Application Platform Productivity Enhancements



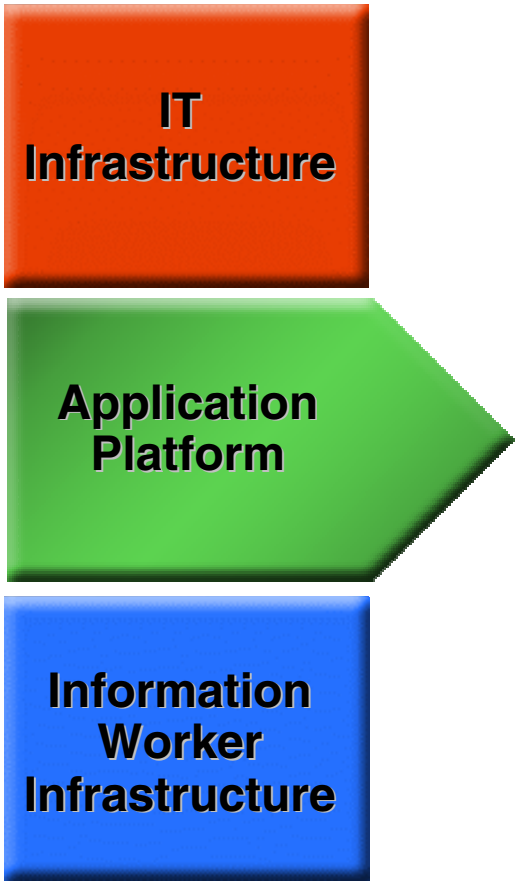
- **Improved Dependability**
  - IIS Enhancements
  - IIS Security, Reliability, Availability, Scalability and Manageability
  - IIS Performance
- **Improved Productivity**
  - Comprehensive Application Platform
  - Simple Web service creation with ASP .NET
- **Improved Connectivity**
  - Secure Web Services Registry and Discovery
  - SOAP-enable COM apps
  - Mobile development

Application Platform Enhancements

Build, Deploy and Manage Applications

- Productivity
  - Write less code with .NET Framework
  - Easy Web service creation with ASP.NET
  - Rich set of built-in services
  - Simple deployment
- Dependability
  - Code access security
  - Application security framework
- Connectivity
  - Built-in standards: XML, SOAP, WSDL, UDDI
  - Passport integration

Application Platform Connectivity Enhancements

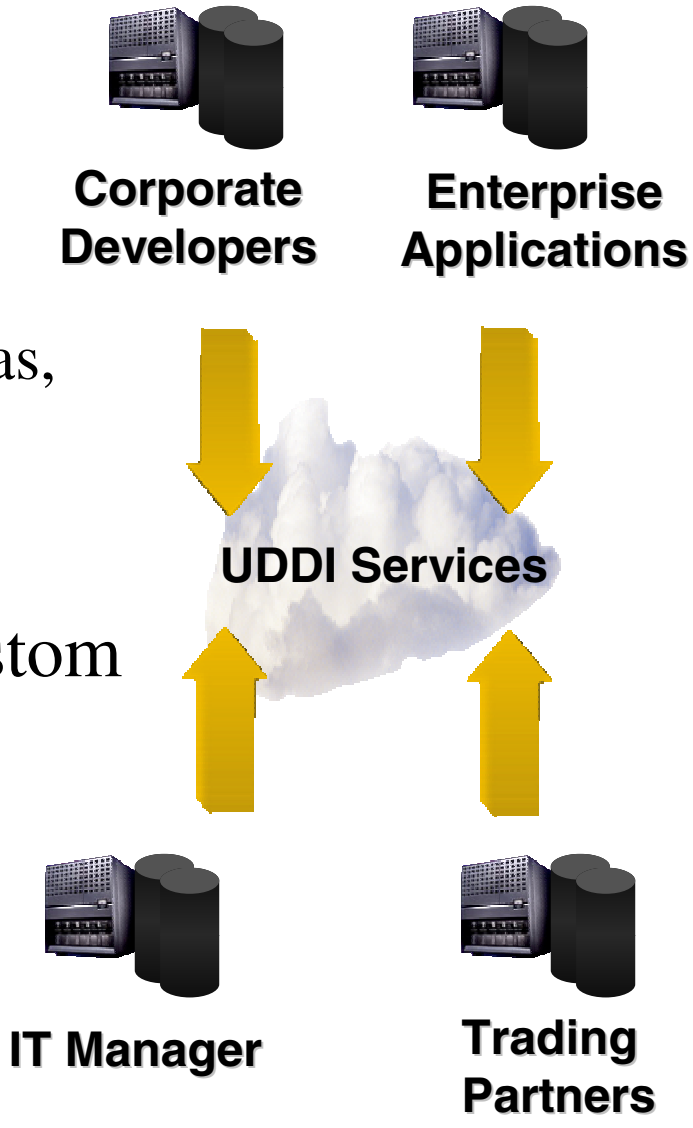


- **Improved Dependability**
  - IIS Enhancements
  - IIS Security, Reliability, Availability, Scalability and Manageability
  - IIS Performance
- **Improved Productivity**
  - Comprehensive Application Platform
  - Simple Web service creation with ASP .NET
- **Improved Connectivity**
  - Secure Web Services Registry and Discovery
  - SOAP-enable COM apps
  - Mobile development

Secure Web Services Registry And Discovery

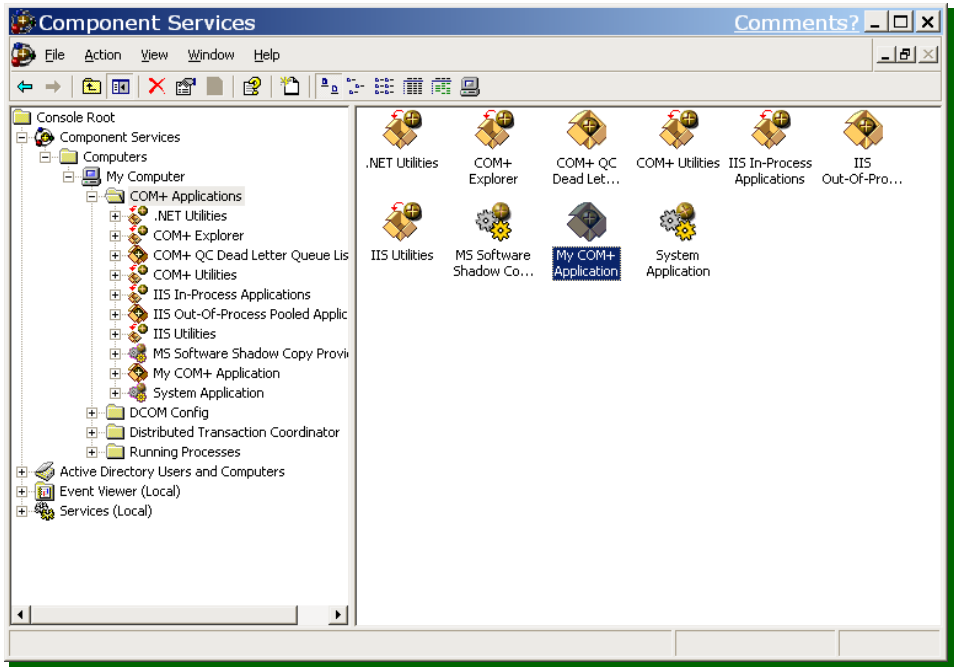
Enterprise UDDI Services

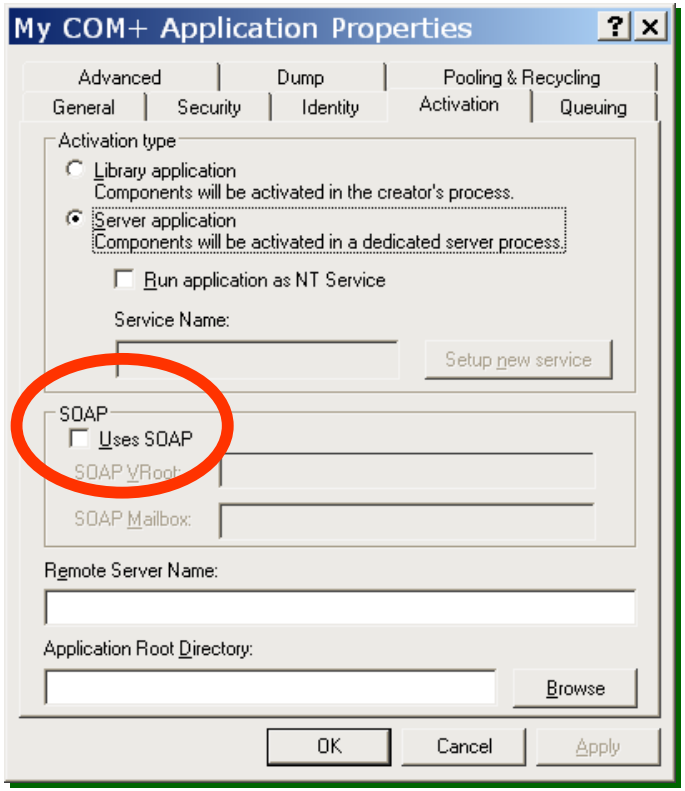
- Developer platform
  - Discover, share and reuse schemas, taxonomies and Web services
  - VS and Office tools integration
- Classify applications and Web services using standard and custom taxonomies
- Dynamic binding of applications to Web services



SOAP-enable COM Applications

- Use SOAP with no new code
- Leverage existing apps in new architecture
- Traverse firewalls with existing applications

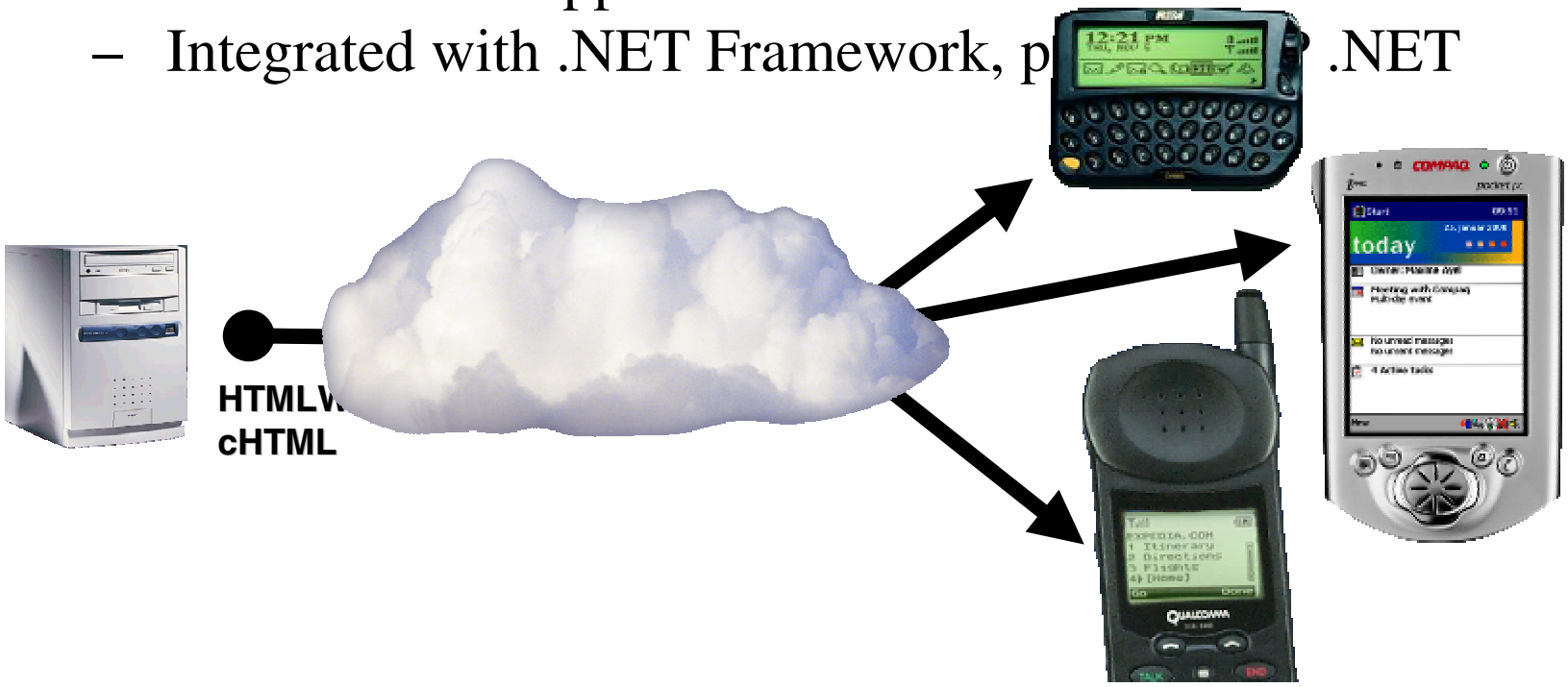




Mobile Development

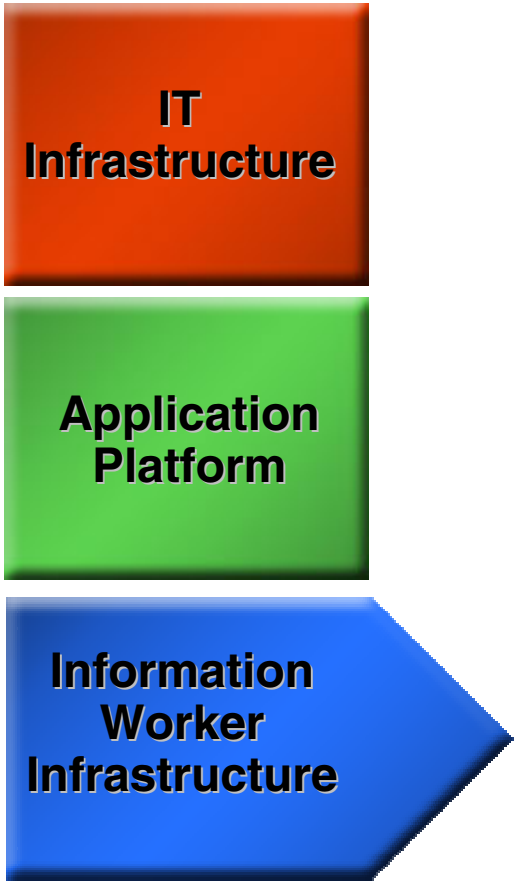
Write Once, Deploy On Any Device

- Mobile controls
  - Quickly build mobile-aware applications
  - 140+ devices supported out of the box
  - Integrated with .NET Framework, p .NET



Information Worker

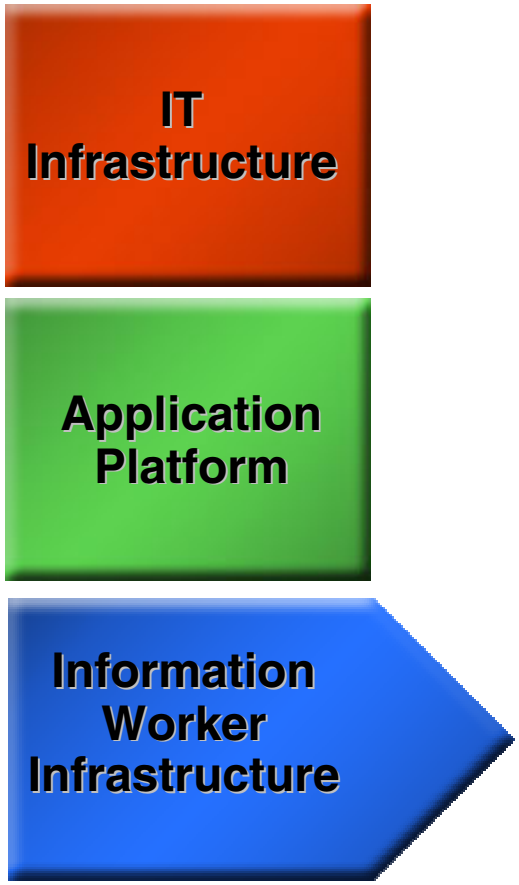
Infrastructure Enhancements



- **Dependable**
  - Terminal Server
  - Intelligent reconnect for RAS, Windows Media Services
  - 100-140% Faster file performance
- **Productive**
  - Shadow Copy Restore
  - Local Resource access for Terminal Server Sessions
  - “No touch” VPN, RAS, PKI setup
- **Connected**
  - Collaboration enhancements
  - Windows Media Services

Information Worker

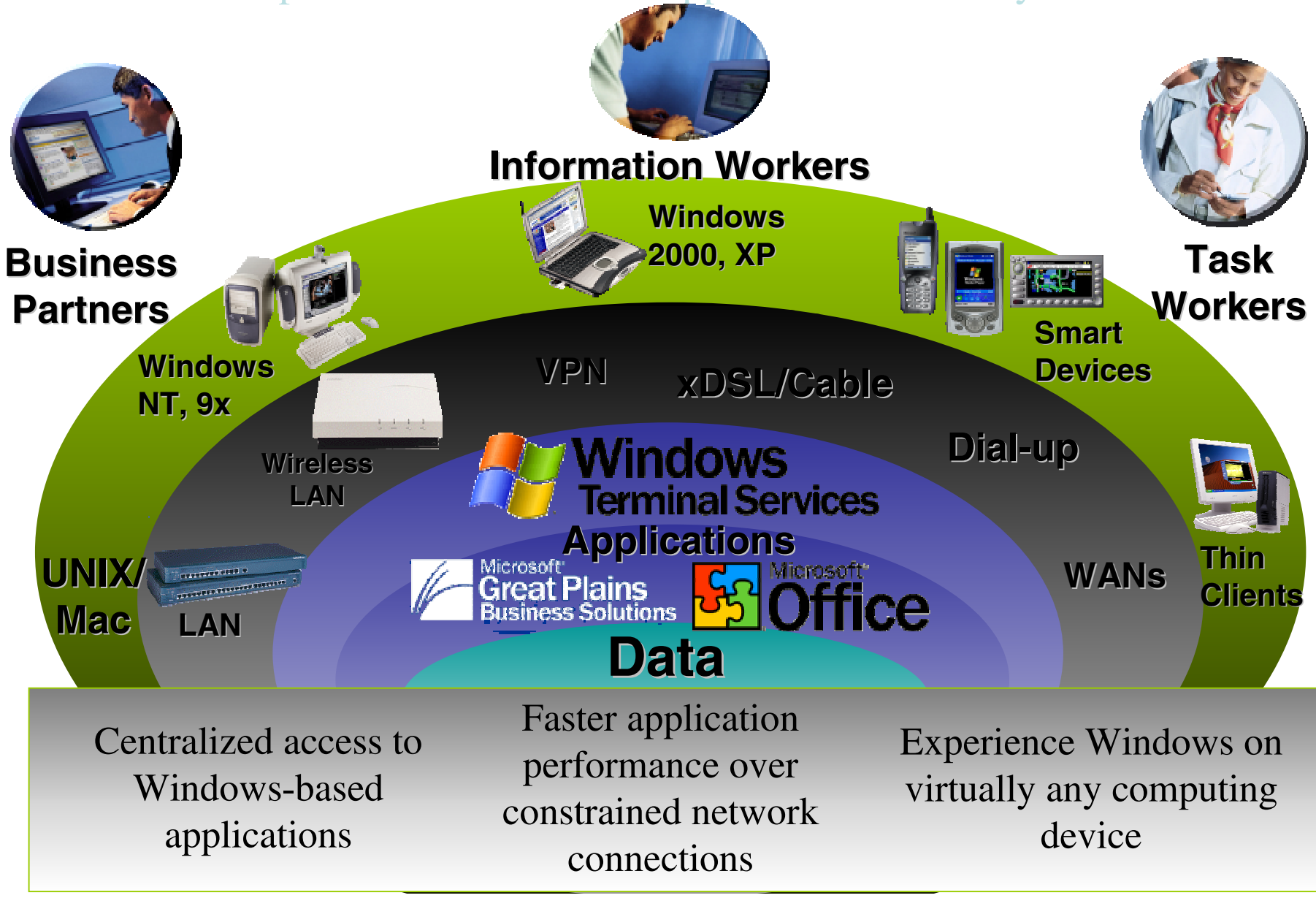
Infrastructure Dependability Enhancements



- **Improved Dependability**
  - Terminal Server
  - Intelligent reconnect for RAS, Windows Media Services
  - 100-140% Faster file performance
- **Improved Productivity**
  - Shadow Copy Restore
  - Local Resource access for Terminal Server Sessions
  - “No touch” VPN, RAS, PKI setup
- **Improved Connectivity**
  - Collaboration enhancements
  - Windows Media Services

Terminal Server in Windows Server

Rapid access to data and applications from anywhere



Centralized access to Windows-based applications

Faster application performance over constrained network connections

Experience Windows on virtually any computing device

Terminal Services Technology In Windows Server 2003

- Remote Desktop for Administration
  - Formerly known as “TS remote administration mode” in Windows® 2000 Server
  - Similar to Windows XP Remote Desktop
    - Allows one console (local or remote) + two remote virtual sessions
  - No TS CALs required
- Terminal Server
  - Formerly known as “TS application server mode” in Windows 2000 Server
  - Provides remote execution of applications for multiple concurrent users
  - TS CALs required
    - Console connection doesn’t require TS CAL
- Remote Assistance
  - Identical to Windows XP Remote Assistance
  - Users on a Terminal Server can receive assistance from other TS or Windows XP users
  - Also used for remote administrator collaboration

Remote Desktop Connection - RDP 5.2

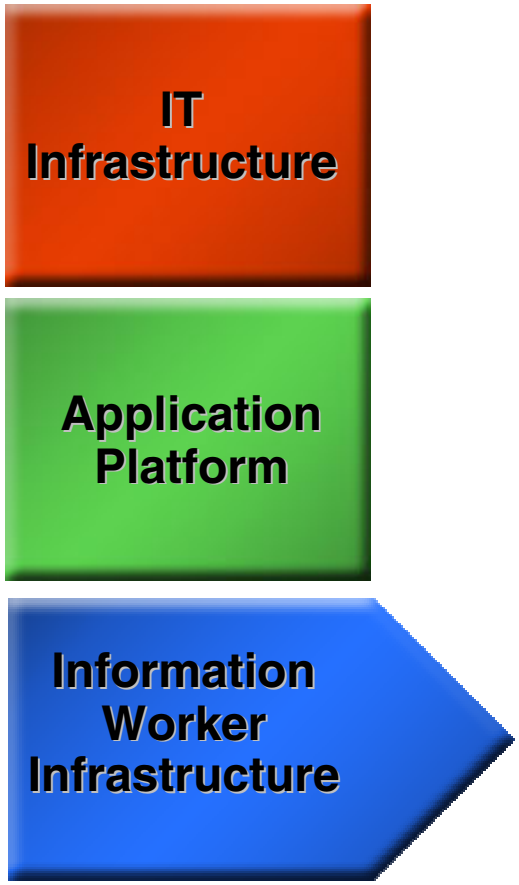
- Full (.MSI), MMC and Web (ActiveX®)
  - Full client included with Windows XP
- Improved usability
  - Full screen connection bar
  - Save connection settings from same UI
  - Enhanced client error messages (40+ new messages)
- High color (up to 24-bit), 1600x1200
- Resource redirection
  - Audio output, Windows key combos, disk drives and printers (local and network), serial devices, Smart card, clipboard (+files)
- Full desktop or specific application
- Network and performance improvements
  - Increased network bandwidth savings over RDP 5.0
  - Remote 'experience' turns off wallpaper, visual styles, etc. depending on network connection
  - Auto-reconnect (new with .NET RC1 and XP SP1)
- Enhanced security
  - 128-bit bi-directional RC4
  - User prompted if redirections enabled

demo

Terminal Services

Information Worker Infrastructure

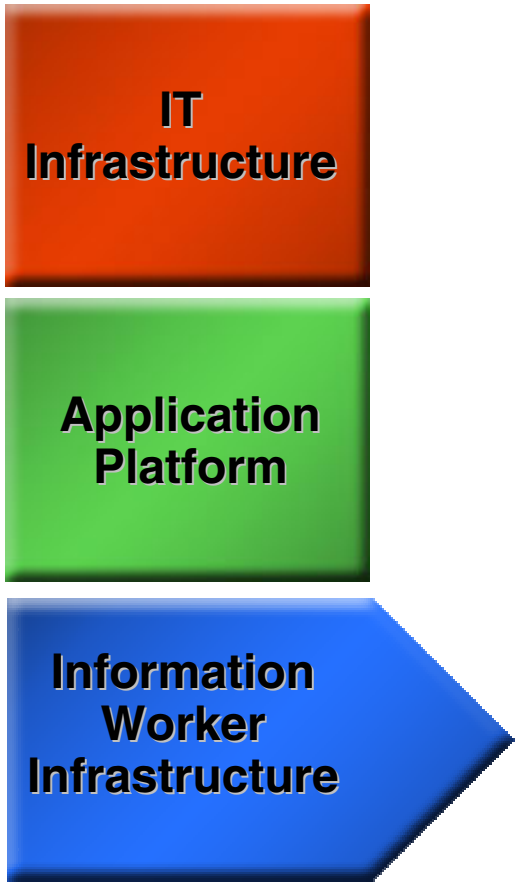
Productivity Enhancements



- **Dependable**
  - Terminal Server
  - Intelligent reconnect for RAS, Windows Media Services
  - 100-140% Faster file performance
- **Productive**
  - Shadow Copy Restore
  - Local Resource access for Terminal Server Sessions
  - “No touch” VPN, RAS, PKI setup
- **Connected**
  - Collaboration enhancements
  - Windows Media Services

Information Worker Infrastructure

Connectivity Enhancements

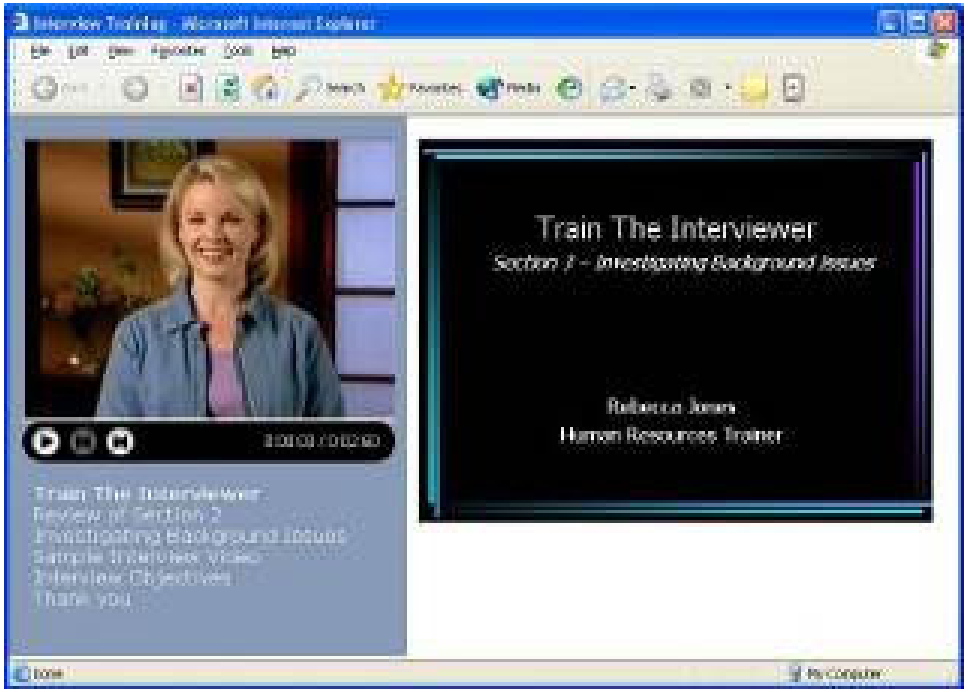


- **Dependable**
  - Terminal Server
  - Intelligent reconnect for RAS, Windows Media Services
  - 100-140% Faster file performance
- **Productive**
  - Shadow Copy Restore
  - Local Resource access for Terminal Server Sessions
  - “No touch” VPN, RAS, PKI setup
- **Connected**
  - Windows Media Services

Windows Server Media Services

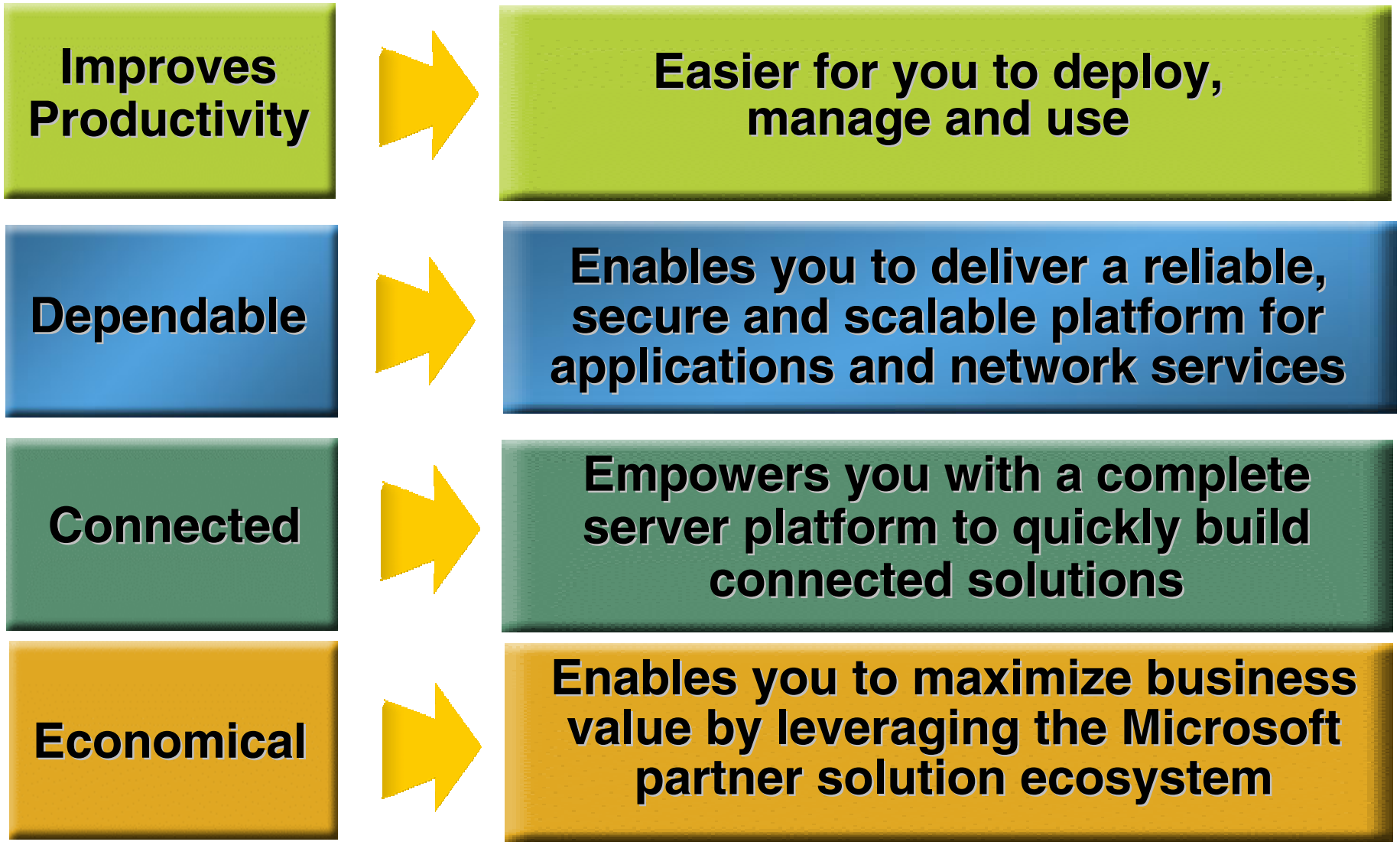
Comprehensive streaming media distribution platform

- End-user experience
  - Fast Streaming (Fast Start + Fast Cache)
  - Graceful recovery from network disconnects at loss-point
- Scalability and Manageability
  - 2x concurrent users vs. Windows 2000 Server
  - MMC, Web browser, or command-line scripts administration
- Extensibility and developer reach
  - New plug-in architecture: supported by familiar languages and scripting
  - Object Model: over 1000 server interfaces



Summary

Windows Server Delivers



Community Resources

Attend a free chat or web cast

http://www.microsoft.com/communities/chats/default.mspx
http://www.microsoft.com/usa/webcasts/default.asp

List of newsgroups

http://communities2.microsoft.com/communities/newsgroups/en-us/default.aspx

MS Community Sites

http://www.microsoft.com/communities/default.mspx

Locate Local User Groups

http://www.microsoft.com/communities/usergroups/default.mspx

Community sites

http://www.microsoft.com/communities/related/default.mspx

RETURN TO INDEX