Making Computing More Trustworthy

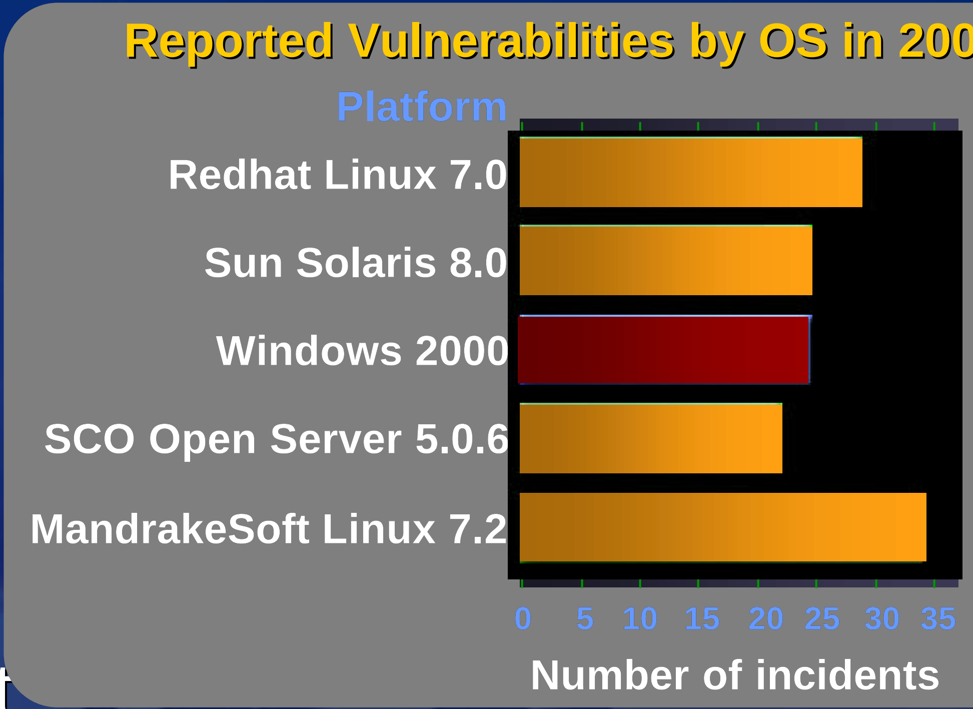
Microsoft AG
Enterprise & Partner Group
Andre Hagmann
Senior System Engineer
ahagmann@microsoft.com

Agenda

- Microsoft Security Framework
- Microsoft Software Update Services
- Microsoft Baseline Security Analyzer
  - HFNetChk
- Office Update Inventory Tool
- Security Resources

Our Industry has a Problem

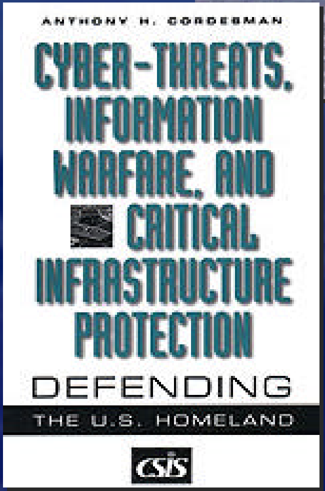
- Security breaches common
  - Malicious code
  - Good code with bugs
- Escalating challenges
  - Connectivity
  - Administration
- Adoption of IT in doubt
  - Customers need to believe in technologies, companies and services
- No common framework for discussion



John McCormick, TechRepublic, Inc., September 24, 2001, based on data provided by Security Focus Bugtraq

Critical Infrastructure

- Computers are increasingly essential our everyday lives
- Evolving markets drive new priorities
  - Complex, interconnected systems
  - Devices at all scales
  - Enterprise reliability requirements
- Information Technology is essential but vulnerable
- Customers won’t depend on what they don’t trust



ANTHONY H. CORDESMAN

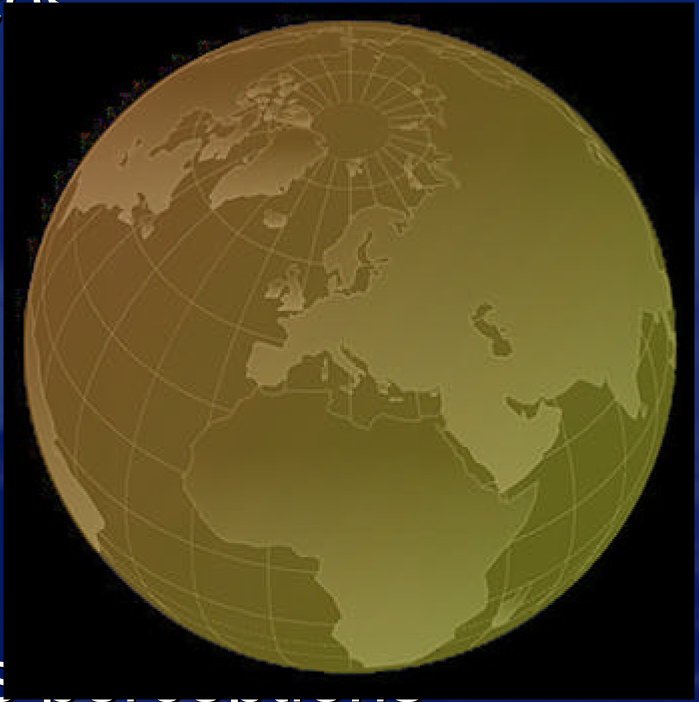
CYBER-THREATS, INFORMATION WARFARE, AND CRITICAL INFRASTRUCTURE PROTECTION

DEFENDING THE U.S. HOMELAND

CSIS

Tackling the Problem

- Work on all fronts
  - Security, privacy, reliability, business integrity
  - All platforms and experiences
  - Across the organization
  - With all our customers
  - Across the industry
- Culture shift
  - Trustworthiness as priority
  - Now and Forever
  - Change behavior as well as perceptions



Microsoft Security Framework

SD^3 + C

Secure by D n

- ❑ Secure architecture
- ❑ Security aware features
- ❑ Reduce vuln

Secure by D t

- ❑ Reduce attack surface area
- ❑ Unused features off by def
- ❑ Only require

Secure in Deploym

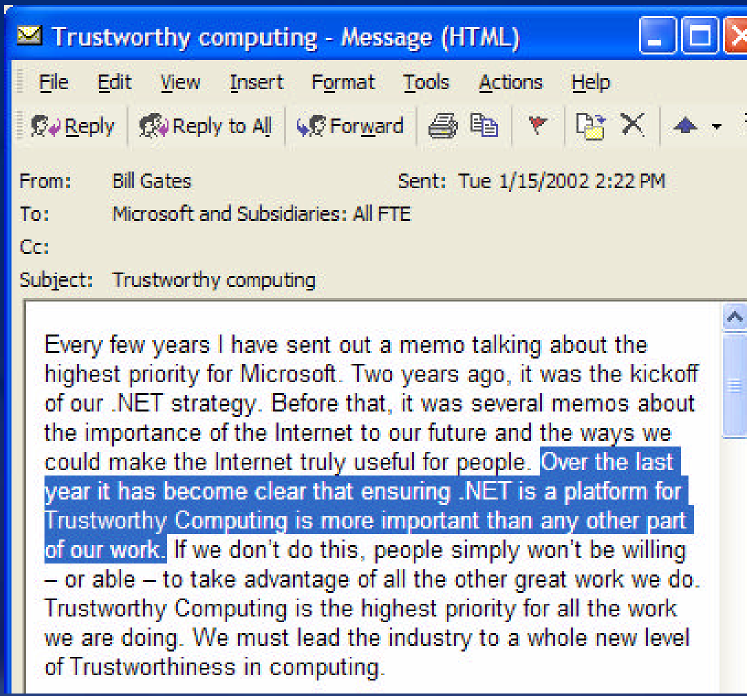
- ❑ Protect, Detect, Defend, Recover, Manage
- ❑ Process: How To's, Architecture Guides
- ❑ People: Training

Communications

- ment
- ❑ er of the security community
- ❑ Microsoft Security Response Center

Secure by Design

- Product
  - Security Push
  - New tools, compiler improvements
  - Security Business Unit
- People
  - Retrained dev, test, PM
  - Appointed Chief Security Strategist
  - Leads driving best practices across company
- Process
  - R&D budget for security tripled
  - Threat model-driven reviews
  - Bug feedback loop & code sign-off reqs

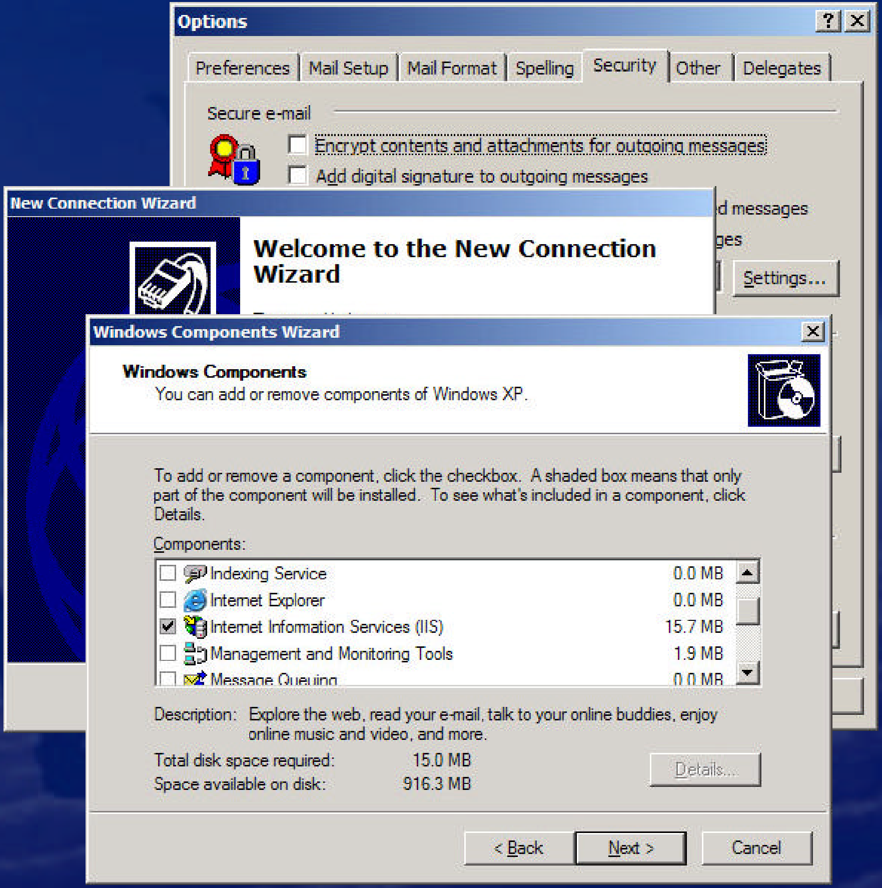

Trustworthy computing - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

From: Bill Gates Sent: Tue 1/15/2002 2:22 PM
To: Microsoft and Subsidiaries: All FTE
Cc:
Subject: Trustworthy computing

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing – or able – to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

Secure By Default

- Office XP
  - .exe receipt, script access disabled
- Windows XP
  - Internet Connection Firewall
- Major products to ship secure by default
  - .NET server, IIS6, SQLnext, Office 11
  - Backporting to Windows 2000, IIS5.x and earlier



Options

Preferences | Mail Setup | Mail Format | Spelling | Security | Other | Delegates

Secure e-mail

□ Encrypt contents and attachments for outgoing messages

□ Add digital signature to outgoing messages

d messages

ges

Settings...

New Connection Wizard

Welcome to the New Connection Wizard

Windows Components Wizard

Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

□ Indexing Service	0.0 MB
□ Internet Explorer	0.0 MB
☑ Internet Information Services (IIS)	15.7 MB
□ Management and Monitoring Tools	1.9 MB
□ Message Queuing	0.0 MB

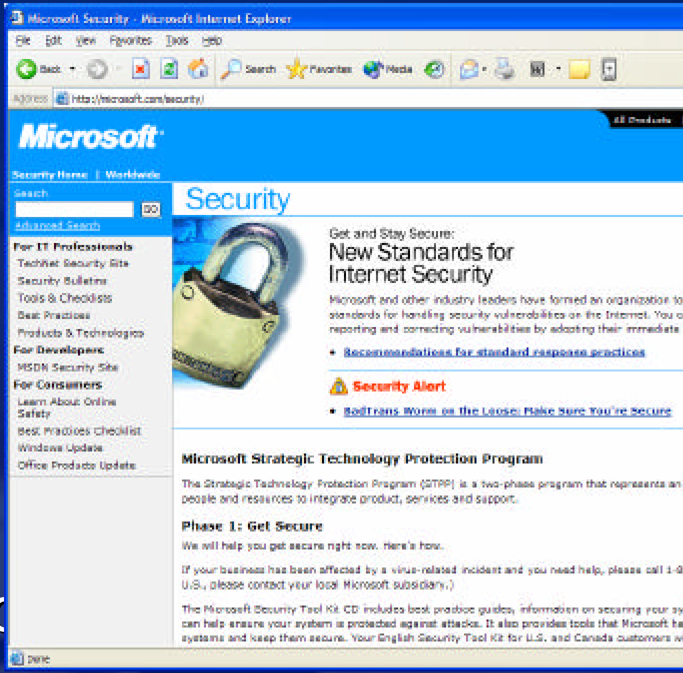
Description: Explore the web, read your e-mail, talk to your online buddies, enjoy online music and video, and more.

Total disk space required: 15.0 MB

Space available on disk: 916.3 MB

Secure in Deployment

- STPP - Get Secure
  - Microsoft Security Toolkit
  - Microsoft Baseline Security Analyzer
  - Security Assessment Program
  - Deployment, update, lockdown tools
- STPP - Stay Secure
  - Windows 2000 Security Rollup
  - Windows 2000 SP3
  - Microsoft Software Update Servic
  - SMS Valuepack
- Microsoft Security Response Center
- Systems Integrator Source Licensing Program
- Windows Update



Microsoft Security - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://microsoft.com/security/
All Products
Microsoft
Security Home | Worldwide
Search
GO
Advanced Search

For IT Professionals

TechNet Security Site

Security Bulletins

Tools & Checklists

Best Practices

Products & Technologies

For Developers

MSDN Security Site

For Consumers

Learn About Online Safety

Best Practices Checklist

Windows Update

Office Products Update

Security

Get and Stay Secure:

New Standards for Internet Security

Microsoft and other industry leaders have formed an organization to
standards for handling security vulnerabilities on the Internet. You c
reporting and correcting vulnerabilities by adopting their immediate

- Recommendations for standard response practices

Security Alert

- BadTrans Worm on the Loose: Make Sure You're Secure

Microsoft Strategic Technology Protection Program

The Strategic Technology Protection Program (STPP) is a two-phase program that represents an
people and resources to integrate product, services and support.

Phase 1: Get Secure

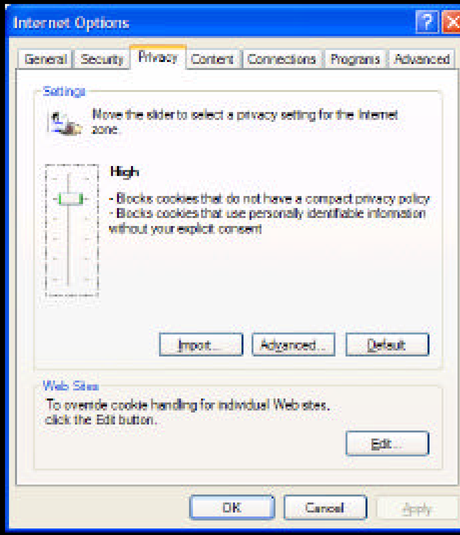
We will help you get secure right now. Here's how.

If your business has been affected by a virus-related incident and you need help, please call 1-8
U.S., please contact your local Microsoft subsidiary.)

The Microsoft Security Tool Kit CD includes best practice guides, information on securing your sy
can help ensure your system is protected against attacks. It also provides tools that Microsoft ha
systems and keep them secure. Your English Security Tool Kit for U.S. and Canada customers w

Privacy: Products & Process

- Product design
  - P3P support in IE 6
  - Kerberos for Passport
  - Office XP Privacy
  - Anonymous XP activation
  - MSN 8 tools to manage what kids access
- Business practices
  - MSN shows users data held on them
  - FIP, GLB, Safe Harbor
  - Third party audits
  - Privacy Directive and Handbook
  - Privacy Health Index



Move the slider to select a privacy setting for the Internet zone.

High

- Blocks cookies that do not have a compact privacy policy
- Blocks cookies that use personally identifiable information without your explicit consent

To override cookie handling for individual Web sites, click the Edit button.

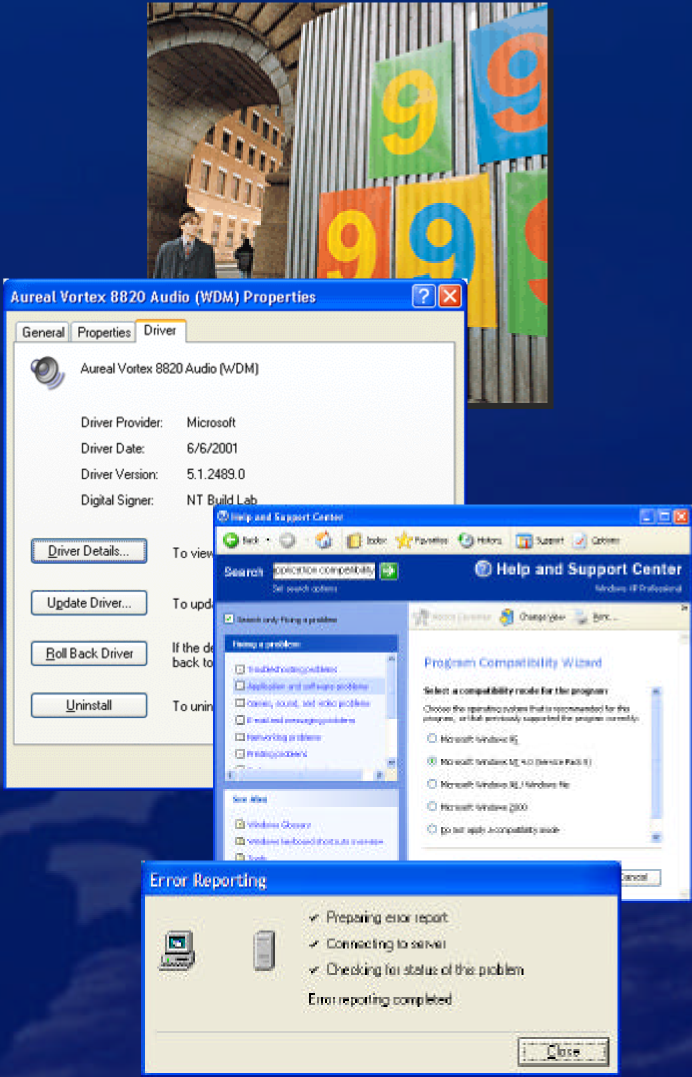
PRIVACY BBBOnLine

CLICK TO VERIFY
Reviewed by TRUSTe
site privacy statement

online privacy alliance

Reliability

- Five Nines
- Windows XP
  - Driver management
  - Shared DLL support
  - Improved installation, update, backup, repair, recovery
- Product Quality Initiative
  - Documentation, feedback, measurement, integration
- Error reporting
  - Office fixed 40% of crashes for SP1
  - VS fixed 57% crashes in beta
  - Vendor web site



Aureal Vortex 8820 Audio (WDM) Properties

Aureal Vortex 8820 Audio (WDM)

Driver Provider: Microsoft
Driver Date: 6/6/2001
Driver Version: 5.1.2489.0
Digital Signer: NT Build Lab

To view

To upd

If the de
back to

To unin

Help and Support Center

Program Compatibility Wizard

Error Reporting

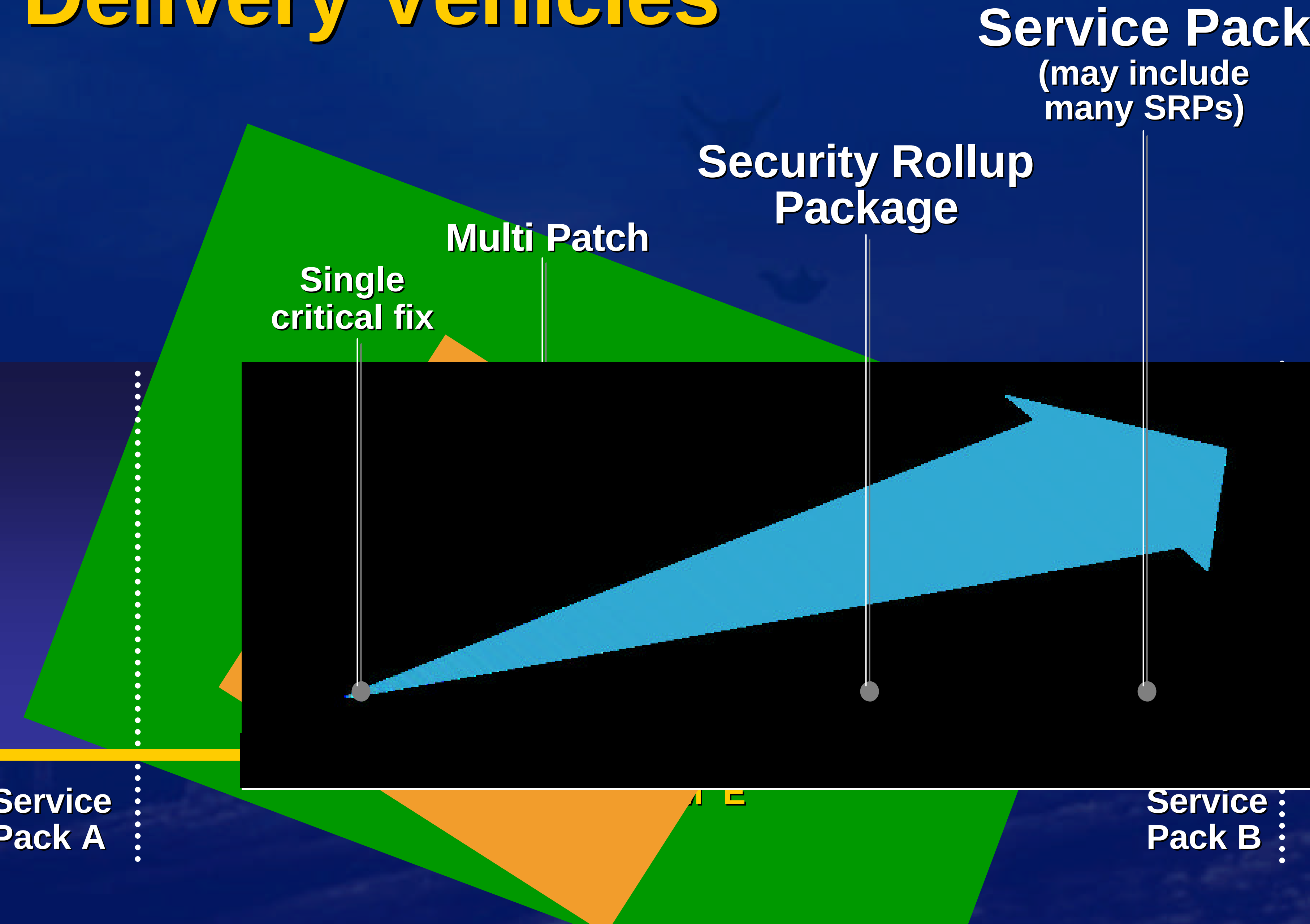
✓ Preparing error report
✓ Connecting to server
✓ Checking for status of this problem

Error reporting completed

Microsoft Security Response Center

- Works within framework of Microsoft Security Commitment
  - Responds to every report within 24 hours, 7 days a week
  - Works with product groups when issue requires
  - Provides bulletin and web posting of patches or workarounds
- Ensures wide distribution of information
  - Free email list
  - Proactive media notification of serious issues
  - Key priority is getting patches to more customers

Delivery Vehicles



Service Pack
(may include
many SRPs)

Security Rollup
Package

Multi Patch

Single
critical fix

Service
Pack A

M E

Service
Pack B

Microsoft Security Tools for Corporate System Administrators

Microsoft AG
Enterprise & Partner Group
Andre Hagmann
Senior System Engineer
ahagmann@microsoft.com

Security in a Complex World

- Security requires a framework composed of:
  - Process (procedures, guidelines)
  - Technology (hardware, software, networks)
  - People (culture, knowledge)
- Security will fail if only focusing on part of the problem
- Technology is neither the whole problem nor the whole solution

Microsoft Software Update Services 1.0

Microsoft®
Software Update Services

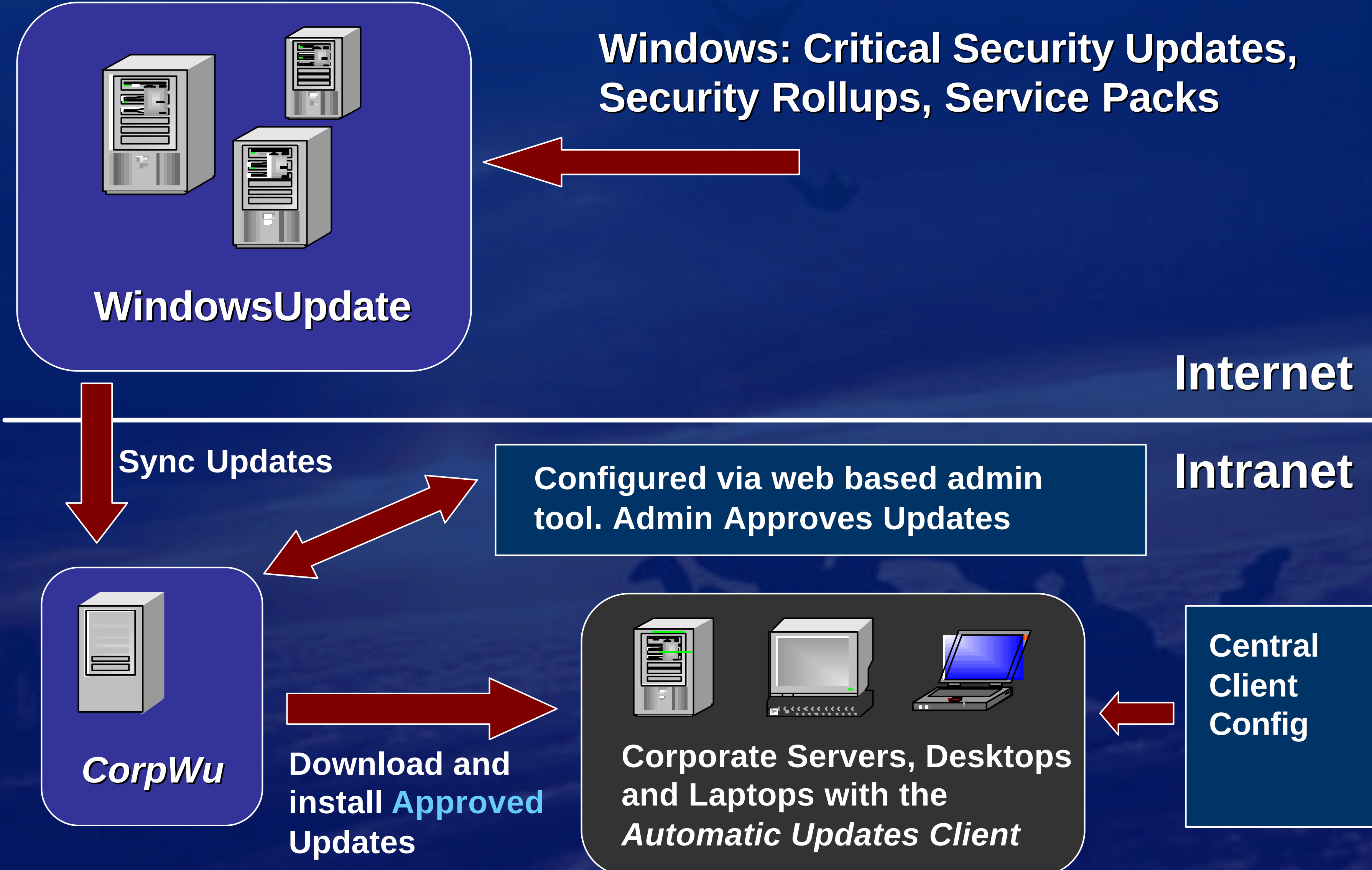
Patch Management for IT controlled desktop

- IT departments today do not allow users to go to the public Windows Update site
- IT departments do not want users to install Security updates and other Windows Update packages without them being tested in their Standard Operating Environment
- **Solution:**
    - Microsoft Software Update Services

Microsoft Software Update Services – SA Edition

- As part of our ongoing efforts to add value to Software Assurance (SA) customers, we have decided to create a special level of MSUS that gives SA customers additional benefits. Microsoft Software Update Services, SA Edition will be available in July 2002. It will build on the free version of Microsoft Software Update Services and provide these customers access to additional content.
  - Service Packs
  - Recommended QFE’s

Architecture: Microsoft Software Update Services



WindowsUpdate

Windows: Critical Security Updates, Security Rollups, Service Packs

Internet

Intranet

Sync Updates

Configured via web based admin tool. Admin Approves Updates

CorpWu

Download and install Approved Updates

Corporate Servers, Desktops and Laptops with the *Automatic Updates Client*

Central Client Config

CorpWU Components

- Auto Update Client
  - Based on Windows XP Auto Update
  - Check corporate or public WU for updates
  - Can be configured centrally by Administrator or locally configured by the local administrator
  - Can auto-download and install updates under admin control
- CorpWu Server
  - Hosted on the corporate intranet
  - Synchronization service with public WU
  - Administrator control over updates that can be deployed

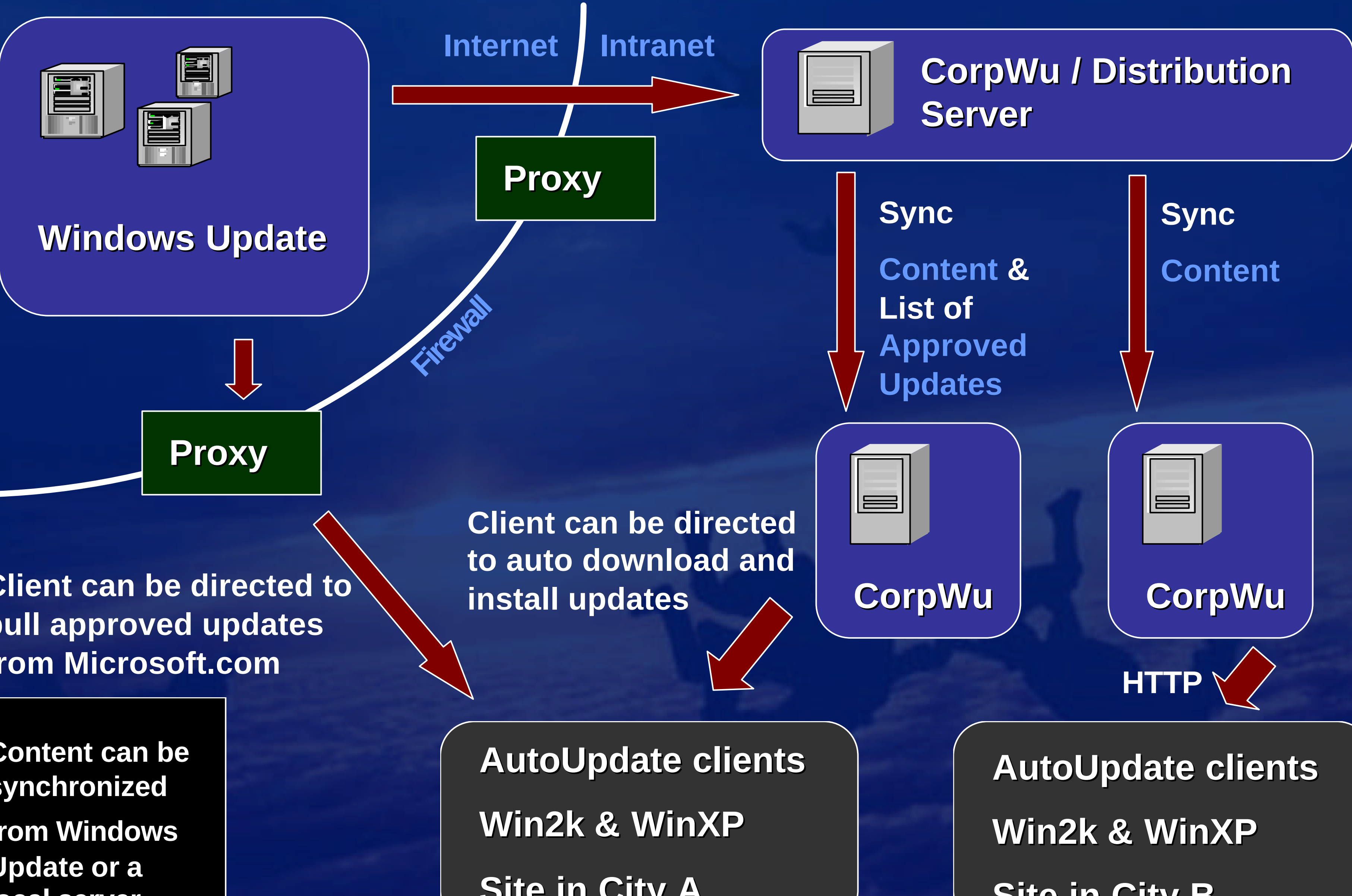
CorpWU Server Details

- Support for:
  - Intranet hosted WU server to support AutoUpdate v2.2 and higher clients
  - Administrator control over which patches get distributed within the corporation
  - Support for only Windows critical updates and service packs hosted on Windows Update
- Not Supported in V1:
  - Support critical non-Windows updates (e.g. SQL, Exchange, Office)
  - 3rd party update publishing
  - Full app distribution
  - Driver deployments
  - Targeting, i.e. integration w/Active Directory

CorpWU Server Features

- Web-based administration
  - http to the server using IE 5.5 or greater
- Synchronization
  - Manual & Scheduled metadata and update file synchronization options
- Software updates location
  - Local on the intranet or leverage the public Windows Update infrastructure
- Scale out
  - Synchronize content and list of approved items from a local CorpWU server or distribution point
- Admin control
  - Updates are not made available to clients until the admin approves them
- Server-side logging
  - Operations log – synchronization and content approval processes
- Client Status
  - Download and install status is pinged to a statistics (web) server

CorpWu Server Scale-out



Windows Update

Internet

Intranet

Proxy

Firewall

Proxy

CorpWu / Distribution Server

Sync

Content & List of Approved Updates

Sync

Content

CorpWu

CorpWu

lient can be directed to
ull approved updates
rom Microsoft.com

Client can be directed to auto download and install updates

HTTP

Content can be
ynchronized
rom Windows
pdate or a
ocal server

AutoUpdate clients

Win2k & WinXP

Site in City A

AutoUpdate clients

Win2k & WinXP

Site in City B

CorpWu Security

- AutoUpdate client will only install packages that have been signed by Microsoft
- All of the data files used by the CorpWU server are also checked to see that they have been signed by Microsoft

CorpWU Server Roadmap

- Server
  - **CorpWU *RTM*** in early Q2 / 2002
  - Localized in English and Japanese only
    - Can distribute updates for all Windows XP and Windows 2000 localized languages
- Supported on Windows 2000 SP2 and Windows.NET Server Beta 3
- Microsoft Software Update Services Overview Whitepaper
  - http://www.microsoft.com/technet/treeview/default.asp?url=/technet/ittasks/support/CorpWU.asp

SMS Value Pack

announcing...

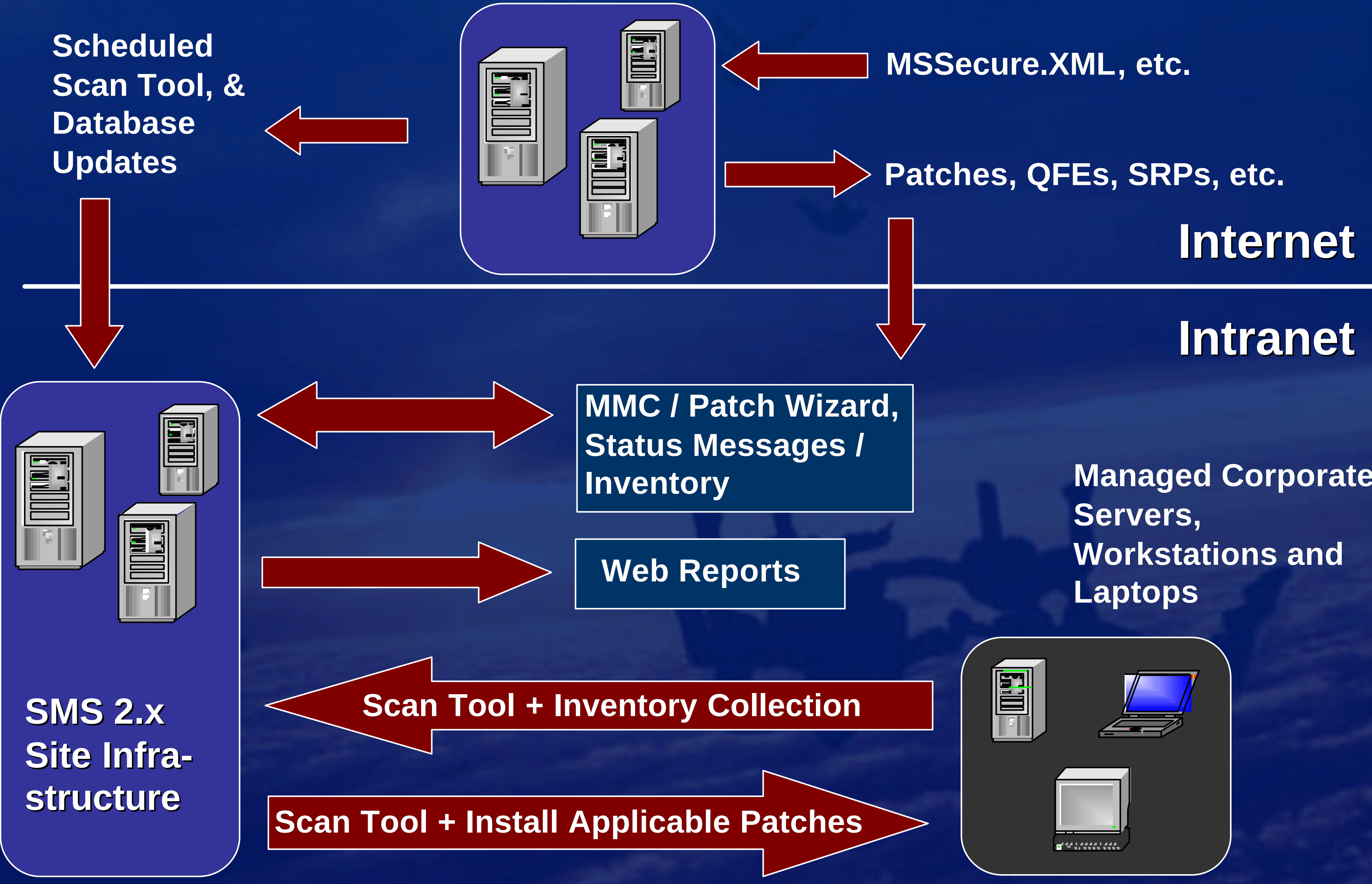
In Beta Now!

SMS Value Pack

- Uses existing SMS software distribution to deploy HFNetChk to all systems
- SMS runs a recurring task automatically, collecting information about which computers need what patches
- Data reported to a single enterprise-wide repository using existing SMS inventory features
- SMS generates rich IT reports of up-to-date results
- Clients are automatically sent patches using SMS distribution features (with status reports)

SMS Architecture

Download Center /
Office Update, etc.



Scheduled
Scan Tool, &
Database
Updates

MSSecure.XML, etc.

Patches, QFEs, SRPs, etc.

Internet

Intranet

MMC / Patch Wizard,
Status Messages /
Inventory

Web Reports

Managed Corporate
Servers,
Workstations and
Laptops

SMS 2.x
Site Infra-
structure

Scan Tool + Inventory Collection

Scan Tool + Install Applicable Patches

SMS Value Pack

Patch Management Benefits

- Support for download level platforms
  - Windows NT 4.0, Windows 2000, Windows XP
- Support for Windows Updates (critical, non –critical, and service packs)
- Support of Office Updates
- Any patch that can be reported by HFNetChk can be distributed
- Consistent SW Distribution across the enterprise
- Detailed logging and status reporting

SUS / SMS Value Pack

Positioning

- Microsoft's "A" recommendation for which tool to use:

	Recommended Technology to deploy critical updates
Home User	Windows Update
Small Business	Windows Update**
Medium Enterprise	Software Update Services
Large Enterprise	SMS

- **Small Business that work with a VAP should also consider SUS
- Official external positioning is available at: http://www.microsoft.com/windows2000/windowsupdate/sus/suschoosing.asp
- Please attend WINCT303 for a discussion on SW Distribution Positioning, Deployment Issues and Futures

Microsoft Baseline Security Analyzer 1.0

HFNetChk

- HFNetChk is a Command Line executable for Microsoft® Windows NT®, Windows® 2000, and Windows XP
- Scans local and remote computers
- Checks status of security patches for:
  - Windows NT 4.0, Windows 2000, and Windows XP
  - Internet Explorer 5.01 and later versions
  - IIS 4.0 and 5.0
  - SQL 7.0 and later versions
- HFNetChk Webcast for additional Information
  - http://support.microsoft.com/default.aspx?scid=%2Fservicedesks%2Fwebcasts%2Fwc040902%2Fwcblurb040902%2Easp
- HFNetChk Tool Available for Download
  - http://support.microsoft.com/default.aspx?scid=kb;en-us;Q303215
- Knowledge Base Articles
  - Q305385, Q303215, Q315665

Microsoft Baseline Security Analyzer Version 1.0

- Graphical and command line versions
- Presents security report card
  - Overall machine grade
  - Pass/fail score per security check
  - Instructions on fixing vulnerabilities found
- Tool is “read-only” – no remote configuration of machines being performed
- User must have local Administrative access on each scanned machine

Microsoft Baseline Security Analyzer Version 1.0

- Single executable that runs on Windows 2000 and Windows XP
- Performs local and remote scans against Windows NT 4, Windows 2000, and Windows XP systems
- Checks for common security mis-configurations and missing hotfixes or service packs
  - Windows
  - IIS 4 & IIS 5
  - SQL 7 & SQL 2000
  - Desktop applications
    - Internet Explorer
    - Office
    - Outlook

Microsoft Baseline Security Analyzer Usage Scenarios

- Administrators can install MBSA on a single machine and remotely scan their entire network for potential OS and application vulnerabilities
  - Individual machine reports created on the machine hosting MBSA
- Home users can scan their local machines for missing hotfixes and Windows specific security settings
- Network administrators can use the command line version to do scheduled scans of their networks on a regular basis

Microsoft Baseline Security Analyzer Roadmap

- Version 1 Public Release now Available
- Free web download at http://www.Microsoft.com/security
  - Support available through Microsoft PSS
- Version 2 plans under development
  - Support for Windows .NET Server
  - Additional Microsoft application checks
  - Localization to additional languages

Security Tool Relationships

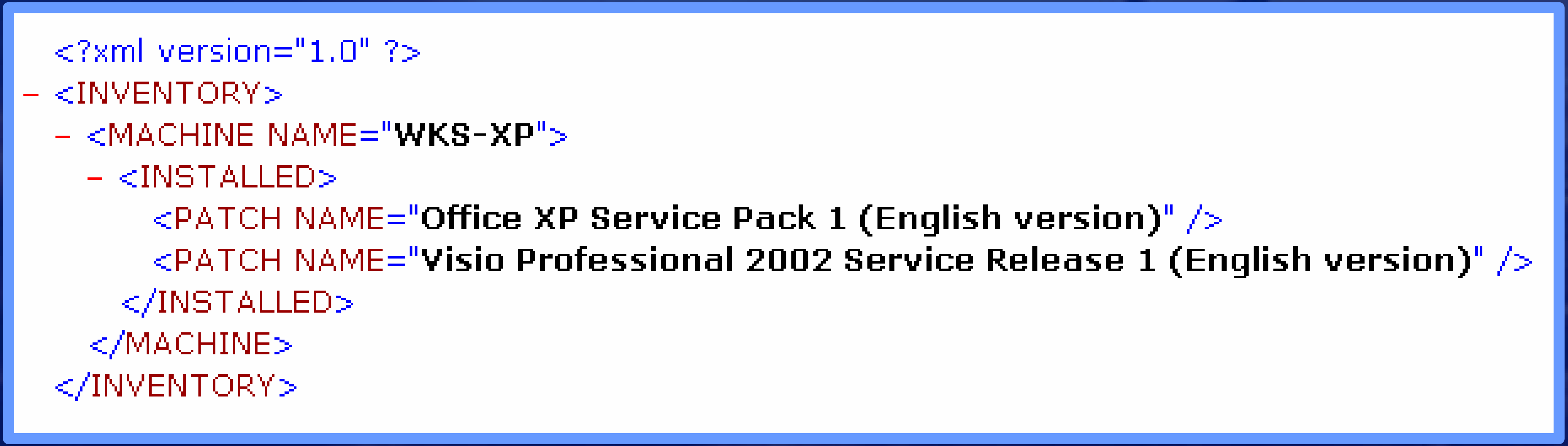
- MBSA replaces the Microsoft Personal Security Advisor (MPSA)
  - MBSA scans both servers and workstations locally and remotely
  - MBSA is a superset of the MPSA tool checks
- MBSA includes a version of HFNetChk for detection of missing hotfixes

Summary

- The MBSA provides…
  - An easy way to scan individual or multiple computers for vulnerabilities and missing patches or hotfixes
  - An easy to use graphical interface for individual home or corporate use
  - A command line interface that administrators may call from a batch file or use in a regularly scheduled job

Office Update Inventory Tool

- Survey the status of Office updates
  - Office 2000 and Office XP
- Command Line Utility
- Office Update Inventory Tool Readme (Q312982)
- Create Patch Status as XML File
- Future Version of MBSA Support Office



```
  <?xml version="1.0" ?>
- <INVENTORY>
  - <MACHINE NAME="WKS-XP">
    - <INSTALLED>
        <PATCH NAME="Office XP Service Pack 1 (English version)" />
        <PATCH NAME="Visio Professional 2002 Service Release 1 (English version)" />
      </INSTALLED>
    </MACHINE>
  </INVENTORY>
```

Security Resources

- Microsoft Security Tools
  - Microsoft Baseline Security Analyzer, EFS Security Tool,URLScan,HFNetChk, IIS Lockdown....
  - Security Checklists
  - HotFix & Security Bulletin Service
  - Product Security Notification
  - http://www.microsoft.com/technet/security
- We Need Your Feedback
  - secfdbck@microsoft.com

Microsoft's Commitment

"To do everything possible to make certain that every customer can work, communicate, and transact securely over the Internet."

Brian Valentine
Senior Vice-President
Microsoft Corporation

Microsoft®