Windows Server 2008 Feature Components

Acronyms

- **API** Application Programming Interface
- **CAPs** Connection Authorization Policies
- **DHCP** Dynamic Host Configuration Protocol
- **DNS** Domain Name Service
- **FVEK** Full Volume Encryption Key
- **HTTP** Hypertext Transfer Protocol
- **IIS** Internet Information Services
- **LOB Applications** Line of Business Applications
- **MMC** Microsoft Management Console
- **NAP** Network Access Protection
- **NAT** Network Address Translation
- **NPS** Network Policy Server
- **RAPs** Resource Access Policies
- **RDP** Remote Desktop Protocol
- **SHA** System Health Agent
- **SHV** System Health Validator
- **SoH** Statement of Health
- **TPM** Trusted Platform Module
- **TS** Terminal Services
- **VHD** Virtual Hard Disk
- **VM** Virtual Machine
- **VMK** Volume Master Key
- **VMM** Virtual Machine Manager
- **VSC** Virtualization Service Consumer
- **VSP** Virtualization Service Provider
- **VSS** Volume Shadow Copy Service
- **WAS** Windows Activation Service
- **WinPE** Windows Pre-execution Environment
- **WinRE** Windows Recovery Environment
- **WMI** Windows Management Instrumentation
- **WWW** World Wide Web
- **XML** eXtensible Markup Language

Legend

- Information
- Important
- Information Bullet
- User
- User Groups
- Service Account
- Client(s)
- User Token
- Active Directory Forest
- Firewall
- Internet
- Management Console
- Restore Backup Wizards
- Backup Server
- Domain Controller
- Web Server
- DHCP Server
- File Server
- BitLocker
- Federation Server
- Monitoring
- Server Core
- Server Manager
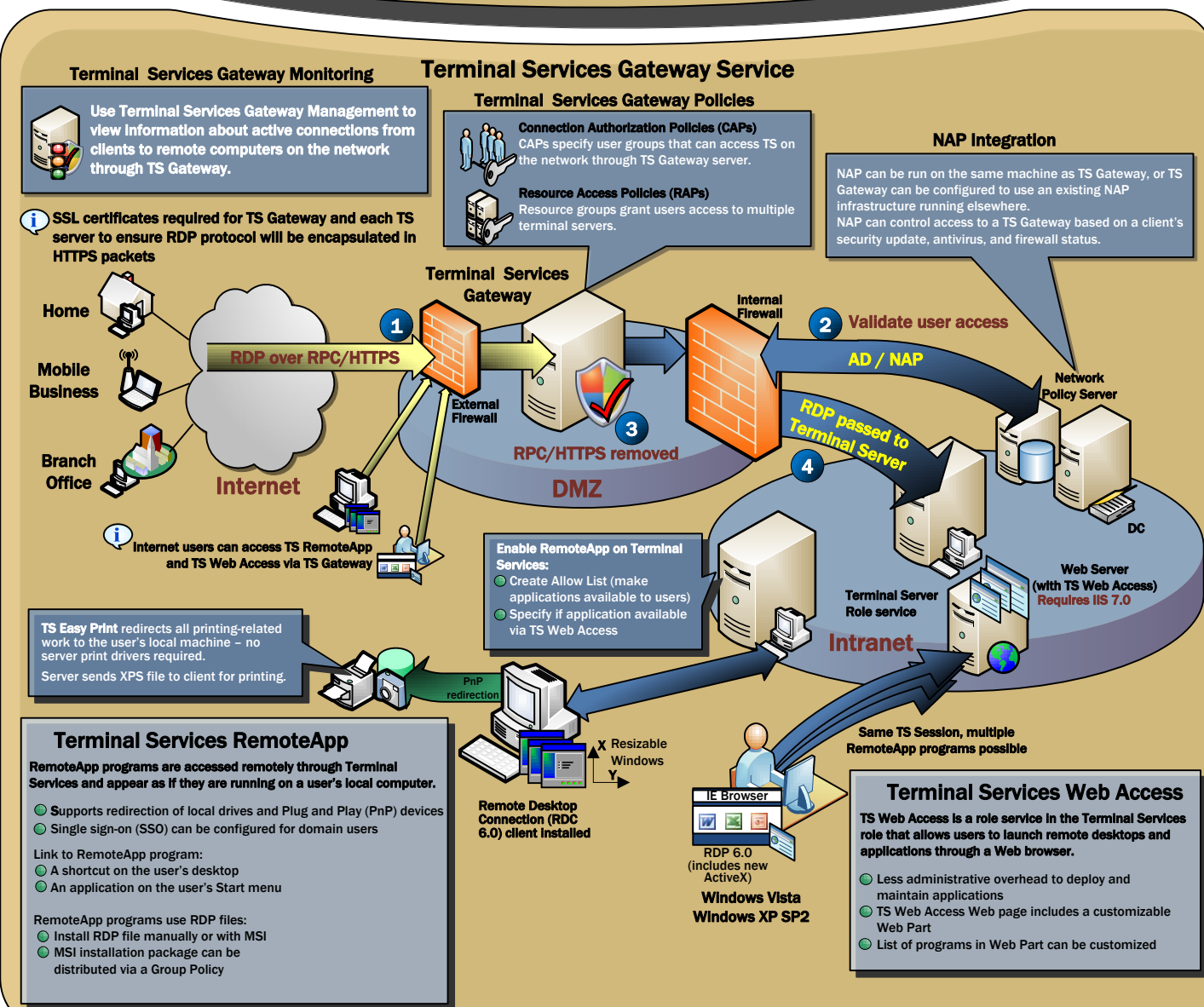- Terminal Services
- Terminal Services Gateway
- TS Web Access

Terminal Services
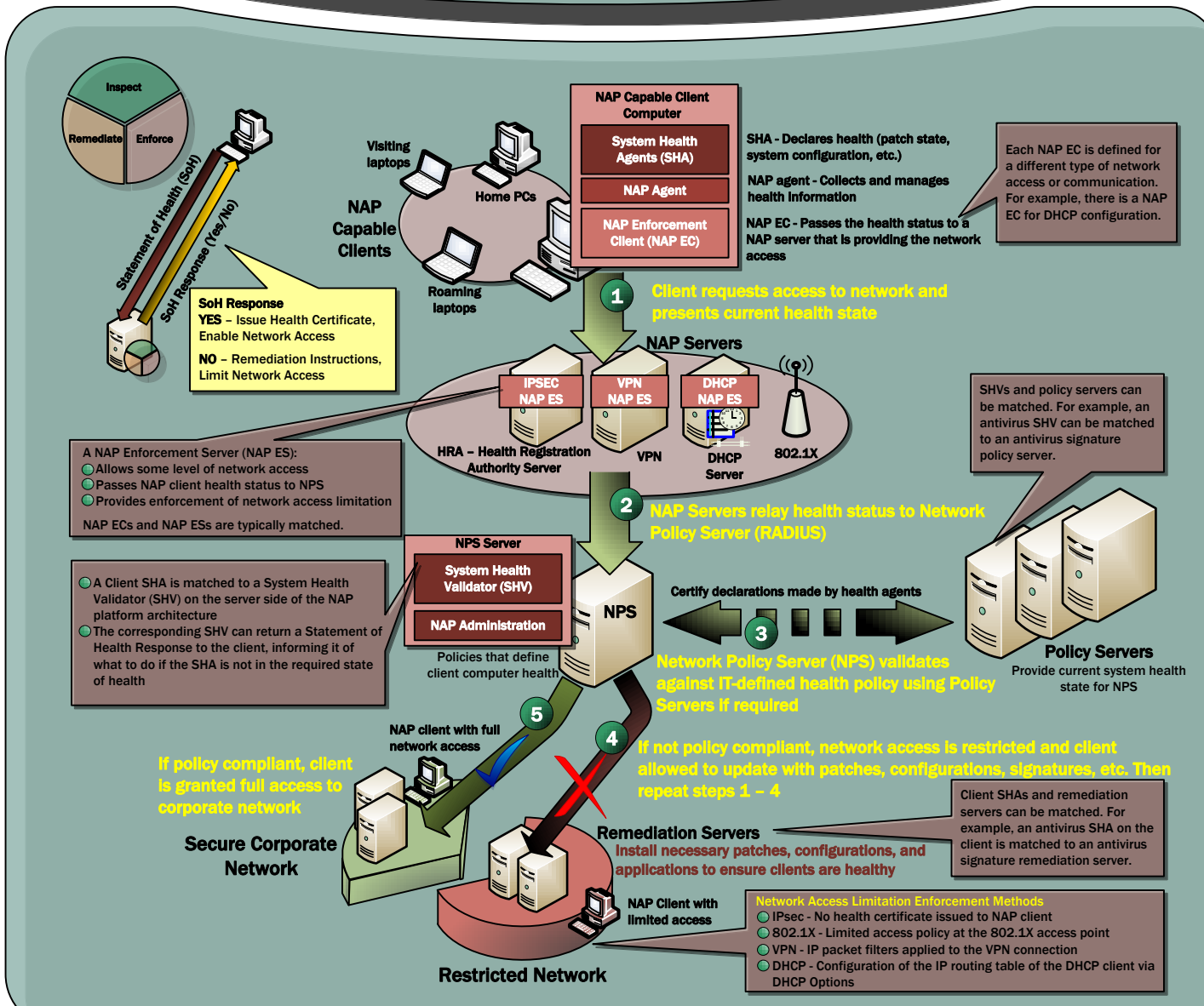### Product Scenario: Centralized Application Access

Terminal Services provides access to Windows-based programs from a variety of devices. Terminal Services is enhanced with Terminal Services RemoteApp, Terminal Services Web Access, and Terminal Services Gateway.

Terminal Services Gateway Service

SSL certificates required for TS Gateway and each TS server to ensure RDP protocol will be encapsulated in HTTPS packets.

Terminal Services RemoteApp

RemoteApp programs are accessed remotely through Terminal Services and appear as if they are running on a user's local computer.

- Supports redirection of local drives and Plug and Play (PnP) devices
- Single sign-on (SSO) can be configured for domain users

Terminal Services Web Access

TS Web Access is a role service in the Terminal Services role that allows users to launch remote desktops and applications through a Web browser.

Network Access Protection
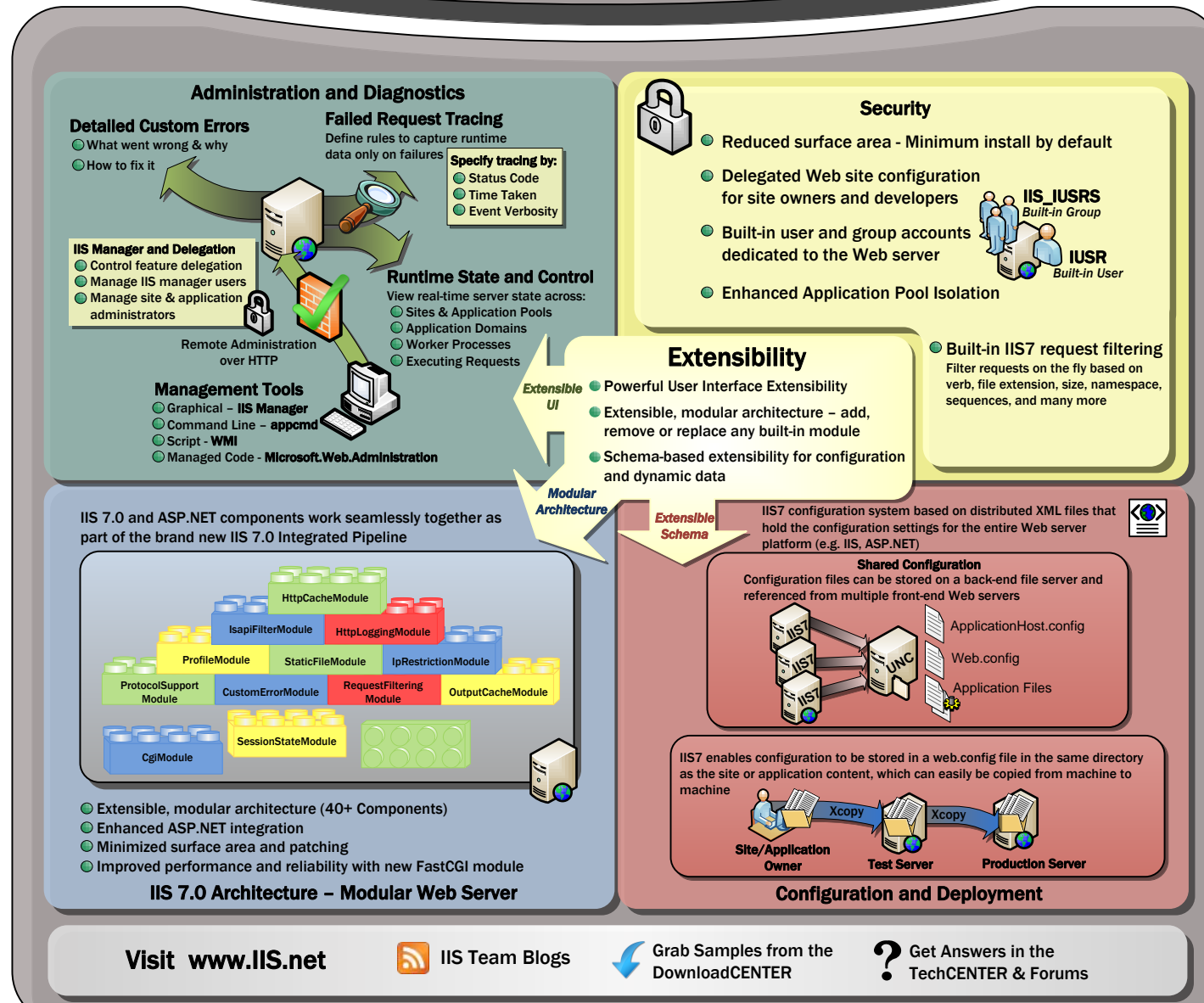### Product Scenario: Security and Policy Enforcement

Network Access Protection (NAP) is a client health policy creation, enforcement, and remediation technology. NAP defines the required configuration and update conditions for a client computer's operating system and critical software.

NAP Servers

Network Policy Server (NPS) validates against IT-defined health policy using Policy Servers if required.

If policy compliant, client is granted full access to corporate network.

If not policy compliant, network access is restricted and client allowed to update with patches, configurations, signatures, etc. Then repeat steps 1 – 4.

Remediation Servers — Install necessary patches, configurations, and applications to ensure clients are healthy.

Internet Information Services 7.0
Product Scenario: Web & Applications Platform

A secure, easy-to-manage server platform for developing and reliably hosting Web applications.

Administration and Diagnostics

- Detailed Custom Errors
- Failed Request Tracing
- IIS Manager and Delegation
- Management Tools — Graphical – IIS Manager, Command Line – appcmd, Script – WMI, Managed Code – Microsoft.Web.Administration
- Runtime State and Control

Security
- Reduced surface area - Minimum install by default
- Delegated Web site configuration for site owners and developers
- Built-in user and group accounts dedicated to Web publishing
- Enhanced Application Pool Isolation

Extensibility
- Powerful User Interface Extensibility
- Extensible, modular architecture – add, remove or replace any built-in module
- Schema-based extensibility for configuration and dynamic data

IIS 7.0 Architecture – Modular Web Server

Visit www.iis.net

Virtualization
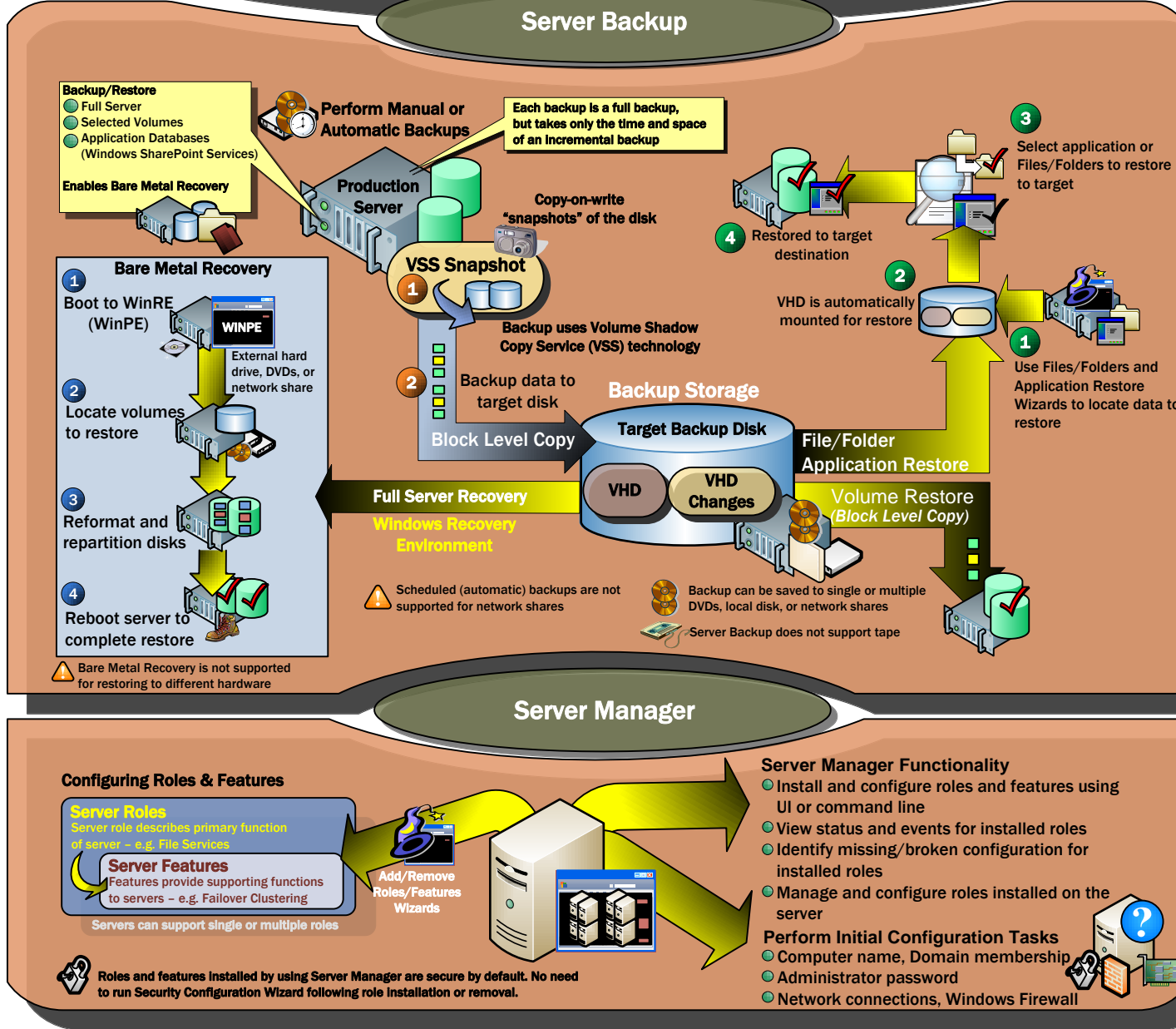### Product Scenario: Server Virtualization

Windows Server 2008 includes Windows Server Virtualization. Windows Server Virtualization is a 64-bit hypervisor-based virtualization technology that facilitates agility and integrated management of both physical and virtual components.

Microsoft System Center Virtual Machine Manager
- Built on Windows Powershell
- Manages Virtual Server 2005 R2 and Windows Server 2008

Microsoft System Center Operations Manager — Monitor Physical and Virtual Machines

Windows Hypervisor
- Thin layer of software running on the hardware
- Supports creation/deletion of partitions
- Enforces memory access roles
- Enforces policy for CPU usage
- Virtual processors are scheduled on real processors
- Enforces ownership of other devices

Partitions
- Each partition is a virtual machine
- Each partition has one or more virtual processors
- Partitions share hardware resources
- Software running in partition is called a guest

"Designed for Windows" Server Hardware — AMD-V or Intel VT Processor with Data Execution Prevention enabled

Server Manager and Server Backup
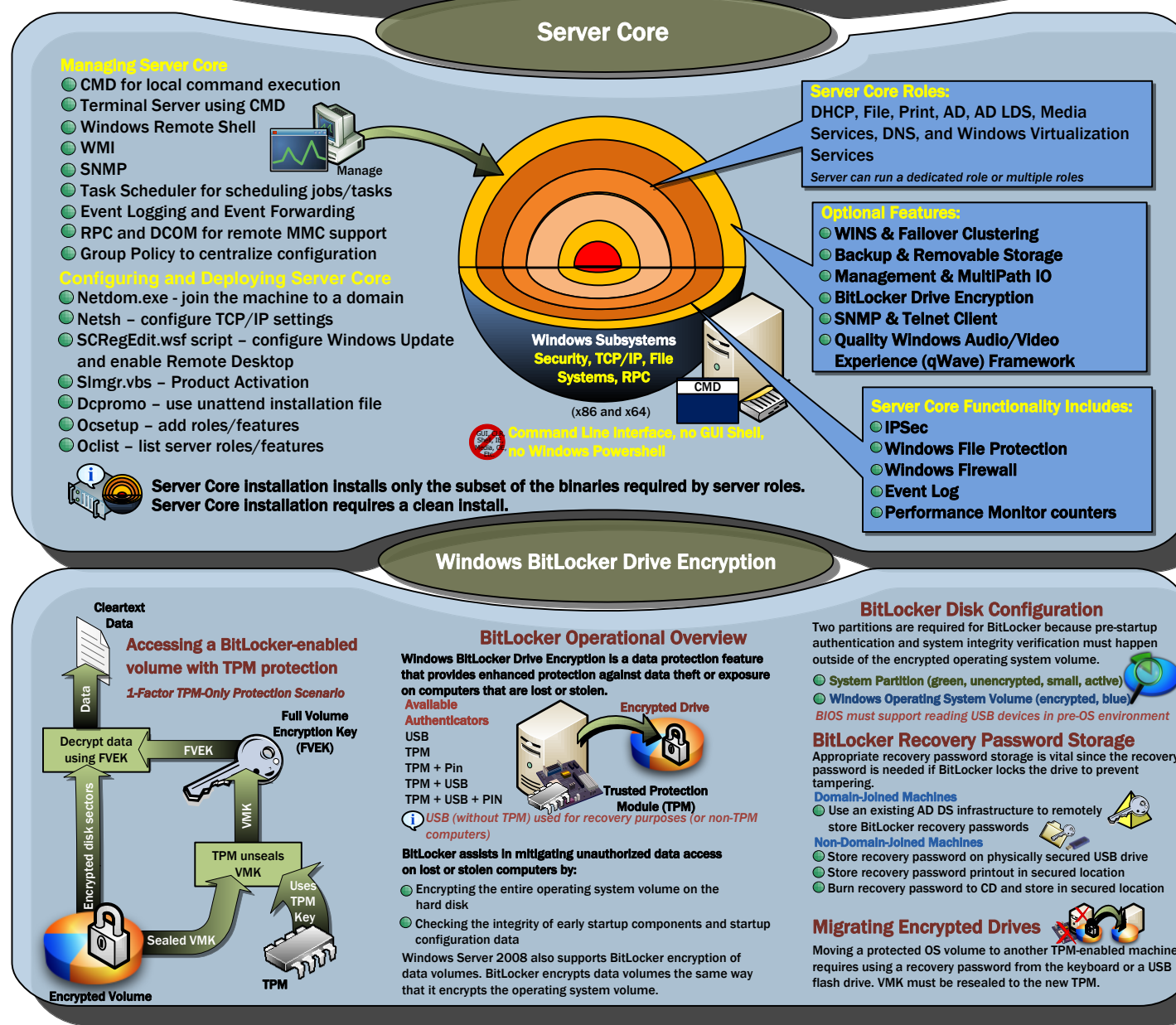### Product Scenario: Server Management

Server Manager provides server configuration and commands for managing roles and features. Server Backup feature provides backup and recovery solutions.

Server Backup
- Full Server
- Selected Volumes
- Application Databases (Windows SharePoint Services)
- Enables Bare Metal Recovery

Perform Manual or Automatic Backups

Each backup is a full backup, but takes only the time and space of an incremental backup.

Bare Metal Recovery
1. Boot to WinRE (WinPE)
2. Locate volumes to restore
3. Reformat and repartition disks
4. Reboot server to complete restore

Server Manager Functionality
- Install and configure roles and features using UI or command line
- View status and events for installed roles
- Identify missing/broken configuration for installed roles
- Manage and configure roles installed on the server

Perform Initial Configuration Tasks
- Computer name, Domain membership
- Administrator password
- Network connections, Windows Firewall

Server Core & BitLocker
Product Scenario: Branch Office

Server Core installation option provides a minimal environment for running specific server roles, reducing servicing, management requirements, and the attack surface for those server roles. Windows BitLocker Drive Encryption protects data by encrypting the entire Windows volume.

Server Core
- CMD for local command execution
- Terminal Server using CMD
- Windows Remote Shell
- WMI
- SNMP
- Task Scheduler for scheduling jobs/tasks
- Event Logging and Event Forwarding
- RPC and DCOM for remote MMC support
- Group Policy to centralize configuration

Server Core Roles:
DHCP, File, Print, AD, AD LDS, Media Services, DNS, and Windows Virtualization Services

Optional Features:
- WINS & Failover Clustering
- Backup & Removable Storage
- Management & MultiPath IO
- BitLocker Drive Encryption
- SNMP & Telnet Client
- Quality Windows Audio/Video Experience (qWave) Framework

Server Core Functionality includes:
- IPSec
- Windows File Protection
- Windows Firewall
- Event Log
- Performance Monitor counters

Windows BitLocker Drive Encryption

BitLocker Operational Overview — Windows BitLocker Drive Encryption is a data protection feature that provides enhanced protection against data theft or exposure on computers that are lost or stolen.

BitLocker Disk Configuration — Two partitions are required for BitLocker because pre-startup authentication and system integrity verification must happen outside of the encrypted operating system volume.

BitLocker Recovery Password Storage — Appropriate recovery password storage is vital since the recovery password is needed if BitLocker locks the drive to prevent tampering.

Migrating Encrypted Drives — Moving a protected OS volume to another TPM-enabled machine requires using a recovery password from the keyboard or a USB flash drive. VMK must be resealed to the new TPM.