

SSL VPNs or IPsec VPNs

The Challenges of Remote Access

February 2nd, 2007

Chris Witeck- Director of Product Marketing



Agenda

- Remote access challenges
 - Drivers for remote access
 - New challenges for IT
- Remote access defined
 - Niche use case?
 - How to provide Remote Access Control
- Remote Access Control defined
 - Basic deployment for SSL VPNs
 - How SSL VPNs address remote access security concerns
- The Aventail approach

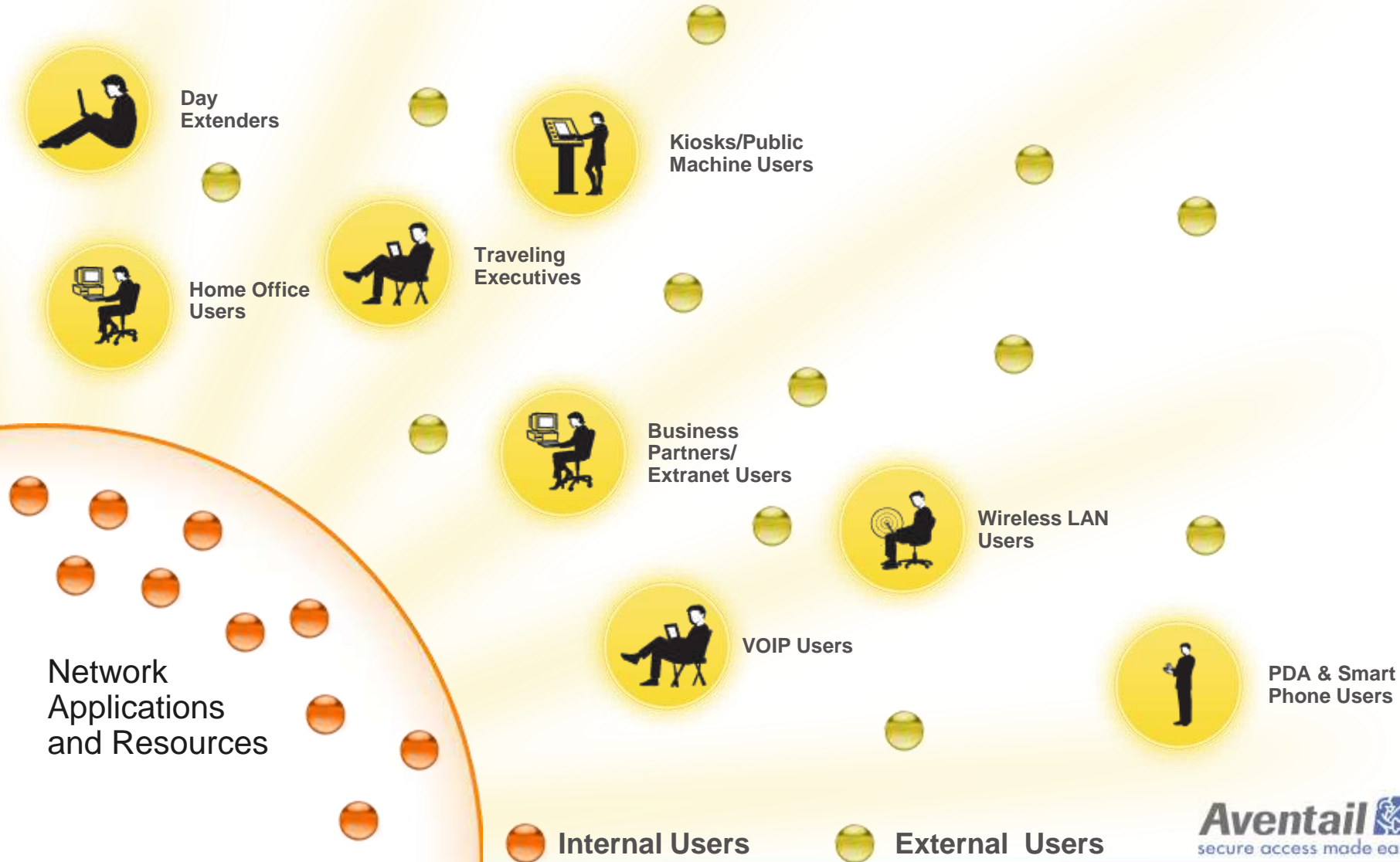
It's a New World

Fundamental Changes in Technology

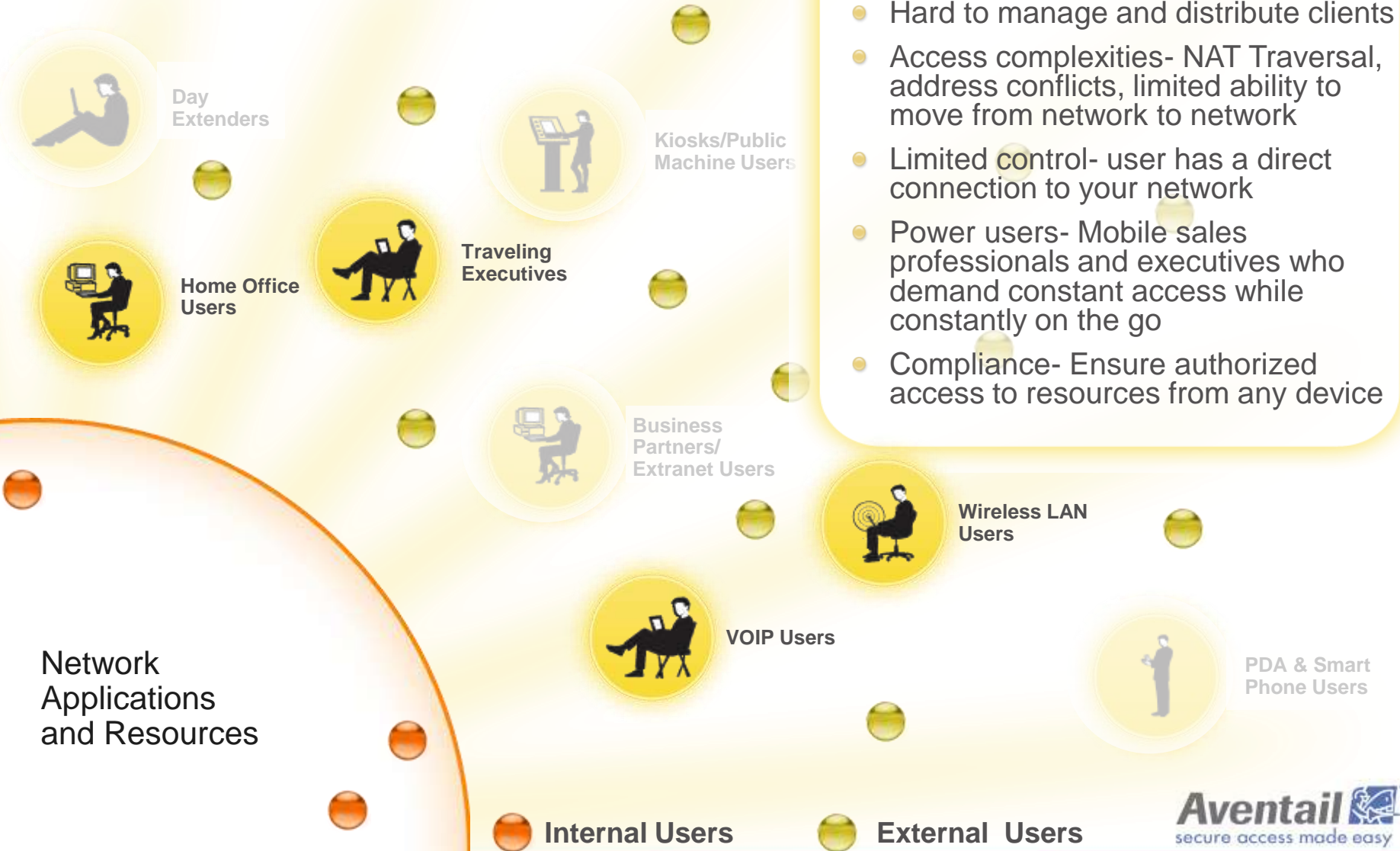
- Ubiquity of broadband
- Proliferation of mobile devices
- Rise in IP telephony
- Increased teleworking



Users are Increasingly Out of Your Control



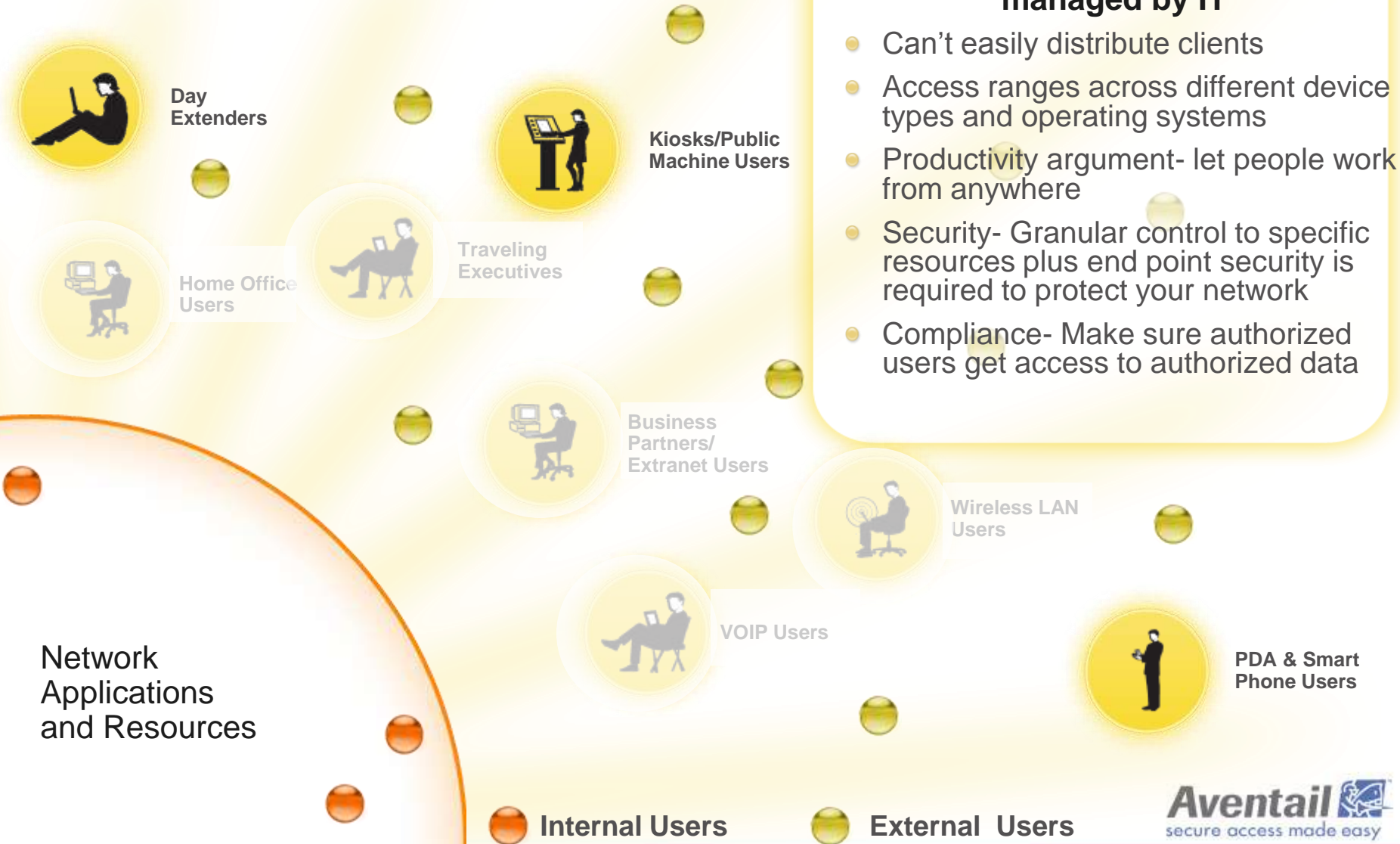
Users are Increasingly Out of Your Control



Challenges with IT Managed devices

- Hard to manage and distribute clients
- Access complexities- NAT Traversal, address conflicts, limited ability to move from network to network
- Limited control- user has a direct connection to your network
- Power users- Mobile sales professionals and executives who demand constant access while constantly on the go
- Compliance- Ensure authorized access to resources from any device

Users are Increasingly Out of Your Control



Users are Increasingly Out of Your Control



Challenges with Extranets/Business Partner Access

- No access to devices
- No responsibility for the user gaining access
- Productivity argument- Let your partners collaborate with your employees
- Security argument- Need to control access to specific applications and nothing else

Users are Increasingly Out of Your Control



Day Extenders



Kiosks/Public Machine Users



Traveling Executives



Home Office Users



Business Partners/
Extranet Users



Wireless LAN Users



VOIP Users



PDA & Smart Phone Users

Network Applications and Resources

More...

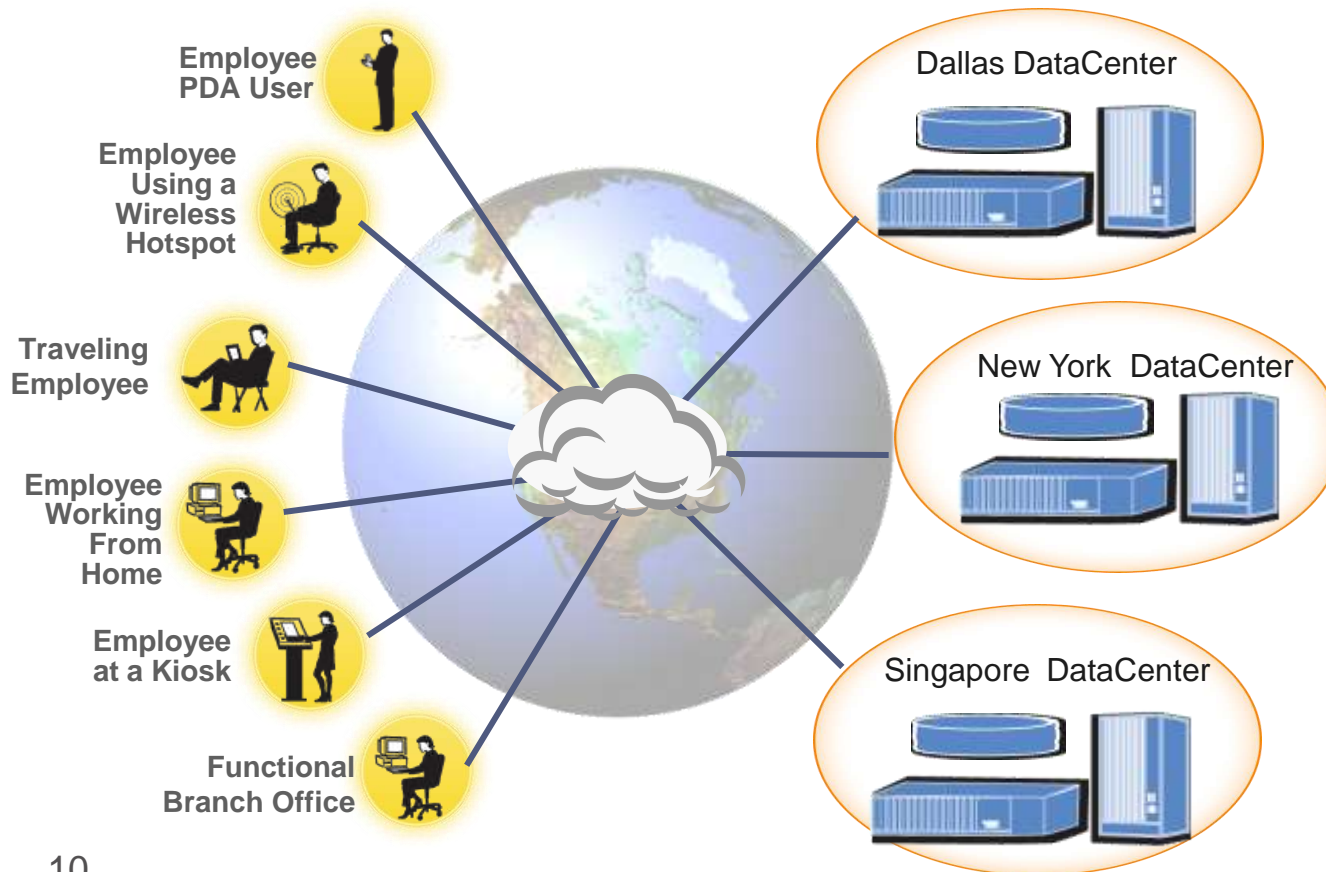
- Users
- Devices
- Network environments
- Mobility
- Remote access

Internal Users

External Users

The Disaster Recovery Challenge

Business continuity and remote access go hand in hand, as typical business disruptions result in employees and other users staying away from the office and the local area network (LAN).— *Tim Clark, Fact Point Group*



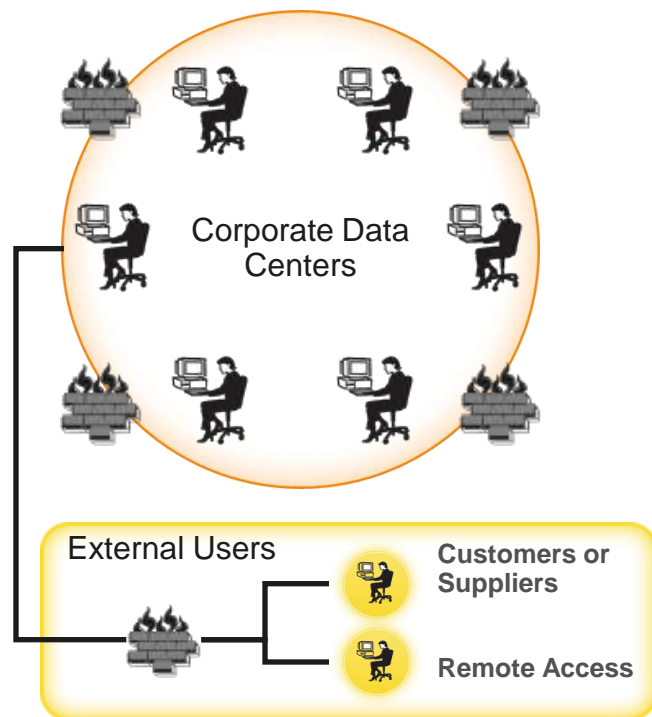
Disaster Recovery & Business Continuity:

- Providing access to relevant information
- Keeping the network up
- Maintaining productivity
- Protecting revenue
- Assuring regulatory compliance
- Allowing access from anywhere

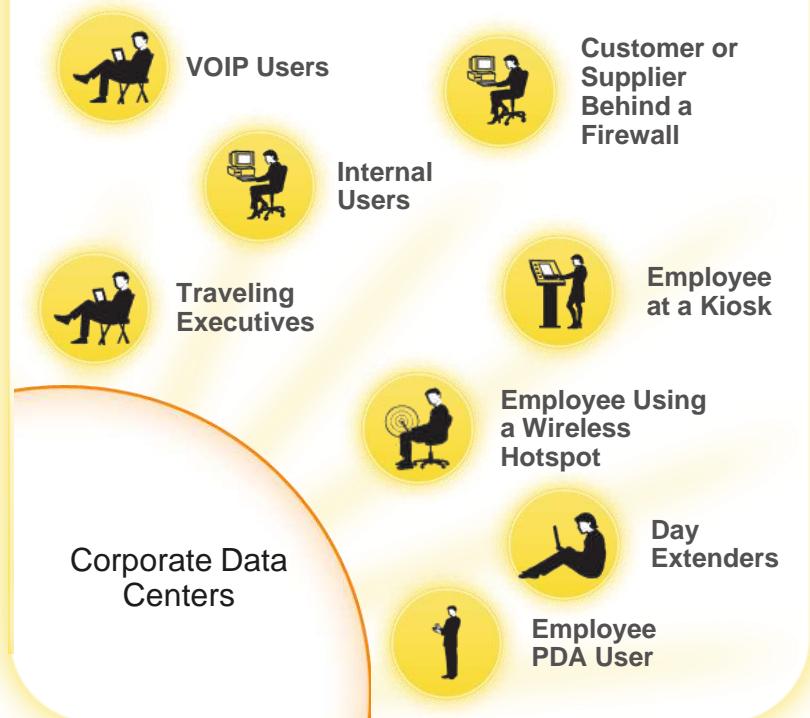
The Business Impact

Most of your network traffic will be coming from outside the private network you are trying to secure

1997: Network Perimeter



2007: Resource Perimeter



Future Enterprise Networks Model E-commerce

Enterprise networks of the future will look more like Internet businesses than traditional multinationals

1997: Network Perimeter



2007: Resource Perimeter



Enterprises Need a New Reference Architecture

What's the Pain Point?

Remote Access

Give all employees remote access solution that is easy to use and deploy.

Disaster Recovery

During a business disruption, demand for remote access could spike to include the majority of your workforce.

Securing Wireless Networks

Many organizations treat users on the wireless network as remote users because of concerns over who has access to the wireless network.

Extranet Access

Open access to partners to increase collaboration, yet do it in such a way that access control and security is not compromised.

Mobility

Mobile devices are increasingly functional for both data and voice, leading to a rise of IT managed (and non-managed) mobile devices used for voice and data.

Enforcing Policy

Collaboration and compliance is encouraging granular access controls, yet IT struggles to enforce policy across disparate points of entry

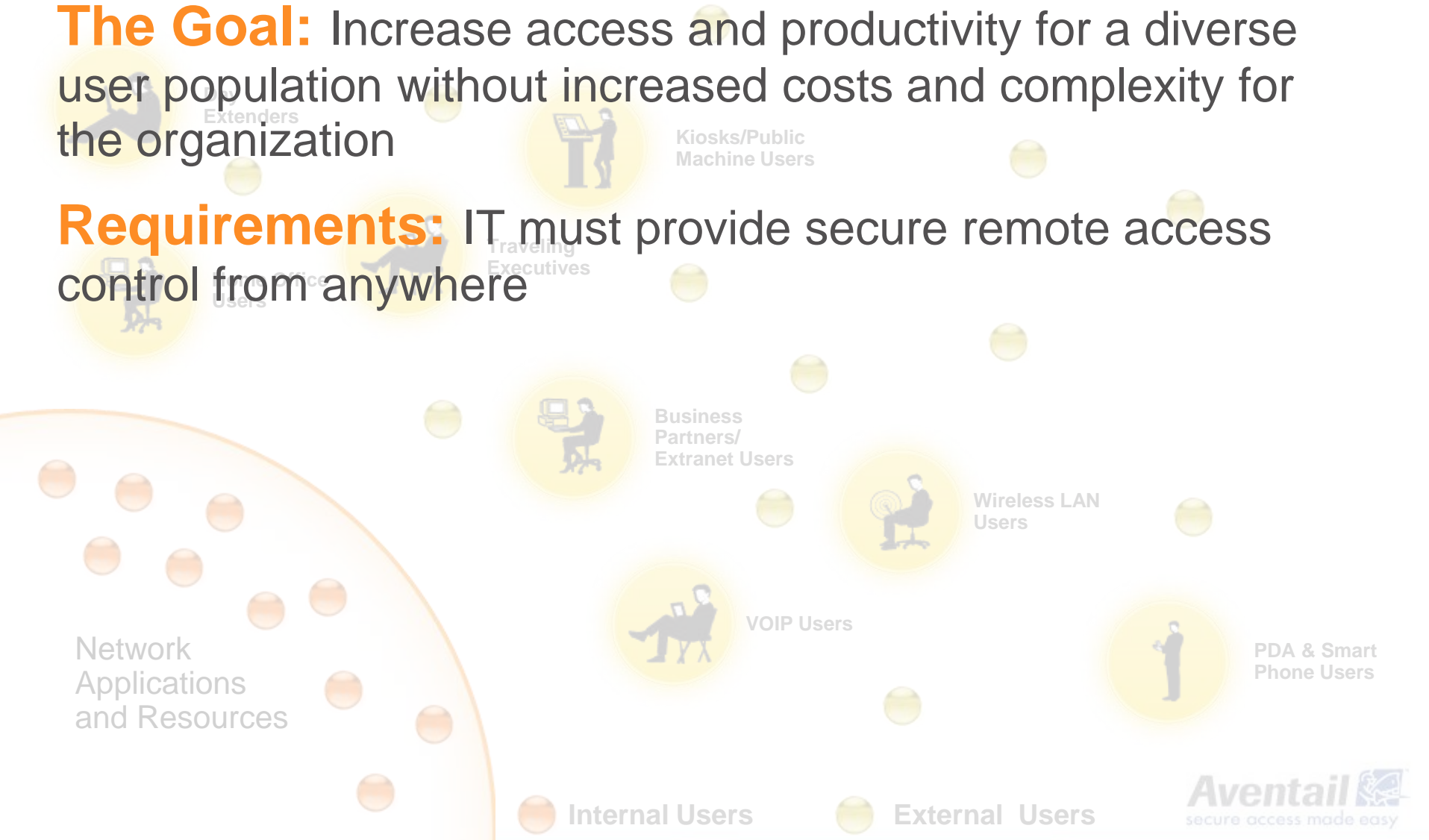
Network Access Control (NAC)

NAC is positioned around host integrity checking and network access, yet many organizations want to extend that to cover application access control as well.

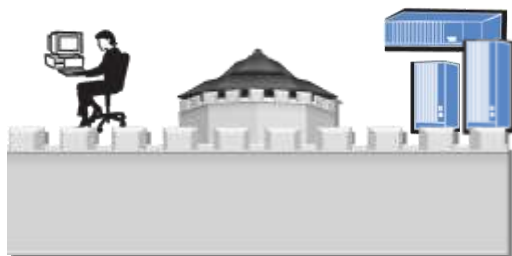
New Requirements for IT

The Goal: Increase access and productivity for a diverse user population without increased costs and complexity for the organization

Requirements: IT must provide secure remote access control from anywhere



Two Approaches Towards Providing Control



Smarter Networks

The network can be made smart, if you try hard enough

- Networks can be made intelligent and secure – at a cost \$\$\$
- More firewalls, more private infrastructure
- Retrofit Infrastructure to ensure security

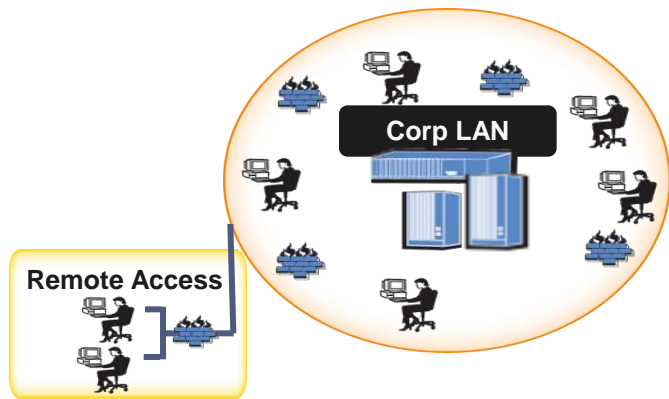


Smarter Access

The network is dumb, and will remain dumb

- Drive secure communications
- Assume the network is insecure
- Leverage public networks, shared infrastructure
- Focus investments on the reliability and transparency of service

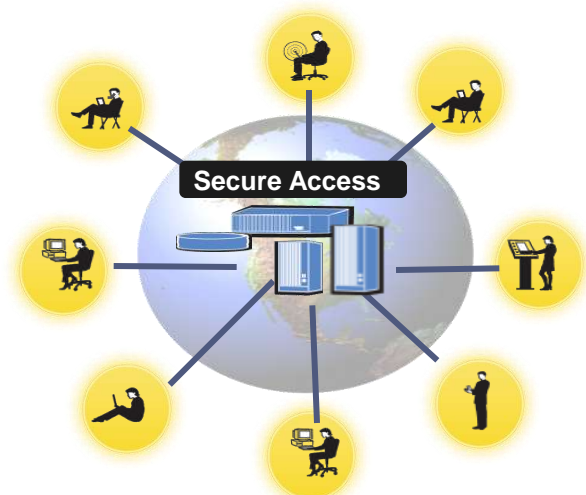
Leading Towards a Different Definition of Remote Access



Smarter Networks

Remote access is a niche use case

- Marginalizes remote access: all about Network Access
- Focus on optimization of traffic with less emphasis on granular policy & end point control
- Manage access by protocol/technology



Smarter Access

Everything is remote

- Remote access is a discrete (and very large) market
- Focus on access/ end point control with less emphasis on network optimization
- Manage access by policy

Is NAC the Answer?

Network Access Control (NAC): Allows network administrators to authenticate, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto *the network*

Challenges with this definition: NAC defined this way is a good concept but it is also:

- Complex- definitions and approaches vary by vendor
- Difficult to implement
- Not yet baked or available
- Expensive
- LAN focused- marginalizes remote access
- Limited focus extending policy to the applications and resources themselves

To Achieve Remote Access Control, What do You Need to Know?

All enterprise communication can be managed and secured if you answer these three questions

1. Who is the user?

Proof as to who the user is without question, based on a strong authentication method

2. What's happening on the end point?

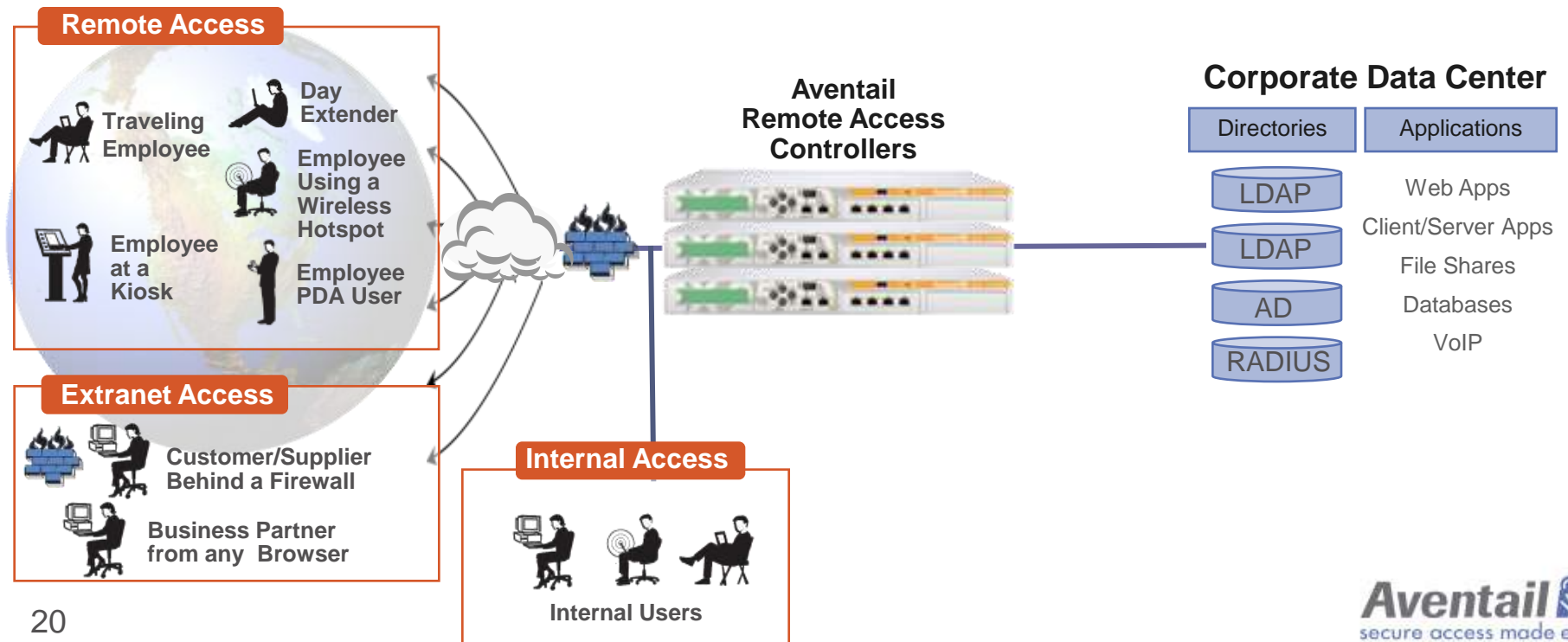
A clear understanding of what is happening on the user's end point to make a policy decision, then classify that device accordingly

3. What are the resources the user is seeking?

Knowledge of what applications the user wants access to, and then grant access according to policy

Remote Access Control is the Answer

SSL VPNs provide secure, remote access control for all users from all devices

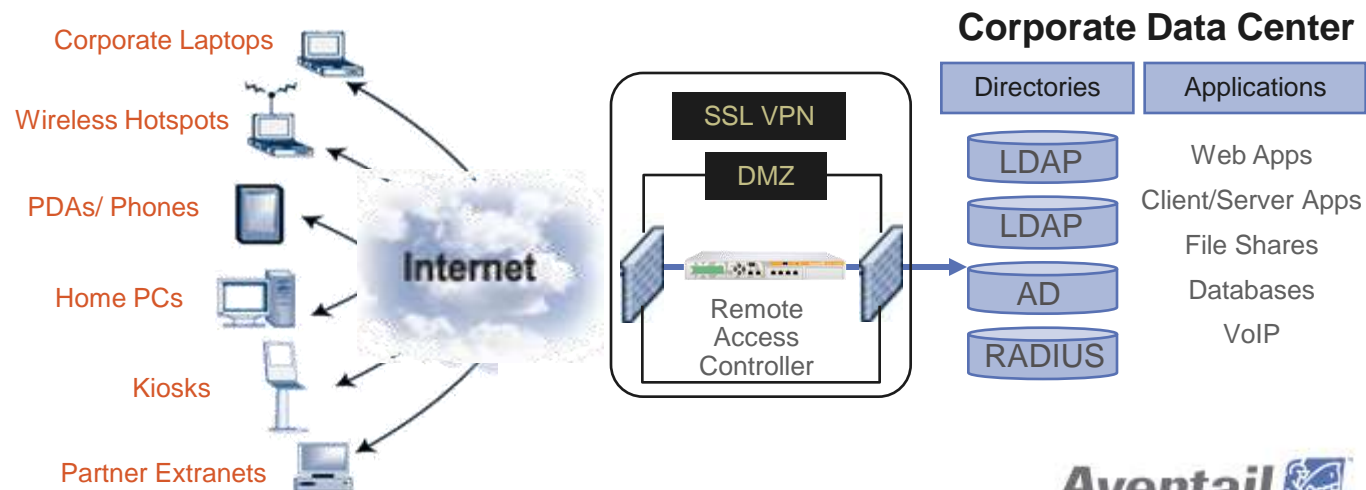


Basic Deployment

SSL VPNs use SSL & strong access control to deliver authorized and secure access to Web, client/server, and file shares

- SSL VPN tied to authentication system, DNS and applications
- Presents web resources and available shares as links to the user
- Authenticates users, encrypts to the end node, applies granular ACLs to the user traffic, detailed audit
- All traffic goes over port 443, regardless of original protocol
- Uses browser-deployed agents to handle C/S applications
- End point interrogation to determine overall trust for the end point device

1. User enters URL for SSL VPN portal from any Internet accessible device
2. The SSL VPN scans end point for O/S, Browser and System Information
3. Access is provided, optimized for the user's end point



SSL VPNs and IPSec VPNs Compared

Compared to traditional remote access via IPSec, SSL VPNs:

- **Are easier and less expensive to deploy and manage:** no complex clients to provision or support
- **Enable employee and partner productivity:** access to any application, from anywhere, via any device
- **Are more secure:** granular access control and end point control
- **Increasingly are replacing IPSec VPNs** as the standard solution for all remote access use cases

Comparison	Result moving to SSL VPN from IPSec
Encryption	No change
Authentication	No change or Improved
Access Control	Improved
Perimeter Profile	Improved
Logging and Forensics	Improved
Web Security	Improved
End-Point Security	No Change or Improved

Remote Access Security Concerns

- **Access from unmanaged locations**
 - Sensitive data inadvertently left on device by legitimate user
 - Sensitive data intentionally captured
 - Unmanaged device is virus entry point to the network
- **Device identification**
 - Difficult to tell provisioned devices from others
- **Application access control**
 - Authenticating the user alone is not enough to determine the appropriate level of access
 - Unmanaged devices should not be a node on the network

Addressing Security Concerns

Access from unmanaged locations

- Sensitive data inadvertently left behind
 - Cache clearing technology
 - Session file encryption and deletion
 - Block attachment downloads for certain devices
 - Restrict location for certain groups
 - Virtual desktop capabilities
 - WTS/Citrix support through SSL VPN
- Data captured (Spyware, Keystroke Logger)
 - Pre-auth scan
 - Virtual keyboard for logon
 - Check status of PFW, A/V and spyware before allowing application access
- Device as a virus entry point
 - A/V and PFW policy enforcement
 - Adjust ACLs when A/V is Absent or not updated
 - Remediate workstation
 - Deny connection based on known threats

Addressing Security Concerns

Device identification

- Restrict source IP
 - Set policy based on source location
- Identify devices based on unique characteristics
 - Domain membership
 - O/S and browser
 - Device Watermark (Device certificate)
 - Mapped directories
 - Secret files
- Change the access policy for provisioned devices vs. unmanaged devices
 - Provisioned devices- full network access
 - Unmanaged- access only via Web portal

Addressing Security Concerns

Application Access Control

- Create “3-D” Security Policy
 - Policy is the intersection of:
 - Trust for the user
 - Trust for the device used for access
 - Applications the user/device wants to access
- Adjust application access on-the-fly based on combination of factors
 - How the user authenticates
 - Device integrity
 - Device identity
 - Time of day

Providing One Gateway for Secure Remote Access

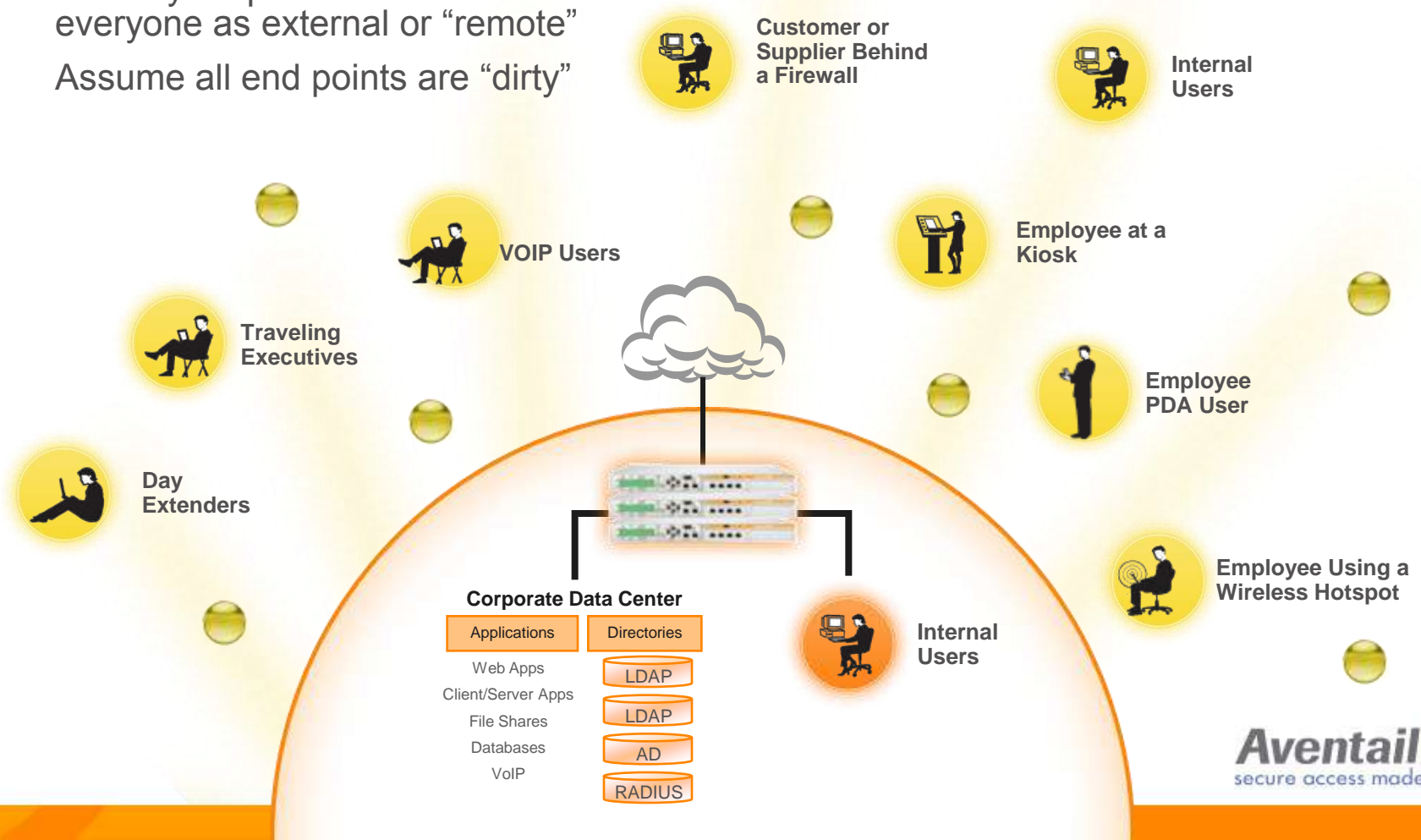
One gateway and a common user experience with centralized management and security



A New Reference Architecture: The Inverted Network

An architecture that always assumes the *underlying network is insecure*

- Shrink your perimeter and treat everyone as external or “remote”
- Assume all end points are “dirty”



What to Look for in an SSL VPN?

The Aventail Approach

Aventail's Remote Access Control Platform

SSL VPNs can...

Easy to Use. Easy to Control.

Detect

Aventail's End Point Control detects the identity and security state of the end device

Protect

Aventail Unified Policy is the enforcement engine, making sure that devices access is controlled and users only access applications they are authorized to access

Connect

Aventail Smart Access & Smart Tunneling is the transport mechanism in NAC, making it easy and secure for users to access all network resources

Detect

End Point Control

Aventail's End Point Control Interrogates managed and non-managed devices prior to connecting in order to identify the device and determine the overall trust level

EPC Device Interrogation

Interrogate by Device Type

- IT Managed
- Non-Managed
- Windows
- Windows Mobile
- Macintosh
- Linux

For Device Identity

- Mapped Directory
- Windows Domain Membership
- Device Watermark/Certificate
- Any Resident File

And Device Integrity

- Malware Scans
- Anti-Virus
- Registry Key
- Windows O/S Level
- Personal Firewall
- Anti-Spyware

With Device Security

- Cache Control
- Secure Desktop

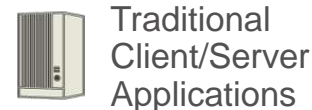
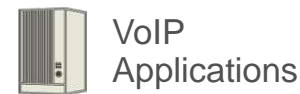
WorkPlace Access
(Clientless Web Access)



Connect Access
(Client-Installed Access)



Corporate Network



Protect

Unified Policy

Aventail's object-based Unified Policy enables application control via easy to setup and manage access rules, covering all devices types and users.

Your Company

Enterprise Admission Control

Define Trust Level for Users

Employee Community
Groups: Sales, Marketing, Executive

Partner Community
Groups: Partners

Define Trust Level for Devices

- Allow
- Quarantine
- Deny

- Allow
- Quarantine
- Deny

- Create allow, deny and quarantine rules easily that govern access for all users and devices based on device identity and device integrity

Application Access Control

Define What Applications Users/Devices can Access

Access Control List			
Application:	CRM App	OWA	Order Entry
User Trust:	Sales, Executive	All in Empl. Community	Sales, Partners
Device Trust:			

- Just one rule set enforces access to all resources across all access methods based on who the user is and the trust level for the device

Connect

Smart Access to Unmanaged Devices

WorkPlace Access: One gateway and a common user experience for access to client server and Web based applications with centralized management and security



Connect

Smart Access to Managed Devices

Connect Agent Access: Easy to provision and manage agents for complete application access for Windows, Macintosh, Linux and Windows Mobile devices



Connect

Connect Mobile

Delivers the 'in-office' experience for Windows Mobile devices: direct access to a broad base of client-server and Web based applications

Benefits

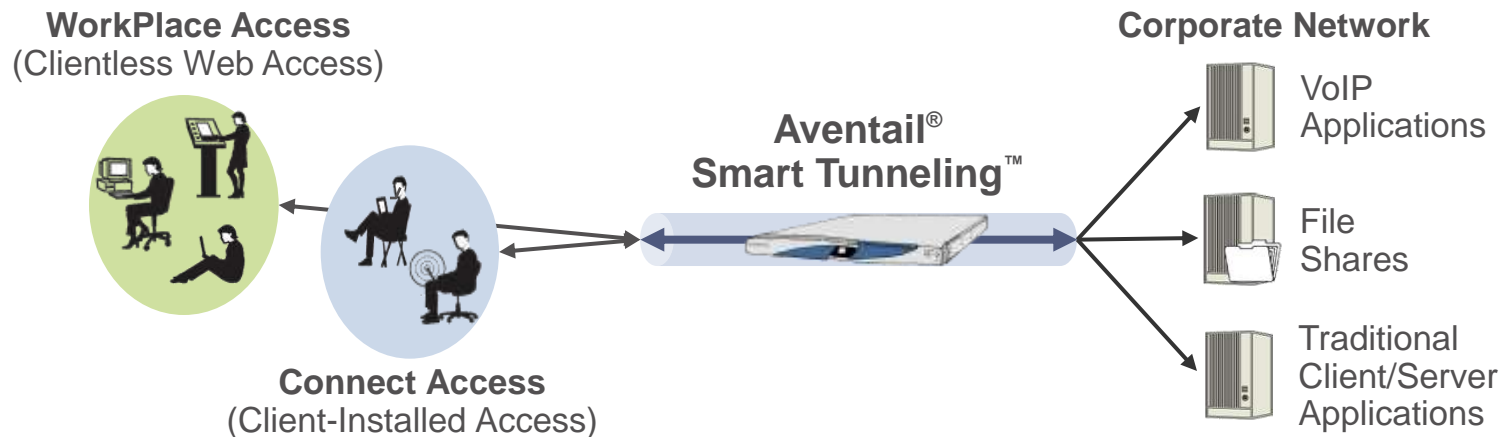
- Use native PIMM applications instead of web interface to OMA/OWA
- Secure, proxied, access-controlled connection to applications & resources
- End Point Control to interrogate the device before allowing access
- Device Watermarking with a certificate for added security and easy revocation if the device is lost
- Authentication: U/P, Token, Certificate
- Embedded Web links active in email
 - External: <http://www.seattletimes.com>
 - Internal: <http://in.mycompany.com/livelinek/roadmap.ppt?func=docfetch>



Connect

Smart Tunneling

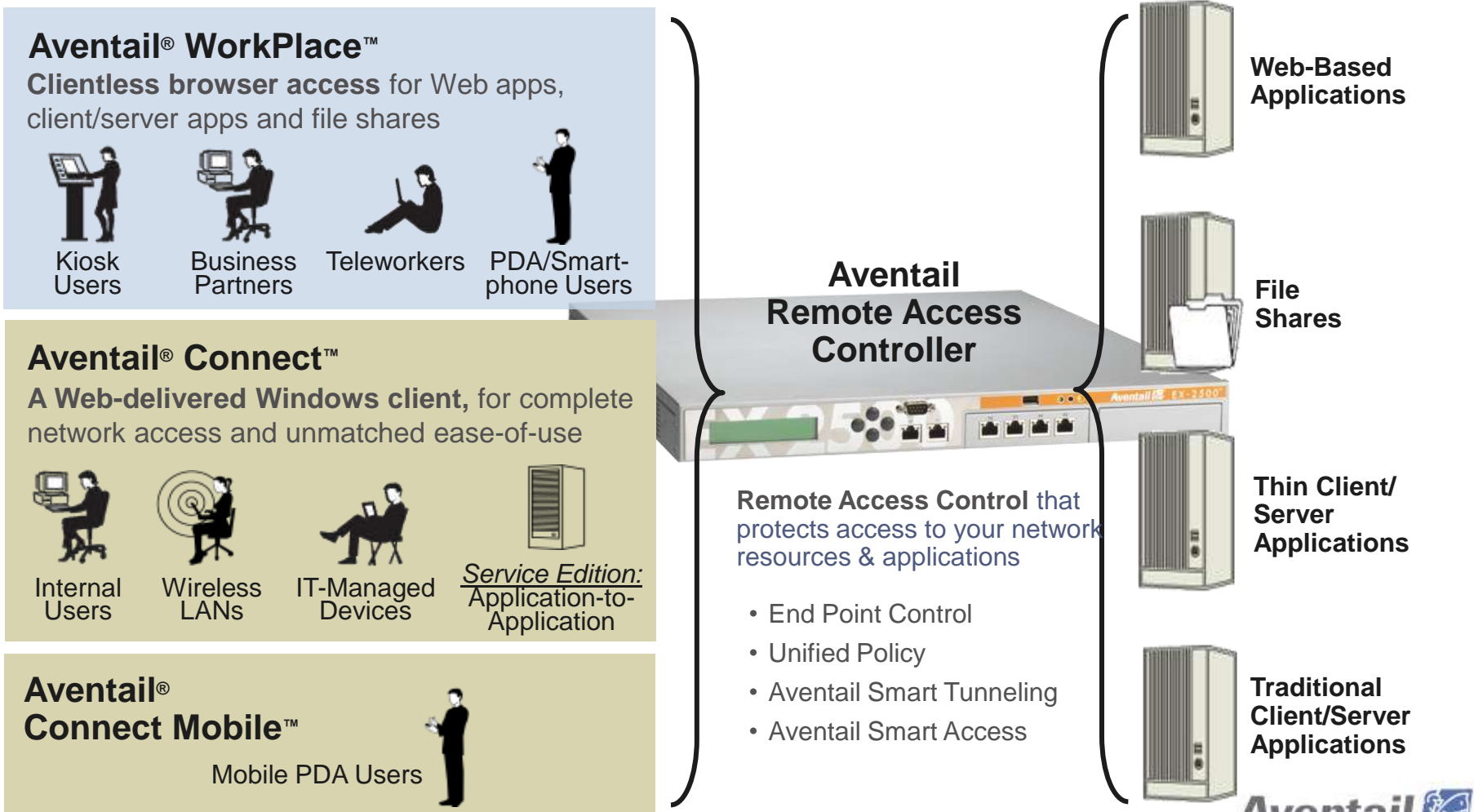
A revolutionary, patent-pending tunneling architecture that provides secure communication to all applications and resources on a network with complete security and control






- ➔ Universal application reach, including complex apps like VoIP
- ➔ Web and client installed options
- ➔ Adaptive addressing and routing
- ➔ Layer 3 tunnel with layers 4 – 7 control, including bidirectional access control
- ➔ Integrated with Aventail's Unified Policy
- ➔ Service edition handles application to application connections

One Secure Gateway for All Remote Access Control

Aventail is the only Remote Access Controller that provides a single solution with centralized management for all devices, applications, and users



Aventail Best-of-Breed SSL VPN Appliances

EX-2500	EX-1600	EX-750
		
<p>For enterprises with hundreds or thousands of remote access users; supports up to 2,000 concurrent users</p>	<p>For midsize companies or enterprise departments; supports up to 250 concurrent users</p>	<p>For small to mid-size companies, an enterprise department or a remote facility; supports up to 50 concurrent users</p>
<p>2 nodes for internal high availability (HA) with integrated load balancing, use external load balancer for up to 8 nodes</p>	<p>Internal high availability (HA) support for 2 nodes, with integrated load balancing</p>	<p>Cost-effective unit for standalone use, with all the advantages of Aventail's best of breed VPN solution</p>

Selected Aventail Customers

Over a 2,000 customers globally rely on Aventail's best-of-breed solution

Healthcare	
Government	
Manufacturing	
Professional Services	
Financial Services & Insurance	
Technology	
Other Industries	

Aventail: The Best-of-Breed SSL VPN Company

- Recognized technology leader
 - Delivering the next generation VPN technology today
 - Investing more in SSL VPN development than any other company
 - SSL VPN pioneer: shipped the first SSL VPN product in 1997

- The most award-winning SSL VPN



In Leader quadrant, Gartner SSL VPN Magic Quadrant – for 5 times



Forrester: Best Secure Remote Application Gateway; SSL VPN leader and strongest pure-play



Frost & Sullivan: Best in Class SSL VPN for Remote Access Connectivity



- Market validation: leading service providers, customers, technology partners, and channel partners rely on Aventail

Thank you

Chris Witeck- Director of Product Marketing

cwiteck@aventail.com

www.aventail.com