Agenda

1. Securing Dynamic Enterprises
2. The Mobile Blind-Spot
3. Alcatel-Lucent’s OmniAccess 3500 Nonstop Laptop Guardian
4. Uses Cases
5. Case Studies
6. Summary and Q&A
## Enterprise Data Portfolio Snapshot

<table>
<thead>
<tr>
<th>Management</th>
<th>IP Address</th>
<th>IP Infrastructure</th>
<th>IP performance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1000.5AC4.3221=192.168.1.10</td>
<td>OmniVista 2500/2700</td>
<td>VitalSuite</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VitalQIP</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data networks</th>
<th></th>
<th>WLAN</th>
<th>MAN/WAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>OmniSwitch 9000</td>
<td></td>
<td>OmniVista MM</td>
<td>Service Router IP/MPLS</td>
</tr>
<tr>
<td>OmniSwitch 6850</td>
<td></td>
<td>OmniSwitch 6855</td>
<td>OmniAccess 6000</td>
</tr>
<tr>
<td>OmniSwitch 6400</td>
<td></td>
<td>OmniSwitch 62x0</td>
<td>OmniAccess 5740</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OmniAccess 4000</td>
<td>OmniAccess 850W</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Appliances</th>
<th>Admission Control</th>
<th>Mobile</th>
<th>Firewall / Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>CyberGate Keeper</td>
<td>OmniAccess Safeguard</td>
<td>OmniAccess 3500 NLG</td>
<td>Brick Firewall</td>
</tr>
<tr>
<td>OmniAccess 5510</td>
<td></td>
<td></td>
<td>OmniAccess 8550 WSG</td>
</tr>
</tbody>
</table>
User-centric Security
A Comprehensive Product Portfolio

Quarantine Manager
FortiGate
InfoExpress
CyberGatekeeper
OmniAccess
SafeGuard
VPN Firewall Brick
OmniSwitch
Access Family

OmniAccess 3500 Nonstop
Laptop Guardian

VPN Firewall Brick
Multimedia Security Gateway

OmniAccess 8550
Web Services Gateway

2
The Mobile Blind-Spot
The Mobile Blind Spot

Question: How many laptops are lost or stolen every year in the US?

a. About 50,000
b. Between 200,000 and 300,000
c. More than 600,000

Answer: c, More than 600,000

The Mobile Blind Spot

Question: What does IT do in your organization when a laptop is lost or stolen? Select all that apply.

a. Write it off and issue a new one
b. Keep fingers crossed that the incident does not go public
c. Report to authorities
d. Check for a backup of the data
e. Other

Answer: No right or wrong answer
The Enterprise Security Challenge

More than 50% of new corporate computer purchases are laptops. There is more confidential data on laptops than ever before.

“More than 600,000 laptop thefts occur annually, totaling an estimated $720 million in hardware losses and $5.4 billion in theft of proprietary information.”

Source: Safeware Insurance, 2003

“Average Value of Business Info on Travelers’ Laptops Equals $525,000”

Source: CIO Magazine, October 2007

“...81% of respondents report that their organizations had one or more lost or missing laptop containing sensitive or confidential business information in the last 12 months...”

Source: Ponemon Institute, 2006

“The average time from vulnerability announcement to exploit is now measured in hours.”

Source: Microsoft Corporation

Laptop Hall of Shame
IT Managers Need to Eliminate the Mobile Blind Spot

Mobile laptops are a “blind spot” in Enterprise Security

When a laptop leaves the enterprise, IT loses control:

- Secured only by local clients (Anti-virus, etc.)
- Difficult to patch and backup
- A lost or stolen laptop is the “nightmare” scenario for IT
- No monitoring of the mobile device activity
- Difficulty to enforce policies
- Lack of asset inventory
- Complicated for the end users

Security Measures Must be Transparent to End Users

Difficult for end users to follow complicated security procedures while “on the move”

Security becomes a nuisance to be avoided

- Manually selecting the access interface (3G, WiFi, LAN, dial-up modem) based on network availability
- Running multiple interactive sessions to establish secure connectivity into the corporate network
- Abrupt degradations of computing capacity during bulk backups and patch downloads
- Need to regularly re-establish secure VPN connection
Alcatel-Lucent Nonstop Laptop Guardian
The Ignition Key to the Laptop

Market’s ONLY, always-on, secure, independent mobile platform that provides 24/7 visibility and control over laptops worldwide!!!

**Mobile**
- Always-on, even when the laptop is OFF or offline

**Visible**
- Always available to monitor laptop location and health

**Controlled**
- Ubiquitous control, easily accessed for remote kill, policy enforcement, delivering patching and updates
Alcatel-Lucent Nonstop Laptop Guardian

Components

- Always-accessible endpoints
- Remote management
- Visibility and control
- All through 3G communications

24x7 remote IT management

Simple, Efficient, Secure Access

Laptop card

3G modem Memory Battery Processor
API GPS Removable memory Operating system

Gateway

VPN Policies IT applications

3G Wi-Fi LAN

Trusted, tamper-proof, independent

Features at a Glance

<table>
<thead>
<tr>
<th>Laptop lost or stolen</th>
<th>Anti-tampering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique location and remote data “kill” capabilities:</td>
<td>Standalone computing technology:</td>
</tr>
<tr>
<td>• IT removes encryption keys and wipes data from the laptop</td>
<td>• “Watches over” applications on the laptop</td>
</tr>
<tr>
<td>• IT receives verification that data is protected</td>
<td>• IT is alerted and action is taken when changes that affect the Nonstop Laptop Guardian or the laptop’s security have taken place</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Laptop Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>A data card provides the “ignition key” for the laptop:</td>
<td>GPS capability:</td>
</tr>
<tr>
<td>• Used as a second or third means of authentication</td>
<td>• IT can access location services for the NLG card</td>
</tr>
<tr>
<td>• IT can revoke access to the laptop anytime, anywhere</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Protection</th>
<th>Third party integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded encryption keys:</td>
<td>An open architecture platform:</td>
</tr>
<tr>
<td>• Protect key data on the laptop</td>
<td>• Simple, open APIs allow third-party applications to become always-on, trusted and location aware</td>
</tr>
<tr>
<td>• Keys are backed up, erased, rotated or recreated based on policies and threat levels</td>
<td>• Enterprises can continue using their best-of-breed point solutions with all the benefits of the Nonstop Laptop Guardian</td>
</tr>
<tr>
<td>• Keys integrate with third-party HD encryption — for even greater security</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VPN usage</th>
<th>100% patch laptops</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic VPN connection:</td>
<td>All patches are installed on all laptops:</td>
</tr>
<tr>
<td>• With no user action, a VPN connection is established automatically — every time, no matter how the user accesses the network (3G, WiFi, LAN).</td>
<td>• Patches are stored on the laptop card and applied when the laptop boots</td>
</tr>
</tbody>
</table>
Alcatel-Lucent Nonstop Laptop Guardian

Lost or Stolen Laptop

More than 600,000 laptop thefts occur annually, totaling an estimated $720 million in hardware losses and $5.4 billion in theft of proprietary information.

Safeware Insurance, 2003

With the Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian:

- IT has the location of the laptop
- Data and encryption keys safely backed up at home office.
- IT revokes encryption key
- IT gets verification

Reduce Risk and Liability
Alcatel-Lucent Nonstop Laptop Guardian
Off-Hour Patches

The average time from vulnerability announcement to exploit is now measured in hours.
Microsoft Corporation

With the Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian:

- IT pushes a priority patch to all laptops via its patch management system
- Laptop card receives the patch and caches it
- Laptop is turned on and patch is immediately applied
- IT patch management system is updated

Protect Laptops From Zero Day Exploits

Alcatel-Lucent Nonstop Laptop Guardian
Automatic VPN - Take the User out of the Security Equation

“Today, my employees can decide if and when they’re in compliance or not and when they’re secure or not...we have no control”
Fortune 500 Customer

With the Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian:

- Automatically connect to VPN without any user intervention
- Secure all traffic - WiFi, LAN and 3G
- 100% compliance with Enterprise policies
- User always behind the corporate defenses - more secure

Access internet solely through the Enterprise policies
Alcatel-Lucent Nonstop Laptop Guardian
Case Study - Visiting Nurses Association of New Jersey

Challenge

- Multiple laptop PCs in the field
- Sensitive clinical/financial data
- Data vulnerable to loss/theft
- No possibility to ‘lockdown’ data if PC is stolen/missing
- Maintaining a reputable public image
- Retain patients and employees

Solution

- Ensures field laptop is always available to IT
- Immediate ‘lockdown’ of compromised PC data
- Helps deter identity theft
- Manage PC upgrades / data retrieval remotely anytime, anywhere even when laptop turned off
- Tracks staff for better safety / accountability
- Remote management keeps staff in field
- Market privacy protection to obtain new business
- Meets/exceeds current HIPAA requirements

“Losing a Laptop is the one thing that keeps me up at night.”

“Trans system solves our biggest security problem because we can now “reach out” to any lost laptop and secure its confidential data.”

Summary and Q&A
Alcatel-Lucent Nonstop Laptop Guardian
Ecosystem—ALU Application Partner Program (AAPP)

- Encryption
- Business Applications
- End-point Security
- Back-up and Restore
- 2 Factor Authentication
- Network Access Control (NAC)
- Configuration Management
- Patch Management
- NLG Partner Ecosystem

Awards and Recognition

- 2008 EDITOR’s BEST AWARD WINNER by Windows IT Pro Magazine
- Editor’s Choice 2008 by Information Security™ magazine and SearchSecurity.com™
- OmniAccess 3500 Nonstop Laptop Guardian Receives 2007 Product of the Year Award!!!

2008 Outstanding Awards
- WINNER - Best Wireless/Mobile Product

2008 Global Excellence
- Finalist in 3 categories -
  Access, Policy Management Solution, Wireless/Mobile Security Solution

Tomorrow’s Technology Today Awards, winner in 3 categories
- Mobile Laptop Data Security, Access, Endpoint Security

2007 3G CDMA Industry Achievement Award for Innovation in Wireless Enterprise Solutions Development
Alcatel-Lucent Nonstop Laptop Guardian

Summary

Question: How does NLG improve encryption?

a. Encryption keys are not known to the user
b. Encryption keys are not stored in the laptop
c. Encryption keys can be revoked anytime over the air
d. All of the above

Answer: d, All of the above
Thank you!