

Breakthrough Laptop Security Evolution

OmniAccess 3500 Nonstop Laptop Guardian

BECOME
A DYNAMIC
ENTERPRISE

Patricio Martelo
July, 2009

Agenda








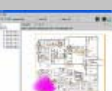



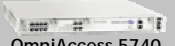





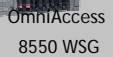
1. Securing Dynamic Enterprises
2. The Mobile Blind-Spot
3. Alcatel-Lucent's OmniAccess 3500 Nonstop Laptop Guardian
4. Uses Cases
5. Case Studies
6. Summary and Q&A

1

Securing Dynamic Enterprises

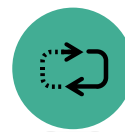
Enterprise Data Portfolio Snapshot



Management	<p>IP Address</p> <p>1000.5AC4.3221=192.168.1.10</p> <p>VitalQIP</p>	<p>IP Infrastructure</p>  <p>OmniVista 2500/2700</p>	<p>IP performance</p>  <p>VitalSuite</p>	
	Data networks	<p>LAN</p>  <p>OmniSwitch 9000</p>  <p>OmniSwitch 9000E</p>  <p>OmniSwitch 6850</p>  <p>OmniSwitch 6855</p>  <p>OmniSwitch 6400</p>  <p>OmniSwitch 62x0</p>	<p>WLAN</p>  <p>OmniVista MM</p>  <p>OmniAccess 6000</p>  <p>OmniAccess 4000</p>  <p>OmniAccess AP</p>	<p>MAN/WAN</p>  <p>Service Router IP/MPLS</p>  <p>OmniAccess 5740</p>  <p>OmniAccess 5510</p>
Security Appliances		<p>Admission Control</p>  <p>CyberGate Keeper</p>  <p>OmniAccess Safeguard</p>	<p>Mobile</p>  <p>OmniAccess 3500 NLG</p>	<p>Firewall /Application</p>  <p>Brick Firewall</p>  <p>OmniAccess 8550 WSG</p>

User-centric Security

A Comprehensive Product Portfolio



 **Quarantine Manager**

 **FortiGate**

 **InfoExpress CyberGatekeeper**

 **OmniAccess SafeGuard**

 **VPN Firewall Brick**

 **OmniSwitch Access Family**
ACCESS GUARDIAN Traffic Anomaly Detection

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



MoD laptop stolen from McDonalds

The Ministry of Defence says a laptop has been stolen from a member of the military as he was eating in McDonalds.

The computer was taken from the Army captain's chair, near MoD's Whitehall headquarters in April, according to the Sun newspaper.

The MoD said the data on the laptop was not sensitive, and was full of non-confidential information.

It comes after a laptop holding sensitive information was stolen from the armed forces in Birmingham, in January.

A Ministry of Defence spokesman said the stolen laptop contained information on 26,000 employees.

Stolen laptop contains patients' records

Jun 18 2008

A laptop containing confidential information about 11,000 patients has been stolen from a Wolverhampton GP's home.

Contrary to Department of Health guidelines which would have made it unreadable without a password, the laptop was among items stolen in a recent burglary from an unnamed doctor, who works at the Castleford surgery.

The information on the computer, which belonged to the doctor, included names, dates of birth, addresses, contact details and medical records.

The practice has written to all of its 11,000 patients to inform them of the theft.

M&S employee details at risk

Salary details contained on stolen laptop

g, 09 May 2007

Hazel Blears's stolen laptop was not encrypted

Laptop stolen from communities secretary Hazel Blears contained restricted information

Wednesday, 18th June 2008

A computer containing information on extremism, defence and the housing market was stolen from the Salford office of communities and local government secretary Hazel Blears last weekend. The restricted information was not encrypted, and government officials admitted breaching data security rules when sending Blears the files.

Peter Housden, chief civil servant from the department of Communities and Local Government, said that the computer was password protected and emphasised that no damage had been done because the documents were not classified.

However, he admitted, "It is clear that laptops have been sent to Hazel Blears in a way that is not fully consistent with the departmental guidance."

The incident is the latest in a series of high-profile data breaches involving government laptops. Other incidents include an MP of four losing his military laptop with data on 600,000 recruits last week, secret government documents on a laptop stolen from a government minister, and a free security analyst at Oxy Day observed "pranking" was improving productivity, "everybody thinks it is impossible to eliminate the risk of such as encryption, can eliminate the risks as various laptop suppliers and security service laptop security, from GPS tracking and automatic wireless modem that can remotely destroy the theft of Blears's laptop coincided with a "formation assurance" event that took place

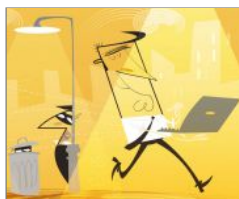


Laptop contained salary details for 26,000 staff

Information on 26,000 employees

56 laptops stolen from government departments in 2007

By Julian Prokaza on Tuesday, 22 January 2008



A total of 56 laptops were stolen from government departments in 2007, according to answers put to ministers in the House of Commons.

11 laptops were stolen from local government departments

in 2007, according to Department for Communities and Local Government and Parliamentary Under-Secretary Parmjit Dhandra

Nationwide fine for stolen laptop

The Nationwide Building Society has been fined £980,000 by the City watchdog over security breaches.



Nationwide security procedures were found to have failed

The fine follows the theft of a laptop from a Nationwide employee's home which contained confidential customer data.

The Financial Services Authority (FSA) found security was not up to scratch after the man had put details of nearly 11 million customers on his computer.

The FSA also found that the Nationwide did not start an investigation until three weeks after the theft occurred.

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



Lack of **Visibility** and **Control** over Mobile Laptops

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 bulky backups and patch downloads
- Need to regularly re-establish secure VPN connection



Remote Security Challenges Reduce End User Productivity

3

Alcatel Lucent OmniAccess 3500 Nonstop Laptop Guardian

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

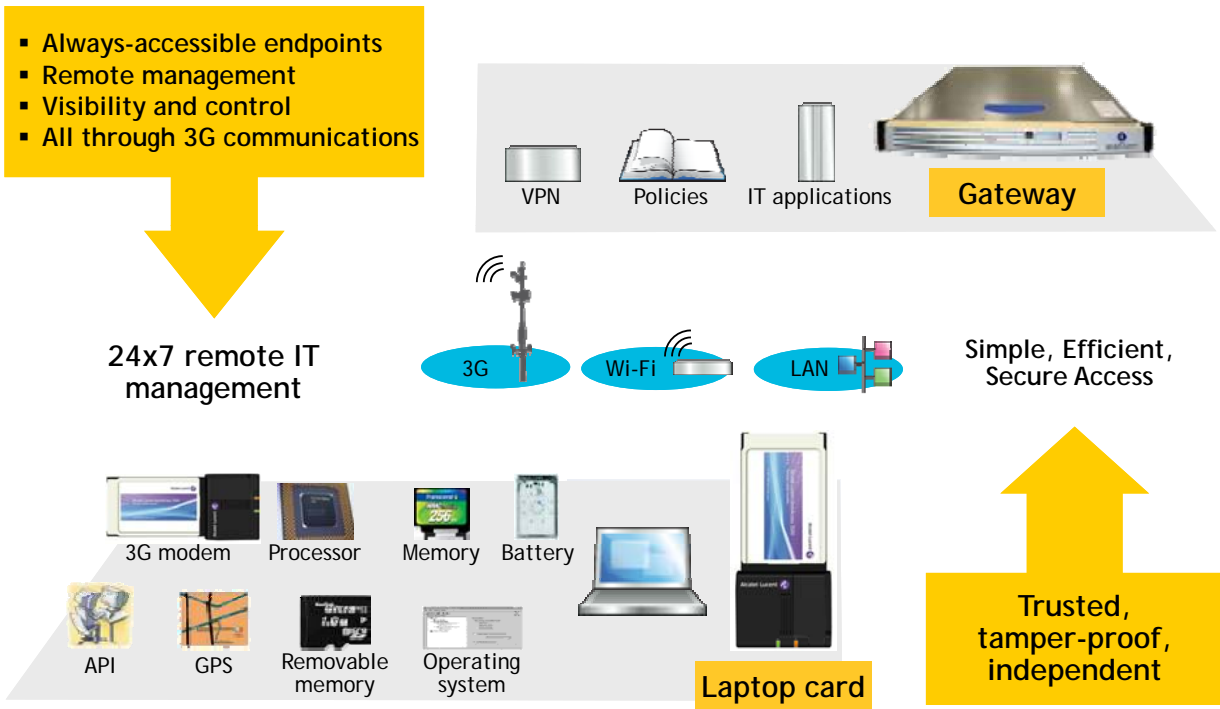
- Always available to monitor laptop location and health

Controlled

- Ubiquitous control, easily accessed for remote kill, policy enforcement, delivering patching and updates



Alcatel-Lucent Nonstop Laptop Guardian Components



Alcatel-Lucent Nonstop Laptop Guardian Features at a Glance

	<p>Laptop lost or stolen</p> <p>Unique location and remote data “kill” capabilities:</p> <ul style="list-style-type: none"> • IT removes encryption keys and wipes data from the laptop • IT receives verification that data is protected 		<p>Anti-tampering</p> <p>Standalone computing technology:</p> <ul style="list-style-type: none"> • “Watches over” applications on the laptop • IT is alerted and action is taken when changes that affect the Nonstop Laptop Guardian or the laptop’s security have taken place
	<p>Authentication</p> <p>A data card provides the “ignition key” for the laptop:</p> <ul style="list-style-type: none"> • Used as a second or third means of authentication • IT can revoke access to the laptop anytime, anywhere 		<p>Laptop Location</p> <p>GPS capability:</p> <ul style="list-style-type: none"> • IT can access location services for the NLG card
	<p>Data Protection</p> <p>Embedded encryption keys:</p> <ul style="list-style-type: none"> • Protect key data on the laptop • Keys are backed up, erased, rotated or recreated based on policies and threat levels • Keys integrate with third-party HD encryption – for even greater security 		<p>Third party integration</p> <p>An open architecture platform:</p> <ul style="list-style-type: none"> • Simple, open APIs allow third-party applications to become always-on, trusted and location aware • Enterprises can continue using their best-of-breed point solutions with all the benefits of the Nonstop Laptop Guardian
	<p>VPN usage</p> <p>Automatic VPN connection:</p> <ul style="list-style-type: none"> • With no user action, a VPN connection is established automatically – every time, no matter how the user accesses the network (3G, WiFi, LAN) 		<p>100% patch laptops</p> <p>All patches are installed on all laptops:</p> <ul style="list-style-type: none"> • Patches are stored on the laptop card and applied when the laptop boots

4

Nonstop Laptop Guardian Use Cases

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



Locate



Deny Access



Destroy Data

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

Live product demonstration

Please visit the Alcatel-Lucent Stand

5

Nonstop Laptop Guardian
Case Studies

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."

Michael Landsittel, IT Manager, VNANNJ



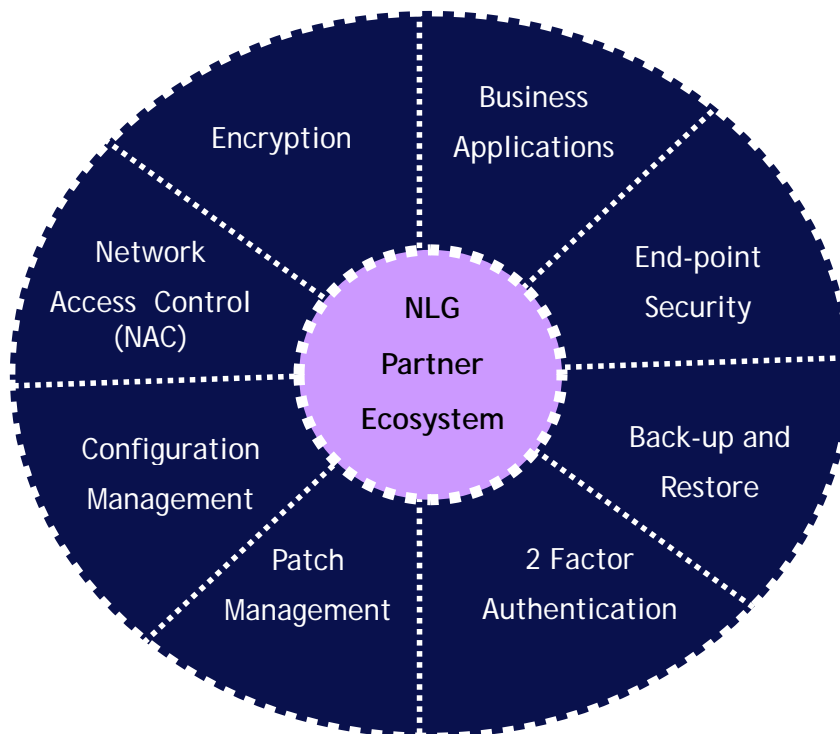
"This system solves our biggest security problem because we can now 'reach out' to any lost laptop and secure its confidential data."

Michael Landsittel, IT Manager, VNANNJ

6

Summary and Q&A

Alcatel-Lucent Nonstop Laptop Guardian Ecosystem—ALU Application Partner Program (AAPP)



Alcatel-Lucent Nonstop Laptop Guardian 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



Questions?



www.alcatel-lucent.com

www.cureinsecurity.com

Thank you!

