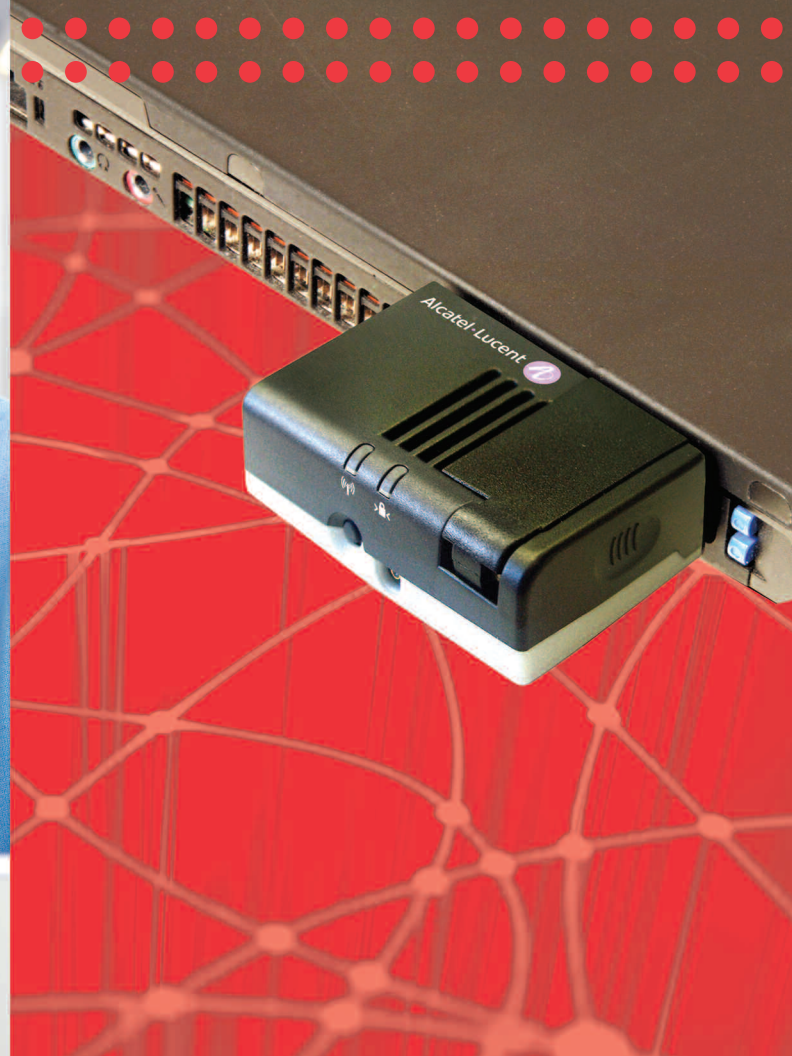
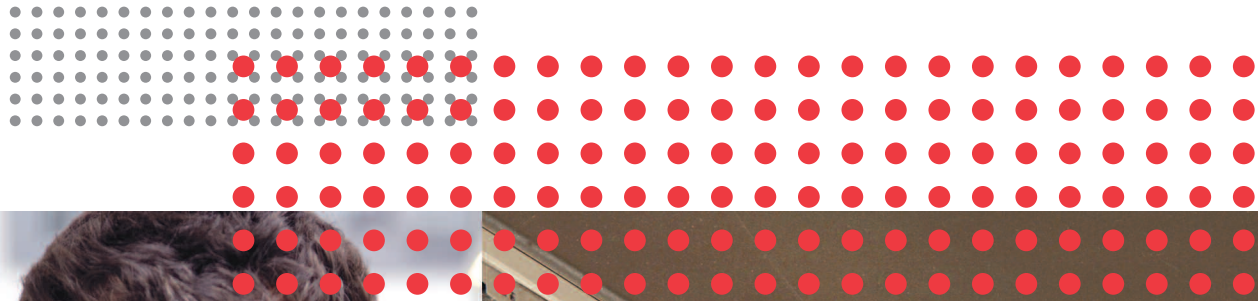



## The Alcatel-Lucent Laptop Security Solution

The Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian (NLG) integrates with McAfee's (SafeBoot) Full Disk Encryption to create the strongest end point security solution in the market.





Loss of confidential data stored on laptops, including customer data, employee records, intellectual property, and business documents has become a pervasive problem for companies worldwide. According to a 2007 survey conducted by the Ponemon Institute, 85 percent of respondents said their businesses had experienced a data security breach. Also reported by the Ponemon Institute, the average cost of a data breach was \$6.3 million.

## Secure the “mobile blind spot”

Managing the security of a laptop that is being used out of the office is a challenge. This “mobile blind spot” can be addressed by the OmniAccess 3500 NLG because it leverages 3G networks allowing IT managers to securely manage laptops remotely – anywhere and any time – even when the laptop is turned off.

A key element in the centrally managed OmniAccess 3500 NLG is a 3G card with a complete processor, memory, operating system and power source. This solution allows simple and seamless integration with third party applications and provides application partners with a unique way to offer enterprises, secure always-on business critical applications and features for mobile laptop computers. In addition, the OmniAccess 3500 NLG card emulates a smartcard interface, to allow integration with full disk encryption (FDE) solutions.



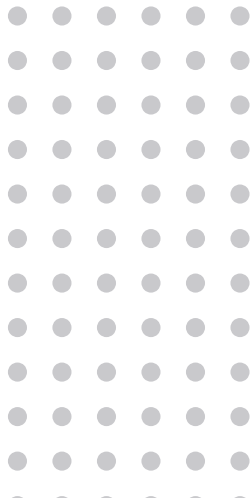
## McAfee Endpoint Encryption

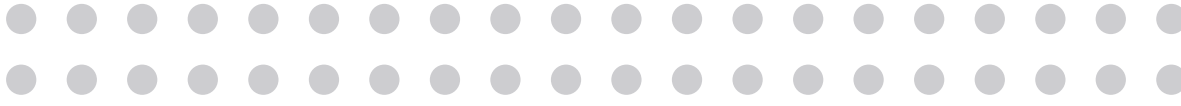


McAfee Endpoint Encryption software provides a scalable, enterprise-wide security solution. This software uses powerful encryption and strong access control to prevent unauthorized data access on desktops, laptops, and tablet PCs as well as smart phones and PDAs.

The McAfee solution uses strong access control with pre-boot authentication and government certified algorithms to encrypt data on endpoint devices, including laptops. Encryption and decryption are transparent to the user and performed “on-the-fly,” with virtually no performance degradation. McAfee Endpoint Encryption seamlessly integrates with existing enterprise systems and provides operational efficiency that ensures low total-cost-of-ownership.

McAfee Endpoint Encryption allows administrators to specify that the contents of certain folders, files created by particular applications, or files of a certain type be encrypted. Groups of users are granted access rights to particular files and folders, and securely share files across the network. No





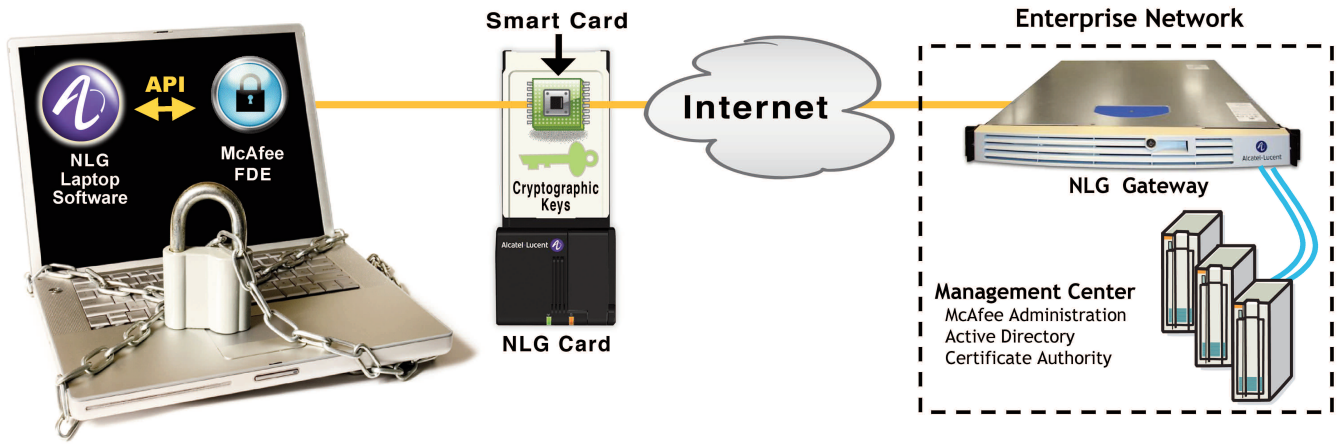
matter where files are saved and transferred, data remains encrypted using Persistent Encryption Technology™. If an unauthorized user tries to save a file that is viewable on a company laptop to an unapproved storage device, that user will walk away with an encrypted and unreadable file.

McAfee Endpoint Encryption prevents the loss of data wherever your data goes and achieves regulatory compliance with a full range of security and encryption solutions all managed from one central console. The McAfee solution provides central management capabilities including administration, central deployment, remote upgrades, auditing, mandatory security policy management, a scripting tool, hot revocation, recovery, synchronization, and more. Extensive auditing capabilities prove the device was encrypted at the time of loss or theft, demonstrating compliance. Mandatory security policies can be transparently enforced by administrators. McAfee Endpoint Encryption also supports single sign-on and secure offline user recovery.

### OmniAccess 3500 NLG integration with McAfee Endpoint Encryption

McAfee's Endpoint Encryption FDE solution supports interoperability with various types of smart cards and USB tokens. Typically these cards are used in certificate-based second factor user authentication, required for the decryption of the hard disk contents (files and folders) as well as for access to Windows. The OmniAccess 3500 NLG card has been integrated with McAfee's Endpoint Encryption as a smart card, providing second factor authentication at both pre-boot and at Windows levels. The OmniAccess 3500 NLG card stores the cryptographic keys needed for Endpoint Encryption FDE functionality to boot up. If the OmniAccess 3500 NLG card is not inserted in the laptop, or if the cryptographic keys are deleted, the FDE will not boot up and the data on the laptop will stay encrypted and secure.

The uniqueness of the solution is that the smart card on the OmniAccess 3500 NLG card is always reachable by the IT administrators due to the "always on" capability of the OmniAccess 3500 NLG card (built in 3G modem and battery). This makes the OmniAccess 3500 NLG card a remotely controlled "ignition key" for the laptop. If a laptop is reported stolen or lost, the administrator can issue a "remote kill" command to secure the data on the laptop. The "remote kill" command remotely deletes the cryptographic keys stored on the card, disables the smart card and forces a laptop reboot. The laptop will then be unable to boot up and the data on the laptop will stay encrypted and secure.



## Alcatel-Lucent Laptop Security Solution's Features and Benefits

The OmniAccess 3500 NLG integrated with McAfee Endpoint Encryption software provides:

### Features

---

- OA3500 NLG card appears to laptop as a smart card
- OA3500 NLG card acts as an additional authentication factor
- OA3500 NLG prevents access to a stolen laptop via administrator initiated "remote kill"
- Forced reboot back to the FDE PBA login
- OA3500 NLG smart card easily recreated when laptop is recovered
- Remote administration of smart cards

### Benefits

---

- Ensures 100% protection of end user data
- If the OA3500 NLG card is not present, McAfee Endpoint Encryption will not boot and data will stay encrypted
- Always on OA3500 NLG card allows admin to prevent hard drive access by disabling the smart card or deleting cryptographic keys on the OA3500 NLG smartcard
- Protects any content that was decrypted
- Minimizes administrative costs and downtime
- Makes new equipment roll out easier

Alcatel, Lucent, Alcatel-Lucent and Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.  
© 2008 Alcatel-Lucent. All rights reserved. P/N 032118 Rev. A 10/08