AlertBoot™

Protect customer and corporate data with AlertBoot mobile device management and managed disk encryption software

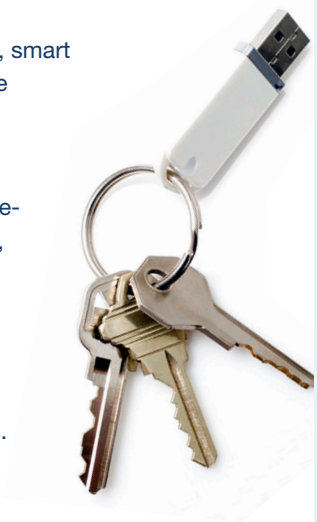
AlertBoot is a cloud-based suite of data security tools for individuals and organizations that need cost-effective, scalable device encryption and management for smart phones, tablets, and computers. AlertBoot prevents unauthorized access to mobile and stationary endpoints if a device falls into the wrong hands, be it a smart device, removable media, or fixed and external computer hard disks, and is a critical tool for supporting and enforcing acceptable use policies for mobile devices in the BYOD era.

Industry-leading data encryption technology and MDM integration
AlertBoot integrates encryption and device management into one easy-to-use unified platform. All physical disks on laptops and desktops use proven encryption algorithms revolutionized by the FIPS 140-2 Certified Mobile Armor Security Engine from Trend Micro. Smart phone and tablet security and encryption is managed using Trend Micro Mobile Security.

Secure user authentication and authorization
Centrally defined and enforced password rules and Power-On Authentication prevents password penetration attacks.

SecureAuth: an added layer of authorization
SecureAuth from MultiFactor Corp. uses encrypted X509 Client certs to prevent phishing, DNS, and man-in-the-middle attacks without the IT headaches that come with other certificate-based solutions.

Centralized security management and IT tools
AlertBoot client applications can be managed online. All users, smart devices, computers, recovery keys, and other functions can be administered remotely.



Company-wide password policy enforcement
Administrators can set customizable password strength requirements, and AlertBoot can ensure that everyone's endpoint PC, smart phone and tablet complies with the password strength policy.

Enterprise-grade auditing and reporting
Centrally managed audit logs and customizable reporting ensure compliance with internal policies and external regulations.

Advanced content encryption for files and USB keys
Advanced Content Encryption lets you protect SD cards and portable USB devices—so they stay encrypted regardless of where they go.

System Requirements

Operating systems

- Apple iOS for iPhones/iPads
- Android phones & tablets
- Symbian devices
- Windows Mobile devices
- Microsoft Windows XP (Service Pack 3)
- Microsoft Windows Vista™ (Service Pack 1)
- Microsoft Windows 7

Support for data recovery, imaging and forensics

- Lenovo® Rescue & Recovery– secure recovery of encrypted operating systems and data
- Windows PE 2.0 (recovery operating system)
- Ready for Encase (Guidance Software), AccessData, and Kroll Ontrack

www.alertboot.com
Inside the U.S.A. call 866.591.1311 (toll free)
Outside of the U.S.A. call +1.702.659.8890

Key Features

Powerful, transparent data security integration

- Unified, centralized computer disk encryption and mobile device security management platform
- Cloud-based, transparent remote management and installation of encryption and security policies for better productivity and ease of use
- Audit logging and customizable reports to better manage security events

Multi-Platform Mobile Device Management

- Secure and manage iOS, Android, Windows Mobile, and Symbian devices, including smart phones and tablets
- Manage remote disk wipes, password policies, Wi-Fi and VPN provisioning, and more
- Control apps and manage additional platform-specific security features

Centralized Disk Encryption Via the Cloud

- AES-256 full disk encryption extends to removable, external media
- Advanced protection: preboot authentication, password penetration prevention, and encrypted hibernation
- Single sign-on and no performance degradation
- Secure password recovery over phone or web, including web self-help

Powerful central administration

- Centrally enforced encryption rules
- Easy, centrally managed installation
- Transparent roll-out over a vast network—reduce the burden on your IT staff

Audit logging and reporting

- All client activities/status and security events are logged and stored locally and centrally
- Types of logs and storage locations are user-defined
- Administrators can filter, view, and print log reports

AlertBoot 24/7/365 live support

- Personal helpdesk for password recovery and assistance
- Secure and confidential; users are challenged with questions to verify identity
- AlertBoot Support will never have access to users' devices or personal data

About AlertBoot Data Security

Based in Las Vegas, NV, AlertBoot has a proven track record of delivering comprehensive, customizable security applications as fully managed services for companies of all sizes. AlertBoot has more than ten years experience in developing and implementing critical cloud-based solutions with a focus on integrating and streamlining the user experience and backend processes. AlertBoot's team is here to support the comprehensive, centrally managed AlertBoot mobile endpoint security solution.

Contact Us

Contact us with comments, questions, or to learn about partnership opportunities.

Inside the U.S.A. call
866.591.1311 (toll free)

Outside of the U.S.A. call
+1.702.659.8890

U.K. National Rate
+44.8708200015

U.K. Toll Free
0.800.098.8490

Send email to
info@alertboot.com

U.S. Headquarters:
3565 Las Vegas Blvd. S
Suite 162
Las Vegas, NV 89109 U.S.A.

AlertBoot™