Futurism
EndPoint Secure

EndPoint Secure for BANKING

EndPoint Secure in Action: Thousands in Fines Wiped Clean

A Bank Manager, while working remotely, relies on an iPhone to access customer records - in addition to calendar scheduling, voice and text messaging.
In a customer meeting away from workplace, the iPhone is stolen—on a bistro table one minute, gone the next.

Without hesitation, the Manager calls and directs the EndPoint Secure Support team, to wipe all information from the device, which is done remotely in a matter of minutes.

Banking - Specific Challenges

Bank employees now increasingly depend on their own mobile devices to access customer data while working remotely.

While mobile technology improves the quality and cost of customer care, it increases IT workloads and the potential for information security and compliance risks. EndPoint Secure is a Managed Service so Futurism does all the work. Futurism manages all of these risks while improving the productivity of your healthcare colleagues and keeping them happy by allowing them to use their own mobile devices.

Conduct Remote Audit

Although Bank management and auditors may not see eye to eye on everything, they can agree that teams must find new ways to effectively work together during any crisis.

Moving to a remote audit can present seemingly unsurmountable challenges, such as tracking PBC requests and status or providing and obtaining supporting documentation. But remote work doesn't have to hinder your productivity.

Banks that enable a technology-driven close and audit processes gain more streamlined collaboration, even with a distributed and virtual workforce

EndPoint Secure Banking Solution

EndPoint-Secure enables banks to secure Customer information on all mobile devices connecting to their network, comply with banking regulations, and reduce the workload and cost of managing mobile devices.

Using EndPoint Secure, Mobile Device Management (MDM), Mobile Application Management (MAM), and document and expense management can be easily and instantly integrated into broader enterprise programs for IT governance, data security and regulatory compliance.

Key Benefits

- Gain 360° visibility and control of all mobile devices, apps, documents and files
- Automate password, encryption and policy enforcement
- Ensure anytime, anywhere device and data security with immediate remote action on nonconforming devices
- No infrastructure changes required
- Rapid implementation
- Low implementation costs and no-fuss maintenance
- Expense management to control costs and overages

Key Features

- Cognitive insights and contextual analytics
- Supports all mobile devices from a single console
- Advisor Alerts to stop threats before they happen
- A real time policy recommendation engine
- An AI ChatBot and voice assistant for mobile users
- Mobile threat management
- Cloud identity management
- Security management
- Remote locate, lock and wipe (full and selective)
- Blacklisting, whitelisting and requiring apps
- Real-time reporting and analytic

Futurism
EndPoint Secure

EndPoint Secure for Banking

Control All Devices

EndPoint Secure gives banking organizations coordinated visibility and control over all devices and operating systems, from Apple iOS to Android, Windows Phone and BlackBerry. Integrated dashboards, analytics, and reporting provide actionable intelligence about their entire mobile environment through a single console. Bank administrators can quickly visualize the distribution of devices, apps and documents across platforms, approval status, device capabilities, ownership, compliance status and more to control the risks of bank workers using mobile devices to access banking apps and customer records.

Improve Mobile Information Security and Compliance

EndPoint Secure provides the ability to know and control information security safeguards on all mobile devices – and react rapidly to lost or stolen devices to ensure regulatory compliance with Federal Information Security Management Act (FISMA), Sarbanes-Oxley (SOX), Federal Rules of Civil Procedure (FRCP) and other statutes. EndPoint Secure Support team can:

- Push policies and Wi-Fi, email and VPN profiles OTA
- Quarantine new devices automatically until authorized to access your network
- Wipe sensitive data from lost or stolen devices remotely
- Blacklist applications and block device access
- Enforce passcode protection, encryption, and security updates

Control Mobile Applications

EndPoint Secure application management allows banks to easily manage and secure the applications that are critical to your users (e.g. KYC, etc.). An on-device application provides users with a catalog of authorized private and public apps. Users can view the apps made available to them, install apps, and be alerted to updates. EndPoint Secure Support team can manage the master app catalog and per-user authorization. Application lifecycle management provides real-time software inventory reports, app distribution and installation tracking, update publishing, provisioning profile management, and app security and compliance management.

Certifications and Compliances

EndPoint Secure uses IBM solution as its core, which is certified and compliant with–

- ISO 27001 certified
- FISMA authorized
- FedRAMP certified
- NIST certified
- FIPS 140-2 validated
- AICPA SOC-2 Type II certified

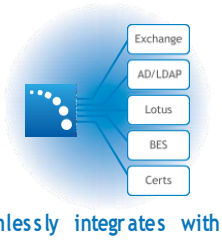
Reduce IT Workload and Costs

EndPoint Secure is a managed service from Futurism. (EndPoint Secure service is delivered through a SaaS model)There are no servers to install, no complex configurations or infrastructure changes, and no investment in expensive business software. Built on a secure, multi-tenant cloud architecture, it enables instant enterprise mobility management in just minutes with effortless scalability, whether from ten to tens of thousands users, and seamless integration into existing enterprise systems. Additionally, EndPoint Secure eliminates the strain and expense that rapidly changing mobile devices and applications used by bank employees can have them updated by automatically incorporating the continuous stream of platform updates.

Why EndPoint Secure - A Fully Managed Service

Proven approach to cloud-based mobility management

Powerful management & security to address the full mobility lifecycle



Seamlessly integrates with all of your existing infrastructure

Simple & fast with an exceptional customer experience

For More Information

To learn more about our technology and services visit EndPoint Secure.
30 Knightsbridge Road, Suite 525| Piscataway, New Jersey 08854
Phone +1 512 300 9744 | **Fax** +1 302.351.8845 |
Email endpointsecure_sales@futurismtechnologies.com