Safe Frontier

Solution Overview

MESOSPHERE

ACTIVE MANAGEMENT CLOUD

Beyond the Operating System

Safe Frontier introduces Active Management Cloud (AMC) – the first out-of-band Cloud infrastructure solution featuring powerful Intel® Active Management Technology (AMT). AMC provides first-class Intel® AMT enabling infrastructure that extends fully featured Intel® AMT into the Cloud and on to the Internet devices, making it mobility viable and cost efficient for large and small organizations.

Intel® AMT is a set of hardware-based capabilities in computing devices with Intel® vPro™ processors that enhance security and provide remote management "beyond the operating system". Intel® AMT is supported by brand-name PCs, including notebooks and servers of many leading manufacturers, and by a growing number of special computing devices, such as Point of Sale (POS) terminals, Automated Teller Machines (ATM), medical and military equipment. The economics are simple. According to the study[1], a reduction of up to 61 percent desk-side visits could be achieved with Intel® AMT. Organizations can realize significant savings and increase employee productivity by considerably reducing IT downtime and costly repair shop visits.

Information security is another important aspect where Intel® AMT and Safe Frontier's Active Management Cloud could make a notable difference. Networks need firewalls; clients need malware protection. But even the most stringent security systems are known to fail in the face of human error, or so called "human factor". The deeper the threat inserts itself, the harder it can be to prevent or remediate. Rootkits, for example, can burrow underneath operating system and could be nearly impossible to detect and remove. Intel® AMT moves security down to the hardware level and can monitor what's happening under the operating system. This technology well could be the only way to truly defend against rootkits. It enables IT support to remotely repair or re-image an infected computer, even when the operating system and security software do not work. These capabilities can help organizations to secure their IT and considerably reduce support costs.

Safe Frontier's Active Management Cloud brings Intel® AMT to every organization. Whether it is financial institution with thousands of computers, hospital, factory, government agency, large or small business - AMC makes the technology affordable and easy to use. With no upfront costs and infrastructure engineering, organizations can immediately benefit from Intel® AMT, realizing quicker return on their Intel® vPro™ hardware investment.

AMC can be used by businesses, information security vendors, IT management vendors, and equipment manufactures. It can be integrated with third party products and services. AMC provides first-class globally distributed cloud infrastructure optimized for mobility, easy over the Internet device provisioning, multi-tenant out-of-band channel, and other important features - all independent of corporate networks. AMC provides Application Programing Interfaces (APIs) and supports Private Cloud deployment. Using the AMC and Intel® AMT Software Developer Kit (SDK), vendors can fully leverage out-of-band security and remote management functionality now available in the Cloud.

Intel® AMT Overview

Intel® Active Management Technology (AMT) is a suite of hardware/firmware based remote device management and security functionality. It increases efficiency of remote management and provides beyond the operating system (OS) security controls.

Intel® AMT hardware architecture and network interfaces are shown on the Figure 1 and 2. Please refer to Intel for detailed and more accurate description. The following are the highlights of Intel® AMT version 8 management and security functionality:

- Out-of-band KVM management (OS state independent);
- Remote media, IDE redirect for booting device over network;
- Remote power on/off/reboot;
- Wireless out-of-band connection;
- Persistent asset information;
- Remote access to BIOS settings;
- Fast call for help;
- Secure communications via HTTP digest authentication, TLS encryption;

- Non-volatile data storage – third-party application can store a limited amount of data in the non-volatile memory;
- Agent presence - software application that runs on the local platform can report its state and send periodic heartbeats to the Intel® AMT in order to indicate its presence. Also, Intel® AMT can be programed to react when application is running or stops running unexpectedly;
- System defense (circuit breaker) - is used by remote and local applications (i.e. management consoles, agent presence, environment detection, etc.) to apply filters to the network traffic. Thus it can stop specific unwanted communications on the hardware level;
- Wireless configuration - embeds wireless profiles into Intel® AMT to enable connectivity with access controlled networks;
- Alerts and event log (audit) – generates event log and alerts, including security alerts that can point to various issues, such as unauthorized access or malware activity;

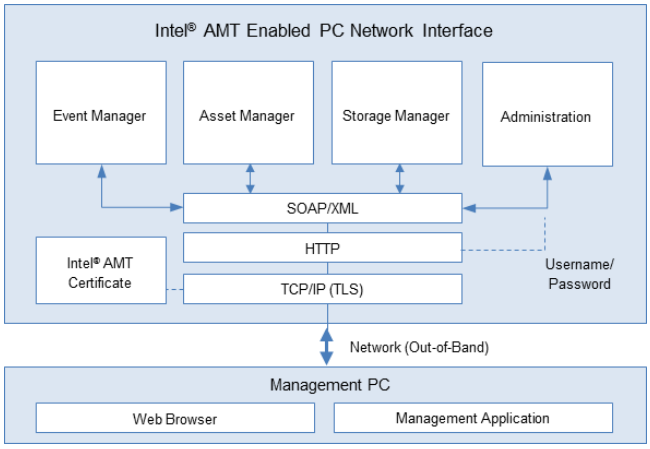

Figure 1

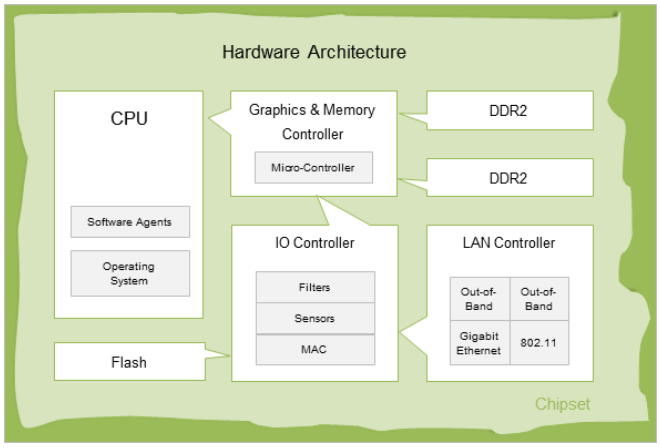

Figure 2

Traditional Intel® AMT infrastructure provides setup and configuration interfaces for management applications, as well as network, security, and storage administration. Intel® AMT supports standards-based encryption through Transport Layer Security (TLS) protocol and robust authentication.

However, the traditional deployment model is generally intended for devices located in the corporate network. It does not provide over the Internet device provisioning and has limited support for multiple out-of-band connections to a single device.

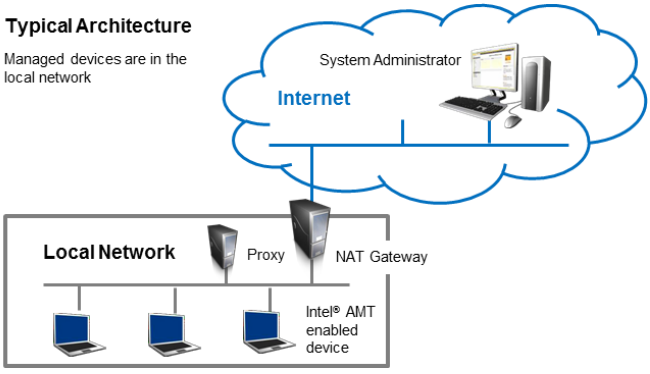

Figure 3

Intel® AMT version 8 provides two types of interfaces: network and local. Network interface consists of SOAP and embedded web user interface. The SOAP interface is controlled by management console applications created by third-party developers. The APIs associated with the SOAP interface are available as part of the Intel® AMT SDK. The local host interface is used by software agents to access and provide agent presence functionality. Please refer to Intel for more information.

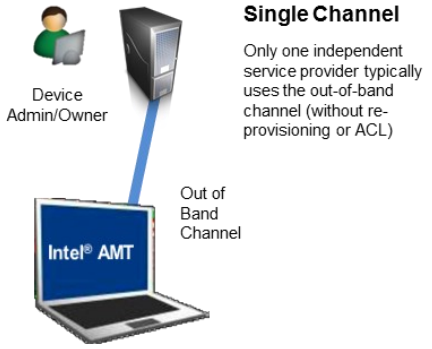

Figure 4

Active Management Cloud

Safe Frontier's Active Management Cloud takes Intel® AMT a step farther enabling its powerful functionality to be delivered in the Cloud — as a service over the Internet. AMC can efficiently service millions of fixed and mobile devices located around the world. The platform is optimized for mobility, utilizing globally distributed infrastructure and quality control automation.

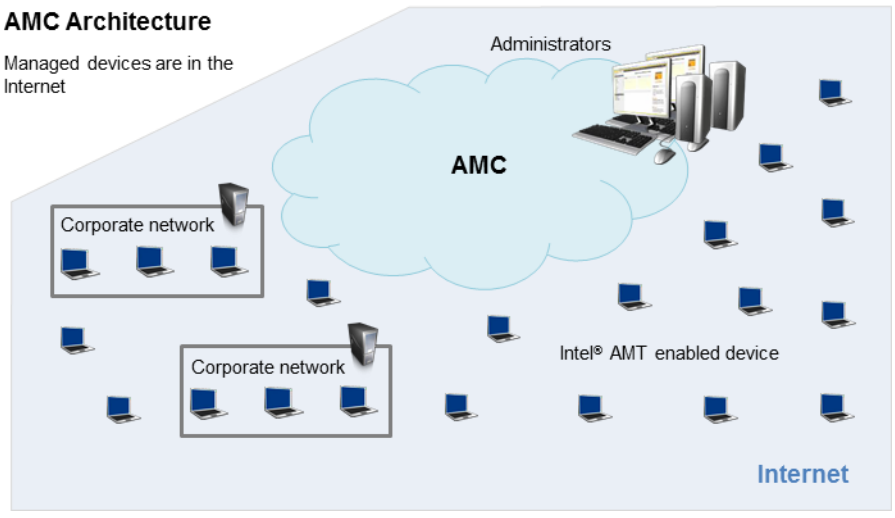

Figure 5

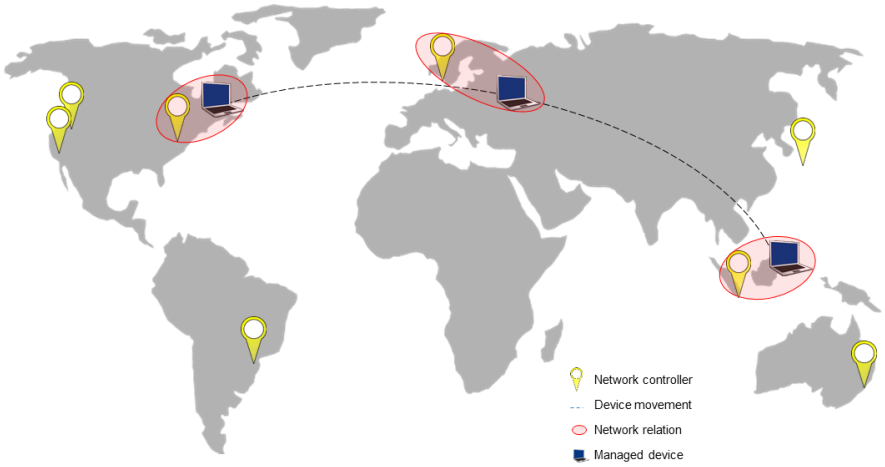

Figure 6

Active Management Cloud consists of:

Computing platform

- Scalable, high availability infrastructure;
- Globally distributed with automated geo-optimization;
- Ability to lock devices to a specific region(s);
- Compliant with SOC 2, Type 2; Level 1 PCI; and FedRAMP (in the process), FIPS 140-2 validated hardware;

Automation

- Secure, over the Internet "Zero-Touch"[2] device provisioning (port 16992/16993 must be open if behind NAT), simplified initialization, and host based over the Internet device provisioning using small software agent (standard Internet ports);
- Over the Internet re-provisioning to another network controller (gateway);
- Multi-channel (multiple service providers) out-of-band connection;
- Web-based account where administrator can manage device provisioning and control access to out-of-band channel;
- Support for Intel® AMT 7+ (limited support for older versions,

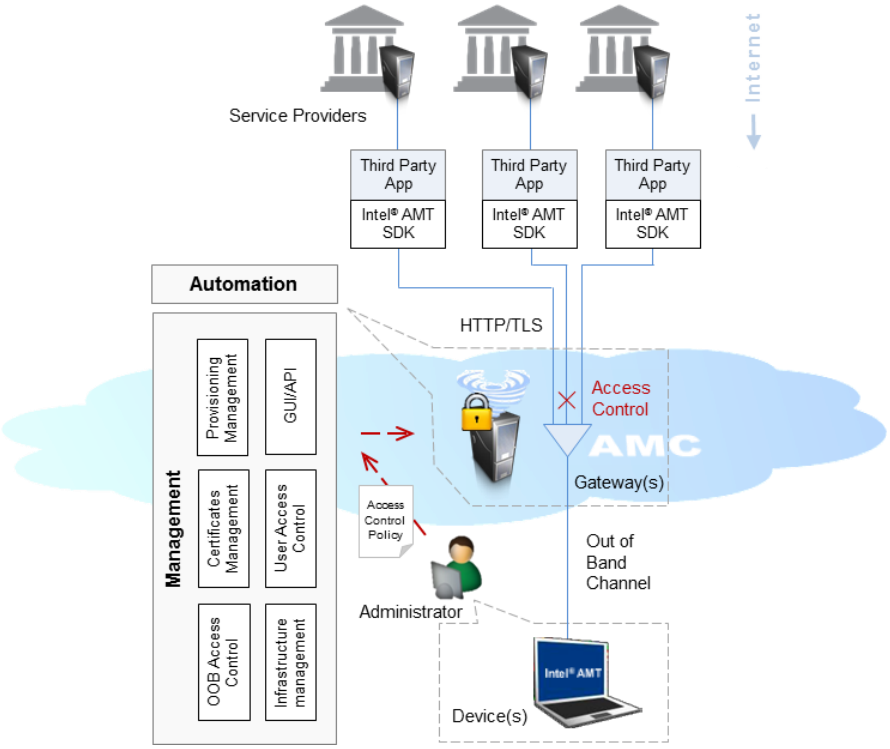

Figure 7

including over the Internet provisioning);

- APIs;

AMC provides the following administrative modules:

Device provisioning management – administrators can centrally manage Intel AMT® deployment. Devices can be provisioned over the Internet, outside of corporate networks. If the device is connected to the Internet, administrator can provision Intel® AMT on the device remotely by entering provisioning information in the web-account, without actually touching the device[2]. Administrator must know the Intel® AMT locally set credentials, and appropriate settings must be activated in the BIOS/MEBx. Administrators have another provisioning option. A small software utility can be deployed on the device, and user (or administrator, using remote access software) can enter Intel® AMT access credentials into the utility, provision the device automatically. This process can also be automated for bulk deployment. The second option works through the standard Internet ports, and therefore can be used even

with the devices behind NAT. Administrator can un-or -re-provisioned devices at any time.

Infrastructure management – this module allows administrators to quickly provision network controllers (gateways) that are used to facilitate the out-of-band communication. Administrator can scale the infrastructure depending on the number of devices under management and their geographical location. Geo-optimization helps managing devices that frequently change location. AMC can automatically find and connect a device to the nearest available gateway. This feature helps maintain connection quality of mobile devices when using resource intensive applications, such as KVM.

Out-of-Band (OOB) access control - enables multi-channel out-of-band connection of several independent service providers to a single device. For example, remote support vendor and information security vendor both require OOB to provide services. AMC implements access control on the device and infrastructure levels, allowing greater security and flexibility. Administrators can setup and control OOB access of each individual service provider. They can also selectively restrict service provider's access to the OOB, even before the Intel® AMT access profile is updated on the device. Therefore, service provider won't be able to access the device even with valid Intel® AMT credentials (Figure 8).

Certificate management – Public AMC allows administrators to install their own Intel® AMT certificates and provision TLS device certificates for secure out-of-band communication.

User access control – AMC allows multiple administrator accounts and supports Active Directory integration.

GUI/API – AMC provides web-based user interface and APIs that can be leveraged together with Intel® AMT SDK to build new management solutions or use AMC with existing solutions[3].

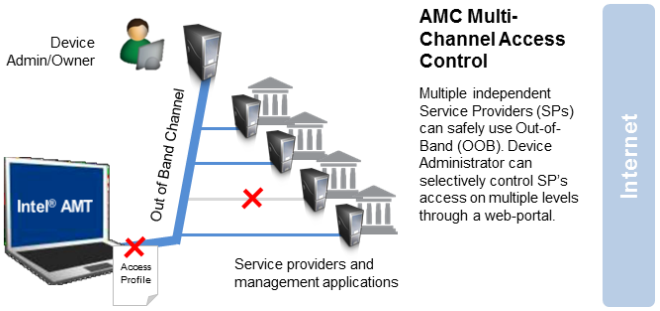

Figure 8

AMC can be Public or Private. Each infrastructure tenant in the Public AMC is isolated by virtualization. Public AMC offers security and flexibility without incurring high costs. Private AMC is deployed on client's premises and managed by the client, allowing greater flexibility and customization. Companies can build sophisticated security and remote management solutions with powerful Intel® AMT - instantly scalable, secure, and geo-independent. End users can now fully leverage Intel® AMT to reduce their IT support costs and enhance security, with no upfront costs and zero infrastructure to deploy and manage.

AMC Use Cases

The following use cases will demonstrate how large and small businesses, IT management vendors, information security companies, appliance

manufacturers and other market players can benefit from the Safe Frontier's Active Management Cloud.

IT Security Vendors

IT security vendors can use AMC to enhance their software and services with Intel® Active Management Technology. The following example shows how a security vendor can use Intel® AMT to offer new endpoint security services. In this example, vendor will remotely clean and repair customer's computer infected with rootkit – problem that would normally require a costly repair shop visit, and would cause several days of computer downtime.

- Client's notebook does not boot or the operating system freezes as a result of malware or malfunction. Client requests a security vendor for assistance. Technician receives client's request and can access the malfunctioning computer out-of-band bypassing the operating system.
- If the technician suspects that problem was caused by malware, technician can remotely scan the entire hard drive for malware presence. This will require booting client's device remotely using small operating system image that contains malware scanner. The entire hard drive, including boot sectors of the resident OS can be scanned for malware.
- Technician can block all or selected in-and-out-bound network traffic of the malfunctioning computer. Intel® AMT allows technicians to restrict selected network activity on the hardware level. It helps limit the possible malware propagation to other computers, as well as protect client's data.
- Technician can access logs of critical hardware/firmware events tracked by Intel® AMT to analyze the incident cause. Operating system events can be read directly from the hard drive.
- If the problem cannot be solved, operator can remotely re-image the computer using a backup copy of the client's OS, or attempt to repair the corrupted files of the resident OS.
- Out-of-band alerts can be configured to notify security vendor about critical hardware/firmware events. Such events could also be analyzed by the vendor for activity patterns. It will help to solve future issues and prevent new malware attacks.
- A security agent installed on the endpoint can communicate with the vendor's monitoring server using small non-volatile memory and out-of-band connectivity of the Intel® AMT. For example, it can transfer small data blocks related to malicious activity bypassing the operating system. This way security vendor can leverage persistent sensors, have better awareness, and can quicker respond to the new threats.
- Presence of security agent on the endpoint can also be monitored out-of-band. For example, if the agent is removed or disabled by malware, an alert can be issued out-of-band to the vendor's monitoring server. The agent can then be reinstalled in the operating system using controls provided by Safe Frontier.

The above tasks can be substantially automated. These capabilities can be incorporated in various security products. It is one example of how AMC and Intel® AMT can be used to provide strong endpoint protection, robust network security, and cost-effective

computer repair services.

Healthcare Enterprise & Medical Equipment Vendors

Modern hospitals are sophisticated computerized medical facilities with intelligent, connected medical devices. These devices almost exclusively use PC-based architecture and include: patient infotainment terminals, drug dispensing carts, diagnostic equipment, laboratory equipment, patient monitoring, endoscopy, etc. Most of these devices are not fixed to a single location but move around the hospital and between the facilities, especially in mobile hospital units.

Remote management of this equipment beyond the networks of a single location becomes crucially important. Healthcare providers deploying more technology into hospitals need to offset the complexity and management costs by providing more sophisticated remote management solutions. Such solutions must be capable of managing medical systems deployed in various locations and able to support mobile hospital staff. AMC would help healthcare enterprises to realize the benefits of Intel® AMT, drastically reducing IT support costs and improving compliance. For instance, Point-of-Care (POC) terminals are typically scattered in many hospital locations, mobile hospital units, or other clinical environments. Leveraging the AMC, healthcare organizations can easily utilize Intel® AMT to manage healthcare systems regardless of their location. The staff will securely provision, manage, monitor, and maintain mobile terminals outside or within hospital networks.

AMC and Intel® AMT enables IT personnel to take complete control of the Internet (or LAN) connected devices with keyboard-video-mouse (KVM) out-of-band access, troubleshoot and repair devices even when they are powered off or don't boot. Computer technicians can persistently monitor in-and-out-of-band security and health of the managed systems, such as presence of security agent, CPU temperature, battery capacity, network status, power state, important security events, etc. IT staff can reliably track assets, remotely re-image devices, boot devices from a different source, access device BIOS settings, and manage data security settings, regardless of the state of the operating system.

This solution will help healthcare enterprises to operate more efficiently, considerably cutting IT support costs by solving problems remotely, improving equipment logistics, and enhancing compliance.

Vending Companies & Vending Equipment Manufactures

Efficiency, availability, and security are paramount in any production environment, including IT systems that support distributed vending and point of sale (POS) equipment. As vending technology evolves, new machines are going well beyond dispensing snacks and drinks. These are intelligent, stand-alone systems with a multitude of features, including cashless payment mechanisms. The machines can be located in various places sometimes far apart from each other or the nearest servicing hub. Each on-site visit of a technician can be very expensive. Therefore proactive monitoring and remote maintenance are paramount for a successful vending business.

Safe Frontier's AMC provides infrastructure for out-of-band remote monitoring and servicing of the vending equipment that supports Intel® AMT. With no upfront costs and complexities, technicians can remotely solve problems that previously required on-site visits. Intel® AMT can also help to proactively alert the maintenance staff of the equipment malfunction. With AMC and Intel® Active Management Technology companies can significantly reduce operating costs and increase vending equipment uptime.

Computer Retailers & IT Service Centers

Today, many computer retailors operate service centers providing repair services. Buying a computer, customer can purchase additional maintenance warranty. A service center then helps fixing computer problems during the warranty term. If a problem cannot be solved using standard remote management tools, service centers would need to absorb the costs associated with sending technician on-site, or having computer mailed to the service center and back to the customer. Handling the computer in the service center is another expense, as well as additional risk associated with having customer's data. Customers also experience inconvenience and possibly business interruption while their computers are repaired.

Retailers that sell Intel® AMT enabled devices can take full advantage of the technology without a need for expensive infrastructure. AMC enables full spectrum of Intel® AMT remote management capabilities over the Internet. Service centers can securely access computers out-of-band for remote repairs. Furthermore, retailers and service centers can create and sell new proactive monitoring and maintenance services, differentiating and creating new revenue streams. With AMC, service centers can significantly reduce operating costs and increase customer satisfaction without incurring capital expanses or managing complex infrastructure.

Next Steps

Contact Safe Frontier to learn what Active Management Cloud can do for your business:

http://safefrontier.com

1. IT Best Practices Manufacturing and Intel® Core™ vPro™ Processors, September 2011.
2. Intel® Core™ vPro™ enabled devices that: 1) Support Intel® Active Management Technology (Intel® AMT) 7 or later. 2) Have the Intel® vPro™ technology activated in the Management Engine BIOS extension (MEBx). Intel AMT® may not be available or certain capabilities may be limited when connecting wirelessly, on battery power, sleeping, hibernating, or powered off.
3. Third party management solutions may not support Active Management Cloud.