AT&T Endpoint Security

November 2016

Security Drivers

Market Drivers

- Online business
- 24 x 7, Always on
- Globalization
- Virtual Enterprise
- Business Process / IT Alignment

Customers

Compliance Drivers

- Compliance with laws and regulations requiring an annual IT assessment

Financial Drivers

- CapEx / OpEx Reduction
- Off Shoring
- TCO / ROI Focus
- Focus on Growth

Suppliers

Risk Drivers

- Broader Threats
- Increased Vulnerability
- Greater Risk and Exposure
- Business Continuity / Security Issues

Organizational Drivers

- Productivity Focus
- Scarce Qualified Resources
- Rightsizing
- Consolidation
- Managed Services / Outsourcing

Employees

Technology Drivers

- Intelligent / Application Networking
- Exponential Storage Growth / ILM
- Mobility / PDAs / Wi-Fi / Wider-Fi
- Application Mgmt & Performance Visibility
- Utility / Grid Computing / Netsourcing
- Natural / Intelligent User Interfaces

Today’s threat landscape requires a multi-layered approach

We help secure connections end to end, helping protect data at rest & in motion

Strategy & Governance
Consulting

Endpoint
Mobile, IoT, Office/Fixed

Connectivity
Securing the network

Data/Application
Securing workloads/ applications

Threat Management
Detection & response

Endpoint Vulnerabilities & Challenges

- Endpoint is often the weakest link in a company's network security defense
- Employees using company assets for unapproved purposes
- Company data on external devices
- Not keeping up-to-date with emerging threats signatures
- Perimeter firewalls that cannotinspect trusted VPN traffic
- Intrusion detection systems that doesn't block attacks

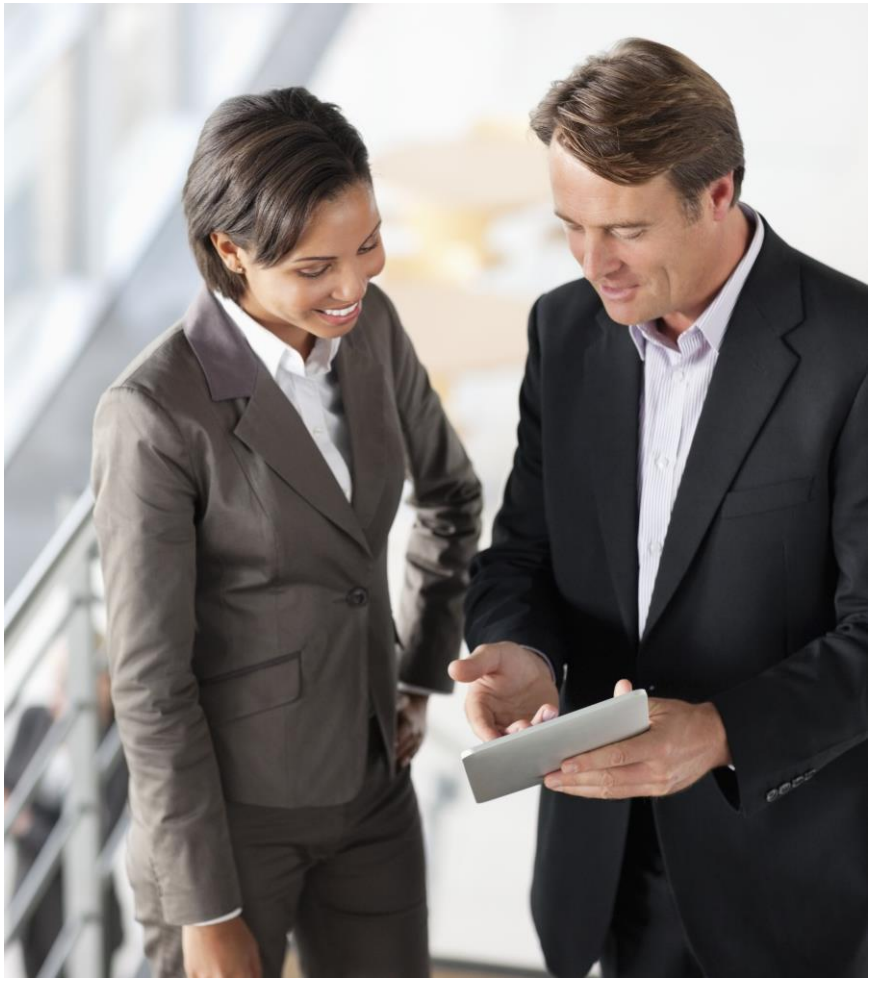
Why AT&T Endpoint Security?

- It is important to protect endpoint devices and the data within them. Compromised endpoint devices can become an entry point for threats in the company network and resources.
- AT&T EPS complements network security as it includes:
  - deploying effective desktop level firewall and Web access policies
  - enforcing company security procedures related to antivirus
  - Protect external devices when inside he company network and remotely.
- AT&T EPS also adds another layer of defense is a great complement to AT&T Firewalls and Managed Intrusion Detection and Prevention Services (MIDS).
- Our 24x7 staff of Security Professionals, and analysis tools

What is AT&T Endpoint Security?

AT&T Endpoint Security – is a part of the AT&T Managed Security Services

- helps protect end user computing devices from hazards posed by doing business on the Internet whether working in the office or remotely.
- designed to help enforce customer-defined policies for firewall, web access control, enforcing company security procedures related to antivirus and the option of allowing/blocking use of external devices.
- provides the flexibility to define unique and detailed policies specific to the customer's security requirements.
- The endpoint software agent installed on the endpoint device. The management server pushes the predefined security policy information and updates to the endpoints.



AT&T Endpoint Security (AEPS) Features

Anti-malware – signature based anti-virus malware scanning and removal.
Web Protection – Website reputation/risk rating, and check files when downloading or executing. Website category blocking (e.g., gambling, Adult sites).
Desktop firewall – Application-aware firewall, controls inbound and outbound traffic.
Device controls – Enables/disables use of external devices (e.g., USB, CD/DVD, etc.)
Encryption – Data at rest and/or file-level encryption for data stored on endpoints.
Behavioral Analysis – monitors different application behaviors and characteristics in order to determine if the application is likely to be malicious.
Application Control – controls file and registry access and how processes are allowed to run. Allows whitelisted applications to run, or blocking blacklisted applications).
Host IPS – monitors all inbound and outbound network traffic, looking for attack attempts or malicious communications to external systems.
Location-Based Policies – automatically switches between multiple policy sets based on dynamic attributes, including a wide range of network configuration attributes, Trusted Platform Module (TPM) usage or a registry key setting.
Advanced Threat Detection (ATD) Intelligence and Analysis – designed to detect stealthy, zero-day malware with a layered approach. It combines antivirus signatures, reputation, and near real-time emulation defenses with in-depth static code and dynamic analysis (sandboxing) to analyze actual behavior. ATD also has intelligence to convert threat information found into action for protection on the endpoints.
Rogue Device Detection – provides near real-time discovery of unknown devices connected to the network.
Anti-Virus for Email Servers – Scans email for signature based virus.
Threat Reputation Monitoring – a cloud-based intelligence application which determines if a new application is likely to be legitimate or malicious.
Host Integrity - checks systems configurations compliance with existing IT policies (e.g., latest antivirus signatures, any configuration item on the system, such as patch levels, password strength settings or the existence of a required application).

AT&T Endpoint Security (AEPS) Offers

Available Offers	Small Busines	Enterprise Customers		
Features	**AEPS - SaaS**	**AEPS - Option 1**	**AEPS - Option 2**	**AEPS - SaaS2**
Anti-Malware	X	X	X	Cloud based, File Attributes
Web Protection	X	X	X	X
Desktop Firewall	X	X	X	
Device Controls	X	X	X	
Encryption	Optional	X		
Behavioral Analysis		X	X	X
Application Control		X	X	X
Host IPS		X	X	
Location-Based Policies		X	X	
Advanced Threat Detection Intelligence and Analysis		X		X
Rogue Device Detection		X		
Anti-Virus for Email Servers		X		X
Host Integrity			X	
Threat Reputation Monitoring		X	X	X
Mobile Device				Android
VPN				X

AT&T EPS Reporting

AT&T Endpoint security reports are available at AT&T BusinessDirect. Security Reports available can be accessible by the Customer Central Point of Contact (Customer CPOC) include:

- Endpoint Monitor
- Endpoint Activity
- Infection History
- Client Events Report

Why AT&T?

We help protect what is important to our customers

Virtually Seamless security experience

- End-to-end solutions
- Virtual security delivered by AT&T Software Defined Networking
- Unparalleled visibility and predictive analytics
- Proactive response

Strategic ecosystem

- Managed solutions with industry leading technologies
- Comprehensive threat intelligence
- Global cyber community

Cyber expertise

- 8 global Security Operations Centers
- 24x7 global monitoring & support
- Cybersecurity thought leaders with decades protecting AT&T assets
- Consultants to help customers best prepare for an evolving threat landscape

Innovation

- 5 AT&T Foundry® locations worldwide
- Mobile, Cloud and IoT security
- 179 security & privacy patents
- 200+ startups engaged with AT&T Foundry®

MOBILIZING
YOUR
WORLD℠