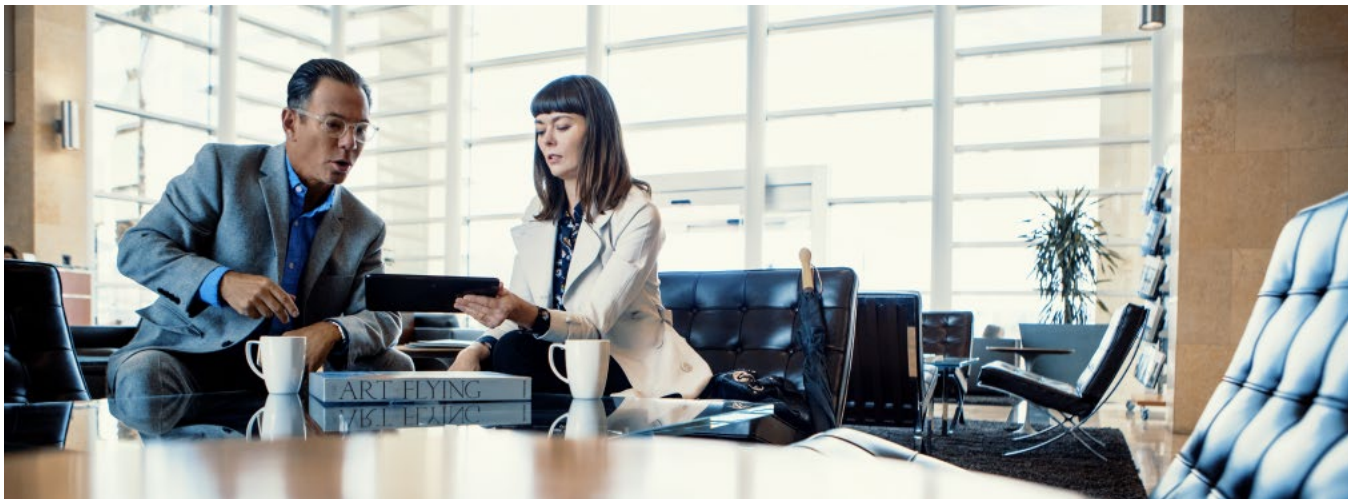
AT&T Business

Harness predictive intelligence and crowd wisdom to build a living picture of mobile threats 24/7



Today's enterprise IT managers are looking for ways to empower their workforces utilizing mobile devices for far more than email and texting. Employees require file sharing, access to corporate data, application downloads anytime, anywhere.

All of these activities can leave enterprise networks vulnerable to attack from network-based threats, malware, OS vulnerabilities and other targeted threats originating from both internal and external sources.

Solution overview

Symantec Endpoint Protection Mobile is a predictive mobile threat defense (MTD) solution that reduces the burden on IT to manage cyber risk in today's increasingly complex mobile threat landscape. Symantec Endpoint Protection Mobile enables proactive mobile security by actively predicting, detecting and preventing cyber-attacks, all without disturbing user privacy or disrupting users' mobile productivity. Symantec Endpoint Protection Mobile helps close mobile security gaps and protect

Benefits

- Near real-time visibility of active mobile threats, targeted attacks and vulnerabilities that may be compromising your covered devices, whether workforce managed or BYOD.
- Centralized risk, security and compliance management.
- Non-invasive end user experience with minimal storage and battery usage.
- Simple EMM integration to automatically enforce corporate security policy for covered mobile devices under attack.

against network based threats, malware, vulnerability exploits and other targeted attacks originating from both internal and external sources. Symantec Endpoint Protection Mobile's predictive technologies leverage mobile threat intelligence gathered by Symantec Endpoint Protection Mobile via massive crowd intelligence and sophisticated machine learning. Symantec Endpoint Protection Mobile identifies threats to the mobile device that some current approaches are not equipped to identify.

Malware Defense
Symantec Endpoint Protection Mobile uses a multi-layer approach to detect malware based on parameters such as signatures, user behavior, static/dynamic analysis, source origin, structure, permissions and known malicious application blacklists.

Network Defense
Network-based mobile attacks are one of the biggest threats to any organization today. Mobile devices connect to networks ten times more often than other endpoints. Symantec Endpoint Protection Mobile's patented "active honeypot" approach helps to proactively secure mobile devices against network based attacks.

OS Level Defense
Attackers exploit specific security holes in mobile applications, software libraries and mobile operating systems to replace normal software functionality with malicious functionality. Symantec Endpoint Protection Mobile leverages its crowd intelligence and dedicated research teams to stay ahead of attackers, partner with mobile OS vendors to patch security holes and notify end users of required OS upgrades or patches.

Physical Defense
Symantec Endpoint Protection Mobile integrates with leading Enterprise Mobility Management (EMM) solutions such as MobileIron, IBM Maas 360 and AirWatch from AT&T. EMM integration takes enterprise protection to the next level, providing automated ability to establish remote communication, take control, or lock down any mobile device that is under attack.

Pricing

Symantec Endpoint Protection Mobile, hosted, ASD 24x7 Support, MRC (per device) – $6.00/month

Symantec Endpoint Protection Mobile Remote Configuration and Training – $500.00 one-time charge

Required services

Remote Configuration and Training

AT&T will provide implementation services associated with the purchase of Symantec Endpoint Protection Mobile software licenses and hosting. The deployment will be conducted in a Symantec Endpoint Protection Mobile hosted environment.

Included services

Application Service Desk Technical Support

ASD 24x7 Support

The ASD 24x7 Technical Support Plan serves Customers that perform the day-to-day administration of their Symantec Endpoint Protection Mobile platform and AT&T for triage, technical support, and FAQs. It includes:

- Help desk to help desk (Tier 2) technical support 24x7x365.
- Support to triage and resolve or escalate service issues or support requests.
- Single point of contact for Tier 2 and above support.
- Basic "How to" and FAQ support for Symantec Endpoint Protection Mobile platform use and configuration.

- Customer notifications of service interruptions, service degradation or major product upgrades.

Note: U.S. based Application Service Desk support is available Monday through Friday 7:30 a.m. to 5:30 p.m. Eastern Time zone, excluding U.S. holidays. There may be circumstances during these hours where Application Service Desk support will be provided by personnel located outside the U.S.

Remote Administration Service Plan (for existing AT&T EMM customers)

If Customer purchases Remote Administration Basic or Advanced for AirWatch or MobileIron EMM solutions from AT&T, remote administration of the Customer's Symantec Endpoint Protection Mobile platform is included.

Optional services

Professional Services to Enhance your Symantec Endpoint Protection Mobile MTD Solution

- **Mobile Strategy, Security, and Roadmap Planning** – Discovery, Analysis, and Actions to align mobility initiatives with corporate goals and drive outcome-based results.
- **Advanced Mobility Lifecycle Services** – Globally-available deployment and protection services to keep users running with optimally configured and support mobile assets.

To learn more, ask your AT&T account representative to introduce AT&T's Mobility Solutions Services team.

Important Information

General: Semantec Mobile Threat Defense as described in this product brief (the "Solution") is available only to eligible customers with a qualified AT&T agreement ("Qualified Agreement"). The Solution is subject to (a) the terms and conditions found at https://www.skycure.com/terms-service/ for the administrative console and https://www.skycure.com/ios-terms-of-service/ or https://www.skycure.com/android-terms-service/ (for iOS and Android end user devices, respectively) ("Additional Product Terms"); (b) the Qualified Agreement; and (c) applicable Sales Information. For government customers, any Additional Product Terms not allowable under applicable law will not apply, and the Qualified Agreement will control in the event of any material conflict between the Qualified Agreement and the Additional Product Terms. Except for government customers, Customer must accept the Additional Product Terms on behalf of its end users. Any service discounts, equipment discounts, and/or other discounts set forth in the Qualified Agreement do not apply to the Solution. The Solution may not be available for purchase in all sales channels or in all areas. Additional hardware, software, service and/or network connection may be required to access the Solution. Availability, security, speed, timeliness, accuracy and reliability of service are not guaranteed by AT&T.

Requirements; Technical Information: The Solution is available for use with multiple network service providers and its functionality is limited to certain mobile devices and operating systems. A list of the compatible devices and operating systems is available by contacting an AT&T Account Executive. With respect to users subscribed to AT&T wireless service, activation of an eligible AT&T data plan with short message service ("SMS") capabilities is required. With respect to use of the Solution with devices subscribed to non-AT&T wireless providers, customer is responsible for ensuring that its applicable end users and the Solution complies with all applicable terms of service of such other wireless carrier(s). All associated voice, messaging and data usage will be subject to the applicable rates and terms of such other wireless carrier(s). Refer to applicable wireless carrier(s) for such rates, terms and conditions. The Solution's administrative interface is accessed via a Web portal and requires a browser with Internet connection. AT&T will not provide technical support to end users. AT&T reserves the right to (i) modify or discontinue the Solution in whole or in part and/or (ii) terminate the Solution at any time without cause. All fees paid for the Solution are non-refundable.

Reservations: AT&T reserves the right to perform work at a remote location or use, in AT&T's sole discretion, employees, contractors or suppliers located outside the United States to perform work in connection with or in support of the Solution. Any warranties related to the Solution that can be passed through under law will be passed through to Customer by AT&T. For government customers, the following applies to the extent not in conflict with the Qualified Agreement: (i) ALL SOFTWARE IS PROVIDED BY AT&T TO CUSTOMER ON AN "AS IS" BASIS; (ii) AT&T disclaims all remedies for claims of infringement by a third party based upon or arising out of customer's or end users' us of the Solution, and (iii) Customer's sole and exclusive remedy for any damages, losses, costs and expenses arising out of or relating to use of the Solution will be termination of service. For all other customers: (i) Symantec Corporation, not AT&T, is responsible for any such warranty terms and commitments; (ii) ALL SOFTWARE IS PROVIDED BY AT&T TO CUSTOMER ON AN "AS IS" BASIS; (iii) AT&T disclaims all remedies for claims of infringement by a third party based upon or arising out of customer's or end users' us of the Solution; and (iv) Customer's sole and exclusive remedy for any damages, losses, costs and expenses arising out of or relating to use of the Solution will be termination of service.

Use of Solution Outside the U.S.: For government customers, see your account representative for additional information regarding use of the Solution outside the US. For other customers, see the Country Specific Provisions in the Solution Service Guide located at http://serviceguidenew.att.com/sg_customPreviewPDFPage?testid=068C0000001fyNEIAY.

Data Privacy: Customer Personal Data may be transferred to or accessible by (i) AT&T personnel around the world; (ii) third parties who act on AT&T's or AT&T's supplier's behalf as subcontractors; and (iii) third parties (such as courts, law enforcement or regulatory authorities) where required by law. Customer will only provide or make Customer Personal Data accessible when Customer has the legal authority to do so and for which it has obtained the necessary consents from its end users, and will camouflage or securely encrypt customer Personal Data in a manner compatible with the Solution. As used herein, the term Customer Personal Data includes, without limitation, name, phone number, email address, wireless location information or any other information that identifies or could reasonably be used to identify customer or its end users. Customer is responsible for providing end users with clear notice of AT&T's and Customer's collection and use of Customer Personal Data obtained via the Solution, including, without limitation, end user device location information, and for obtaining end user consent to that collection and use. Customer may satisfy its notification requirements as to AT&T by advising end users in writing that AT&T and its suppliers may collect and use Customer Personal Data by providing for end user review the relevant links to the product brief or other sales information that describes the Solution and to AT&T's Privacy Policy at http://www.att.com/gen/privacy-policy?pid=2506.

For more information contact an AT&T Representative or visit www.att.com/security.

Share this with your peers

To learn more about Symantec Endpoint Protection Mobile, visit www.business.att.com/products/symantec.html or have us contact you.