Skycure

Mobile Threat Defense

Market Challenge

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

Skycure 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. Skycure Mobile Threat Defense enables proactive mobile security by actively predicting, detecting and preventing cyber-attacks, all without disturbing user privacy or disrupting users' mobile productivity. Skycure helps close mobile security gaps and protect against networkbased threats, malware, vulnerability exploits and other targeted attacks originating from both internal and external sources. Skycure's predictive technologies leverage mobile threat intelligence gathered by Skycure via massive crowd intelligence and sophisticated machine learning. Skycure identifies threats to the mobile device that some current approaches are not equipped to identify.

Malware Defense

Skycure 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. Skycure's patented "active honeypot" approach helps to proactively secure mobile devices against networkbased attacks.

Benefits

- Harnesses predictive intelligence and crowd wisdom and research to build a living picture of mobile threats 24/7 virtually anywhere in the world.
- 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.

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. Skycure 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

Skycure 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

Skycure Mobile Threat Defense, hosted, ASD 24x7 Support, MRC (per device) – $8.00/month

Skycure Mobile Threat Defense Remote Configuration and Training – $500.00 one-time charge

To learn more about Skycure Mobile Threat Defense, visit www.att.com/threat-management or have us contact you.

Share this with your peers

Required Services

Remote Configuration and Training
AT&T will provide implementation services associated with the purchase of Skycure Mobile Threat Defense software licenses and hosting. The deployment will be conducted in a Skycure 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 Skycure 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 Skycure 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 Skycure Mobile Threat Defense platform is included.

Optional Services

Professional Services to Enhance your Skycure 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.

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

Share this with your peers

Important Information

General: Skycure 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") and a Foundation Account Number ("FAN"). The Solution is subject to (a) the terms and conditions found at https://www.skycure.com/terms-service/ for the administrative console ("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. The Solution's 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. The Solution is available for use with multiple network service providers. Customer Responsibility Users ("CRUs"), Individual Responsibility Users ("IRUs"), and individuals who bring their own devices ("BYOD") are eligible to participate in the Solution. 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.

Except for government customers, (i) Customer must accept the Additional Product Terms as the party liable for each user of a Customer owned device, and agrees in such case that each such user will comply with the obligations under the Additional Product Terms; (ii) Customer is responsible for providing each such user with a copy of the Additional Product Terms; (iii) Customer and each such user are individually and jointly liable under those terms.

Requirements; Technical Information: The Solution is only available to Customers in the United States and for users who download the client software in the United States. All fees paid for the Solution are non-refundable. The Solution is available for use with multiple network service providers. For users subscribed to an AT&T wireless service, activation of an eligible AT&T data plan on a compatible device is required. For users of the Solution with devices subscribed to non-AT&T wireless providers, Customer is responsible for ensuring that Customer, its applicable end users and the Solution comply 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. The Solution may be used as a tool to configure and customize certain settings and features. Improper or incomplete configuration and/or downloads performed by Customer may result in service interruptions and/or device failures. Customer is responsible for obtaining the consent of end users that the Solution provides mobile threat defense capabilities and after notifying them that the Solution allows Customer to have full visibility and control of end users' device security in the manner described above.

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. 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.

AT&T shall pass through to Customer any warranties for the Skycure software available from the licensor. Skycure, not AT&T, is responsible for any such warranty terms and commitments. ALL SOFTWARE IS OTHERWISE PROVIDED TO CUSTOMER ON AN "AS IS" BASIS. Except for government Customers, 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.

Data: 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.

**To learn more about Skycure Mobile Threat Defense,
visit www.att.com/threat-management or have us contact you.**