Offer a new breed of security service for competitive differentiation and improved margins

Motive Security Guardian (formerly Kindsight Security)

- **Value-added security services generate additional revenues, enable competitive differentiation and build subscribers' trust**
- **Cloud-based, device-independent malware protection works across mobile and residential services**
- **An innovative, patented approach can catch more infections, more precisely, than traditional malware detection methods**

Most service providers see security as a cost center that's needed to protect their infrastructure. Of course, securing the network is a critical, central piece of any security strategy, and both capital investments and operating expenditures are necessary to ensure effective threat monitoring and quick response.

Today, there's also an opportunity to offer a value-added security service. As the number of threats targeting end users increases, subscribers now expect malware protection from their service providers, and are willing to pay a premium to ensure that their devices, personal information and privacy are safe.

Traditional tools like antivirus software can't meet today's requirements. Public studies also show that antivirus catches only half of infections and can take weeks to provide an update for new threats. As a result, even though 94 percent of U.S. subscribers have an antivirus on their computers, 60 percent

have been infected anyway, our research has found. And only 29 percent of respondents had even installed antivirus on their smartphones.

The study also showed that 65 percent of subscribers expect their service providers to protect their smartphones, but 80 percent don't know whether their service provider offers a protection service.

In summary, these findings indicate that there is no satisfying solution on the market today, even though there's consumer demand and willingness to pay for the service.

Value Proposition

Motive Security Guardian (formerly Kindsight Security) puts the end user at the center of the security strategy and enables service providers to offer a value-added service designed to protect the subscriber experience. It provides a complete end-to-end security layer, alerts subscribers when

a device has been infected and proposes the right remediation tools and step-by-step instructions for removing the malware. This offering can be bundled with a premium technical service, which allows subscribers to take these steps with the help of a customer care agent on the phone.

Many service providers offer an antivirus-based security service today. As outlined above, this approach has several shortcomings, and doesn't provide any significant differentiation. Motive Security Guardian complements antivirus software and adds another layer of protection, like an alarm system in a building. With the Motive Security Guardian, service providers can offer a more complete security service. And subscribers get better malware detection, which promotes trust that their service provider is protecting their experience, which in turn helps improve customer loyalty and decreases churn.

Offering a value-added Security service based on Motive Security Guardian has the following advantages for service provider and subscribers:

- **Extensive library:** With more than 30 million malware samples, the Motive Security Labs' library has one of the largest collections used to identify threats.
- **Highly efficient:** Motive Security Guardian needs fewer signatures and provides wider coverage than behavioral, traffic anomaly and DNS analysis-based systems combined.
- **Any network:** Motive Security Guardian simply analyzes upstream Internet traffic for malware detection. Consequently, it can detect threats on 100 percent of a service provider's fixed and mobile subscriber base, including customers connecting mobile devices over Wi-Fi to a fixed network.
- **Any device:** Because it runs in the service provider's cloud, Motive Security Guardian protects all connected subscriber devices, including computers, smartphones and tablets. Antivirus protects only those users who install the application.
- **Always-on:** The security service is always on and up to date, while most antivirus can be deactivated by the infection, and in many cases, they are not kept up to date.
- **Better experience:** Since malware detection happens in the network, it doesn't drain the device battery or impacts device performance.

Our primary market research indicates that subscribers are willing to pay an average of 4.40 United States dollars per month for a protection service from their service providers. This study also revealed that people with higher incomes seem even more willing to subscribe to malware protection services from their service providers. In addition, when it comes to shared family data plans, the willingness to pay is also higher for parents who pay for their children's data plans.

With this approach, security can be seen as a profitable business – not just a cost center. For example, a service provider in North America deployed this type of value-added service at 2.95 United States dollars per month and achieved great success. It proved to be their fastest selling value-added service ever – further results included:

- 8 percent opt-in rate within a year of launching the service
- 96 percent of subscribers retained the service month after month
- 97.5 percent reduction in care tickets, compared to a service based on antivirus

Clearly, service providers can provide a better security service with Motive Security Guardian than by reselling traditional antivirus.

Solution overview

Motive Security Guardian provides both a network-based infection detection platform and a security analytics solution. It allows service providers to pinpoint and analyze infections in their subscribers' home networks and mobile devices – then take action to protect both the network and subscribers.

Network-Based Intrusion Detection System

The Network-Based Intrusion Detection System (NIDS) detects malicious traffic originating from the subscriber home network or device using a specialized traffic-sensing and intrusion-detection software. Optimized for high bandwidth and flow density, it can be deployed at strategic locations within the network, typically at an aggregation or peering point. The sensors passively monitor traffic using a tap or mirrored port on a router without impacting network performance.

Alert Reporting Cluster

The Alert Reporting Cluster (ARC) is typically deployed in the service provider's data center. It is responsible for processing and storing events from the sensors, notifying the subscribers about security alerts, and assisting subscribers in removing the threats from their computers. It also hosts the Analytics Portal.

Virtualization

Motive Security Guardian can be deployed on standard, off-the-shelf hardware in a virtual environment such as CloudStack or OpenStack. These platforms provide unified management and a coordination layer for simplified maintenance and offer the ability to migrate to a more efficient operations model that supports the following features and functions:

- Application provisioning
- Automated network infrastructure upgrades and patches
- Self-healing and scaling cloud resources

This approach enables cost-effective deployment by minimizing CAPEX with standard, off-the-shelf hardware and reducing OPEX with simple management and deployment. It also provides elastic scaling of the system, when the situation demands additional or fewer resources.

Mobile App and Web Portal

Once an infection is detected, Motive Security Guardian alerts the subscriber using SMS, email, a web interstitial or a mobile application notification. The end user is then directed to a web portal that provides more information about the threat and step-by-step instructions for removing it, as well as appropriate third-party tools. Motive Security Guardian also includes a mobile application to remediate infections on mobile devices.

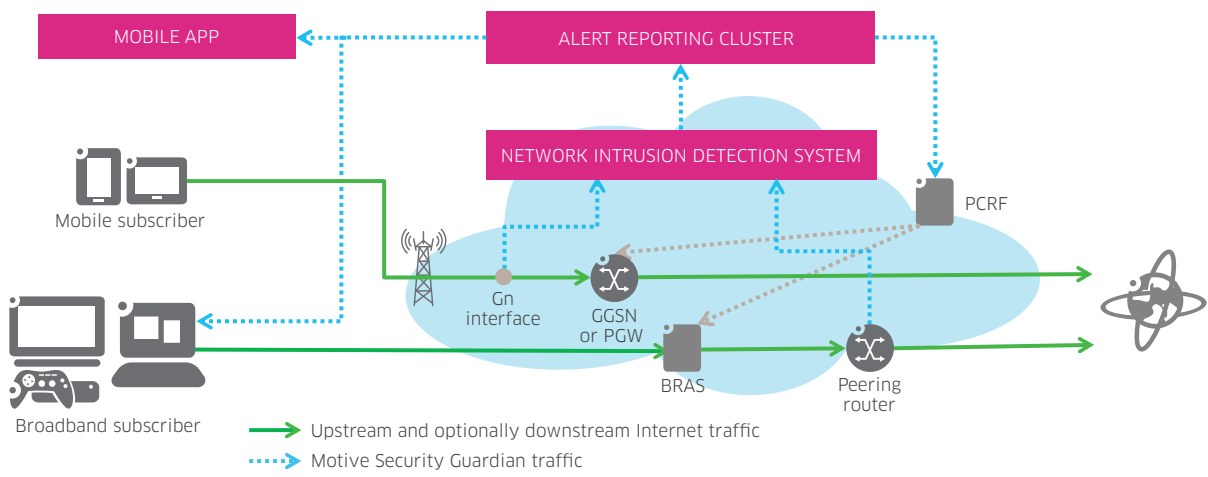**Related products and solutions**

As a part of the Motive Big Network Analytics solution, Motive Security Guardian can act as a standalone system for simplicity and agility, or it can be integrated with the Motive Wireless Network Guardian as a security module. It is also pre-integrated with with Motive ServiceView solutions for for customer care, and the Alcatel-Lucent 5780 Dynamic Services Controller for Policy Control.

The Motive advantage
Motive Security Labs

Motive Security Guardian is empowered by the Motive Security Labs (previously Kindsight Security Labs), a team with a unique combination of malware analysis and network forensics skills that are leveraged to create the detection rule

Motive Security Guardian architecture

Upstream and optionally downstream Internet traffic
Motive Security Guardian traffic

Solution features

FEATURE	BENEFIT
Fast and precise malware detection	Differentiate against traditional antivirus-based solutions by providing better protection that covers all devices and leverages service providers' key asset: the network.
Cloud-based, multi-device protection	Monitor all subscriber devices and detect malware without the need to install software on the device..
Automated alerts for infected subscribers over email, SMS, mobile app notification or web interstitial	Get flexible notification and remediation options for all types of services and devices.
Web portal and mobile app	Promote subscriber self-care, by giving customers tools to see if they are infected, identify the malware and to take independent actions to remove the problem.
Flexible options for value-added, mobile security services	Choose the most effective way to deploy and market the value-added security service, with opt-in or freemium go-to-market models. It can be bundled with premium technical support – or be used to upsell other protection services. The result is strong service differentiation and/or additional, recurring revenue.

set that powers the system. The team monitors global malware trends on a 24/7 basis, analyzing emerging malware and creating new detection rules as the malware eco-system evolves. Updated detection rule sets are automatically pushed out on a regular basis. The malware library currently contains more than 30 million active samples, with over 120,000 samples analyzed each day. Highly active in the industry, our experts share their knowledge widely and provide threat intelligence, particularly through their malware reports, which provide deep insights and analysis of the latest trends in both mobile and fixed malware.

Greater precision and more actionable insights

Motive Security Guardian provides an innovative, patented approach to malware detection. It does not just provide an alert that an infection has occurred, but specifically identifies which malware has caused the infection. This precision results in a very low number of false-positives. Replace with "It is also more efficient since it requires fewer signatures and provides wider coverage than behavioral, traffic anomaly and DNS analysis-based systems combined. Unlike many monitoring systems that simply send a flurry of cryptic events, Motive Security Guardian correlates those events into simple and actionable intelligence, which can be used to help subscribers to deal with the issue.

A solution designed for service providers

Motive Security Guardian has been designed specifically for service providers and leverages their key asset, the network. That means it passively analyzes massive volumes of data in real time and provides the massive performance and scalability required today. In addition, it uses the knowledge of mobile and fixed network architecture and traffic patterns to better detect infections – and to protect both subscribers and the infrastructure. Finally, it can be virtualized to provide cost-efficient NFV deployment and elastic growth.

Learn more

Motive Security Guardian helps service providers build greater trust in their networks while protecting the subscriber experience. Learn more about Motive Security Guardian and how security analytics can help improve security operations, customer care and wireless network efficiency.

More information is available on our website.

Ⓜ MOTIVE
BY ALCATEL-LUCENT