Improve efficiency while protecting the network

Motive Security Guardian (formerly Kindsight Security)

- **Clearly measure and understand malware's impact on scarce mobile network resources, such as bandwidth usage, signaling and airtime**
- **Achieve better return on investments and optimize network availability and quality of service by containing threats**
- **Improve cost-efficiency through elastic, virtualized deployment**

Networks are facing unprecedented traffic growth as demand from our ultra-connected society increases exponentially. Video services, M2M and social media all put pressure on network resources. Yet service providers need to deploy the network in the most profitable way, while meeting this demand.

These business and technical challenges are intensified today, because over 23 millions mobile devices and 14 percent of home networks are infected with malware.[1] In addition to its well known perils, malware can waste a significant amount of traffic, airtime and signaling resources: field results showed almost 1TB/day consumed by a single type of malware on a network connecting 1 million devices. The result is a waste of bandwidth and spectrum, both key investment areas for mobile service providers and increasingly scarce resources.

Therefore, protecting infrastructure and subscribers from malware is now critical for service providers. With effective malware protection, they can make the best use of existing investments, reduce operating expenses and optimize network availability and quality of service.

Value proposition

The Motive Security Guardian (formerly Kindsight Security) addresses these challenges.

Improve efficiency by identifying waste

As demand keeps increasing, network operations teams need to optimize the use of existing network resources to deliver the best quality of service. Although signaling storms and congestion occur in any network, service providers should prohibit malicious traffic as the cause. Motive Security Guardian helps identify network inefficiencies by measuring the bandwidth, airtime and signaling consumed and wasted by malware. This enables the operations team to take adequate actions.

Secure the network for better quality of service

Detecting and helping to remove malware from devices makes the network a safer place and provides a better quality of service. Motive Security Guardian can take these steps in the following ways:

- Contain threats to minimize resource consumption: Motive Security Guardian can work with any Policy and Charging Rules Function (PCRF) through the standard Sd interface. This allows service providers to contain threats and put infected subscribers in quarantine or in a walled garden – ensuring network resources are not wasted due to malware
- Remove existing malware proactively by reaching out to the most-affected subscribers
- Help subscribers avoid infection by providing complete malware protection, by complementing classic device-based protection with network-based protection
- Protect the network from distributed denial-of-service (DDoS) or other large-scale attacks that can severely impact the operation of the network and/or the quality of service

Make the most of existing resources

For mobile service providers, maximizing the return on current investments is critical to cope with demand. Motive Security Guardian helps network operations achieve this goal. It also helps network planning teams deploy new resources more

[1] These estimates are based on the latest research from Motive Security Labs (previously Kindsight Security Labs).

MOTIVE
BY ALCATEL-LUCENT

effectively and more accurately, at the right time and for the right reasons. Insights are provided in the following three dimensions:

- **Bandwidth:** Malware can consume large amounts of bandwidth, both in the access and the core of the network. Motive Security Labs has seen cases of ad-click fraud that consume several hundred of gigabytes per day.
- **Spectrum efficiency:** At a macro-level, spectrum shortage is a top concern for mobile service providers. It is a very costly and scarce resource, and in many markets there is simply not enough available, making it imperative to use it effectively. Malware can typically waste it by sending radio signaling requests and releases very often.
- **Airtime:** Malware can typically maintain very long and costly connections, especially in LTE networks. This must be avoided to make the best use of scarce resources in the RAN.

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:

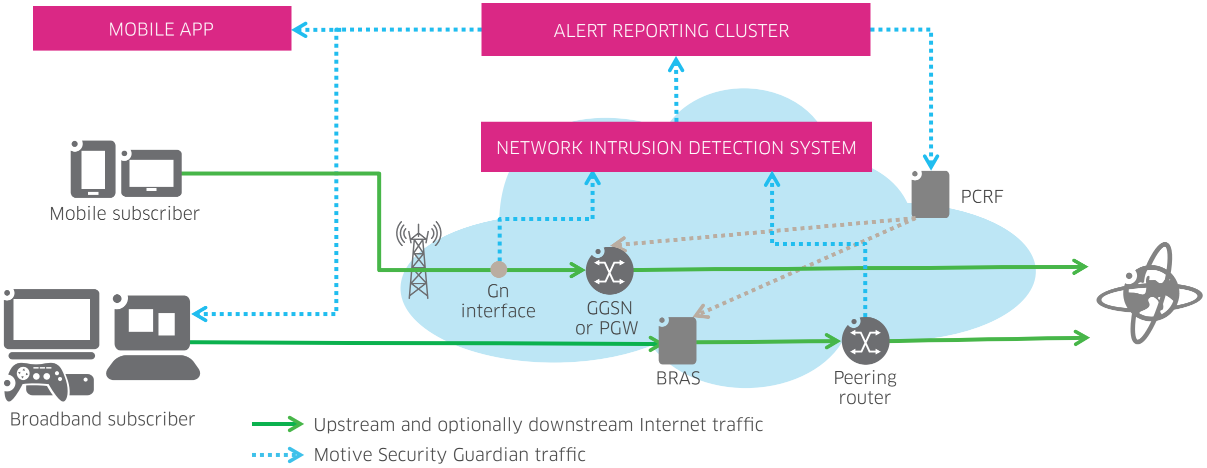
- Application provisioning
- Automated network infrastructures upgrades and patches
- Self-healing and self-scaling cloud resources

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.

Related products and solutions

As a part of the Motive Big Network Analytics solution, Motive Security Guardian can act as a

Motive Security Guardian architecture


MOBILE APP
ALERT REPORTING CLUSTER
NETWORK INTRUSION DETECTION SYSTEM
PCRF
Mobile subscriber
Gn interface
GGSN or PGW
Broadband subscriber
BRAS
Peering router
Upstream and optionally downstream Internet traffic
Motive Security Guardian traffic

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 Motive ServiceView solutions 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 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 doesn't 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. 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 is displayed in an easy-to-use dashboard and customizable reports. The alerts also correlate infections, subscribers and network resources, so security operations saves time in analysis and can coordinate actions with network operations, customer care and marketing teams.

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.

Solution features

FEATURE	BENEFIT
Detection of malware infections by analyzing traffic from all devices	Provide better malware protection than traditional approaches, by covering any device and leveraging service providers' key asset: the network.
Measurement of network resources consumed by malware	Gain insights into the exact amount of resources wasted because of malware.
PCRF integration	Get the ability to put infected subscribers in quarantine or redirect them to a walled garden, and contain the infection.
Performance and scalability	Support the largest fixed and mobile service provider networks, unlike other solutions designed for enterprise deployments.
NFV and virtualization	Deploy cost-effectively in virtualized environments to support elastic growth as demand changes.

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. It can also enable a revenue-generating, value-add security service for both mobile and residential subscribers.

More information is available on our website.