Improve customer care and protect the subscriber experience

Motive Security Guardian (formerly Kindsight Security)

- **Significantly reduce the number of security-related tickets**
- **Pinpoint and resolve malware-related issues faster**
- **Proactively address subscriber security issues and enable self-care**

In many markets, service provider offerings all seem very similar, and the customer experience has become the new frontier for competitive differentiation. That's why customer care teams must provide a best-in-class experience – to retain existing subscribers and attract new ones. Consumers can easily switch providers, so they expect and deserve flawless, engaged support when they have a problem.

However, delivering this kind of support is a growing challenge for customer care teams. The way customers use broadband services results in support calls for a wide range of reasons, making it harder than ever to resolve an issue. Successful resolution requires having comprehensive insights and the right expertise to identify the root cause and provide effective guidance for getting the issue fixed. This is particularly true for security issues, which can result in many lengthy calls before problems can be identified and solved.

Security is a challenging topic for subscribers as well. Antivirus software is the most common tool to fight malware, but even when used, it often fails to identify threats. Moreover, mobile subscribers often don't understand the need to install antivirus on their devices, and they don't know which software to choose. As a result, a recent Motive study has shown that 65 percent of subscribers expect their service providers to protect their devices.

Value propostion

The Motive Security Guardian (formerly Kindsight Security) helps service providers build trust in their network while protecting the subscriber experience.

Improve time to resolution with better insights

Customer care teams can leverage a security analytics dashboard to improve First Call Resolution, Average Handling Times and overall Customer Satisfaction Scores. Knowing immediately that malware is involved helps customer care engage more effectively with a subscriber and provide a better customer experience.

For example, subscribers might call because their mobile device's battery is draining too quickly, because they experienced bill shock at the end of the month or even because they get unwanted ads on their computer at home. These problems might seem completely unrelated, but they might all be evidence of a single issue: The subscriber has been infected with malware. Having information about malware infections enables a customer care agent to provide a better response and solve problems faster.

Motive Security Guardian provides an easy-to-use visual dashboard with all the information customer care agents need when a subscriber calls about a problem. With this information, agents can immediately determine whether a subscriber is infected with malware, and which malware is

MOTIVE®
BY ALCATEL-LUCENT

involved. Then they can quickly prioritize which actions to take and provide more insightful answers for subscribers.

In addition, the number of security-related tickets can be reduced dramatically: For a service provider offering a security service based on Motive Security Guardian, that number decreased by 97.5 percent, compared to a service based on a traditional antivirus solution.

Make security simple to build trust in the network

In addition to the advantages it provides for customer care, Motive Security Guardian offers the following advantages for subscribers and service providers:

- It catches more malware, with more accuracy.
- It does not require software installation on customer devices to detect malware.
- Its cloud-based malware detection protects all subscriber devices at once. It's always on and always up-to-date. And it doesn't slow performance or drain the battery while looking for malware.

Then, if a subscriber device is infected, it sends the subscriber an alert, proposes the right tools and offers step-by-step instructions for removing the malware. These remediation capabilities make it as simple as possible for subscribers to protect their devices and solve malware issues.

This promotes subscriber trust that their service provider is protecting their experience, which in turn helps improve Customer Satisfaction Scores and Net Promoter Scores, key metrics of customer care performance.

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.

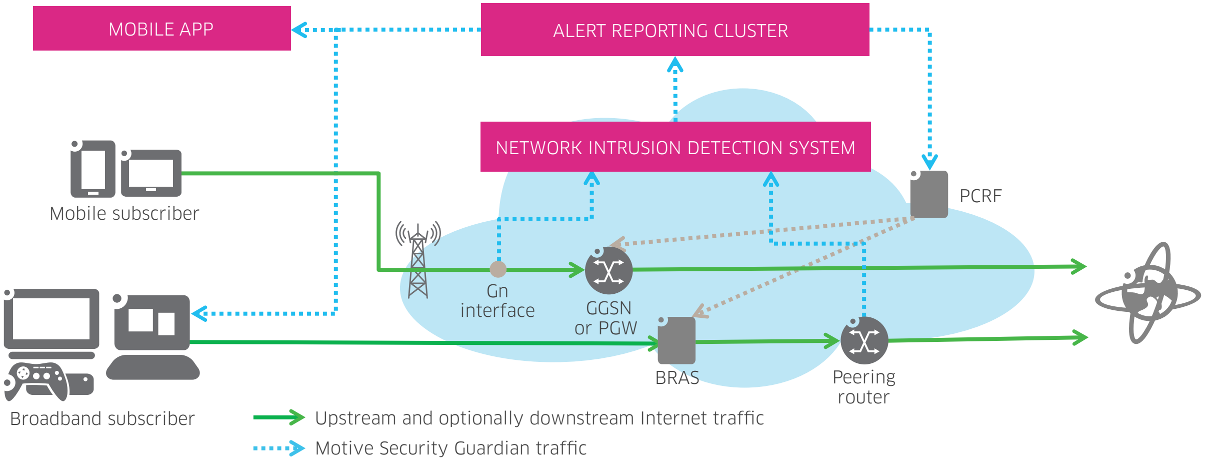
Alert Reporting Cluster

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

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

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.

Easy integration with customer care platforms

Motive Security Guardian can be integrated with customer care solutions, and is pre-integrated with Motive Customer Care Solutions. The following models can be used:

- Integration in the customer care console. This gives agents immediate access to key information when subscribers call. So they know right away when an issue is caused by malware.
- Integration with a self-care system, allowing subscribers to see and resolve the issue themselves, without having to call for support.
- Pro-active resolution: The security analytics dashboard identifies the most-infected subscribers, allowing customer care teams to contact them before they even know they're infected, then help remove the malware before it does further damage.

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.
Measure traffic, airtime and signaling generated by malware, per subscriber	Enable customer care agents to know if customers are infected.
Integration into customer care agent's console	Enable customer care teams to know immediately if subscribers' devices are infected, which malware is active and the exact volume of traffic generated by the devices. This helps improve First Call Resolution, Average Handling Times and overall Customer satisfaction scores.
Automated notification and remediation workflow for self-care	Fix issues by sending alerts to the infected subscribers over email, SMS, mobile app notification or web portal, with instructions and tools to remove the malware. This approach gives subscribers more freedom and power and reduces calls to the helpdesk.
Detection and blocking of malware traffic	Improve the customer experience and reduce subscriber churn, as infected devices can cause sub-par performance or unexpected data charges that result in unhappy subscribers.

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.

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

More information is available on our website.

MOTIVE
BY ALCATEL-LUCENT