Empower security operations with actionable malware intelligence

Motive Security Guardian (formerly Kindsight Security)

- **Malware protection for networks and subscribers, even for attacks that originate from within the network**
- **An innovative, patented approach to malware detection that is always on and always up to date – leveraging the service provider network to catch more infections, more precisely**
- **Dashboards and reports that provide clear insights into how infections impact the network and subscribers and enable a specific and rapid response**

As subscribers rely increasingly on their devices and services from the cloud, they expect and deserve more-effective malware protection. That means protecting the customer experience is no longer an option for service providers. However, security operations teams are also facing tougher challenges as they work to meet these new expectations.

Attacks are becoming more elaborate. Networks and IT systems are more complex, and the growing variety of devices outside their control makes their job more difficult. The question is not whether an attack will occur. It probably already has. The real question is: What's the most effective way to detect an attack – and enable a fast reaction?

With security threats becoming more frequent and more dangerous, all service providers want to protect their infrastructure. However, the reality is that they often focus on threats that originate from outside their network, and overlook devices and endpoints when defining their security strategy. This approach might have been adequate in the past. But today, it is not sufficient. Service providers worldwide must now find ways to protect subscriber devices, including those used for machine-to-machine communication.

Many large-scale, severe attacks, such as advanced persistent threats (APTs) or distributed denial of service (DDoS), use infected endpoints to attack the network from within. That's why these endpoints must be an integral part of any complete security strategy and need to be protected from malware. Protecting these devices helps to protect the network as well.

Unfortunately, traditional antivirus software is not sufficient for today's challenges and leaves many devices unprotected. Public studies show that it catches less than half of infections, and the updates needed to detect new threats often take several weeks. Furthermore, mobile subscribers often don't understand the need to install antivirus on their devices. Service providers must take action now to protect the network, subscriber devices and the overall subscriber experience.

Value proposition

The good news is that service providers are in a unique position to provide the most-effective malware protection – by leveraging their key asset, the network. Motive Security Guardian (formerly Kindsight Security) offers cloud-based malware detection. It identifies malware infections in residential and mobile devices without requiring any software installation on the devices and is always on and always up to date.

MOTIVE®
BY ALCATEL-LUCENT

A patented, more efficient approach to detecting malware

Rather than scanning files, Motive Security Guardian's innovative, patented approach looks for network communications between devices and command-and-control (C&C) infrastructures. This has proven to be a much more efficient way to detect malware, and it provides extremely low false-positives. To accurately detect that a user is infected, the Motive Security Guardian signature set examines network behavior, looking for unequivocal evidence of infection coming from a user's computer or mobile devices. This distinctive behavior includes:

- Malware C&C communications
- Backdoor connections
- Attempts to infect others, such as exploits
- Excessive e-mail
- Denial of service (DoS) and hacking activity

To support accurate malware detection, the Motive Security Labs (formerly Kindsight Security Labs) vault contains more than 30 million malware samples, and more than 120,000 samples are collected and analyzed daily.

Actionable insights for faster response times

Motive Security Guardian is designed to bring new insights, not just alerts. As an infection generates hundreds of network events, the product aggregates and filters the information, and correlates three dimensions — subscribers, infections and network resources. So, instead of sending hundreds of hard-to-interpret alerts, the system shows the most-infected subscribers, the most common malware in the network and the associated resources that are consumed. The Motive Security Guardian dashboard provides these crucial insights, and it also reports on the impact of malware on network bandwidth and signaling. This information can be viewed for individual users or aggregated on a per-malware or system-wide basis. This helps security teams understand the issues faster, then prioritize the actions required to resolve them.

Containing threats with policy enforcement

The Motive Security Guardian can be integrated with a Policy and Charging Rules Function (PCRF). Network actions, like quarantine or redirection to a walled garden, can be triggered to isolate infected subscribers. These steps help ensure that a threat does not spread throughout the network — protecting the integrity of the network and the overall quality of service for other subscribers.

Integration with customer care and self-care

Integration with customer care solutions is another important option. For example, this enables helpdesk and customer care teams to proactively reach out to the most-infected subscribers, helping them remove infections before they even realize they're under threat. And it can save time in issue analysis when an infected subscriber calls in.

In addition, Motive Security Guardian helps eradicate problems at their root. It sends alerts to infected subscribers through a mobile application, SMS, e-mail or even a web portal — then guides the subscriber with step-by-step instructions and tools to remove the malware. Marketing and product development teams can also offer these capabilities as a value-added service to help minimize the problem at large.

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:

- 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.

Related products and solutions

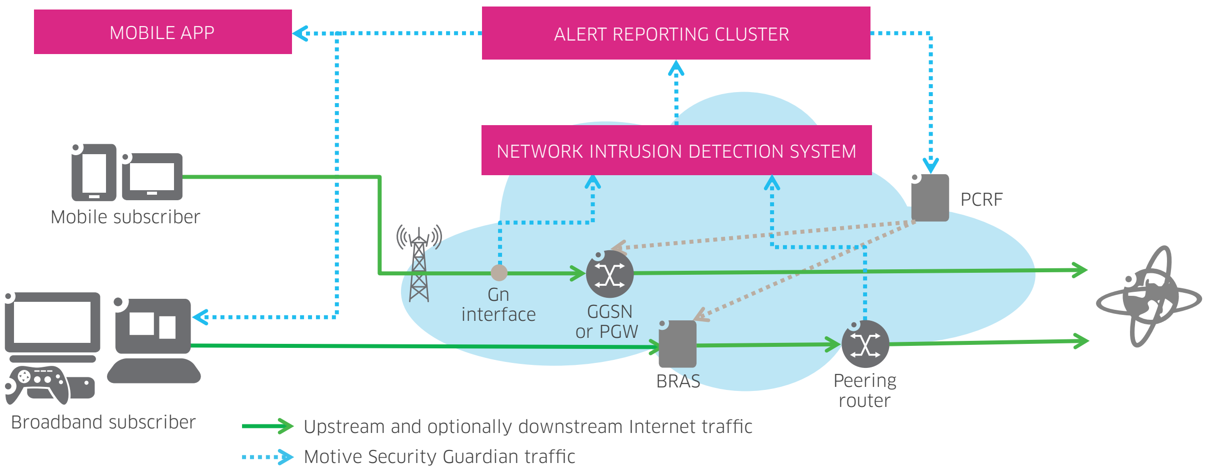
As a part of the Motive Big Network Analytics solution, Motive Security Guardian can act as a standalone system for simplicity and agility, or it can be integrated with the Motive Wireless Network Guardian as a security module. It is also pre-integrated with Motive ServiceView solutions for for customer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

The Motive advantages

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

Motive Security Guardian architecture


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

Solution features

FEATURE	BENEFIT
Passive, real-time traffic analysis for both fixed and mobile networks	Malware detection in any type of network with no impact on network performance
Better malware detection by analyzing upstream Internet traffic	Greater precision than traditional approaches – while protecting any device without software installation on the devices and remaining always on and always up to date
Correlation of key measurements	Easy identification of most-infected subscribers, the most common malware in the network and the associated resources that are consumed
Actionable intelligence displayed in easy-to-use dashboards	Quicker insights into the actions required to contain the threat and solve the issue
Versatile and flexible platform	Customization that allows use across the service provider's organizations, including security operations, customer care, marketing and product development, and network operations
High-performance network sensors that support 20 Gb/s of traffic analysis and more than 100,000 events per minute	Support for even the largest networks with hundreds of millions of subscribers
Deployment in physical as well as virtualized environments	Cost-effective deployment through standard, off-the-shelf hardware, with simplified management and lower OPEX

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 and threat intelligence widely, 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. It's 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.