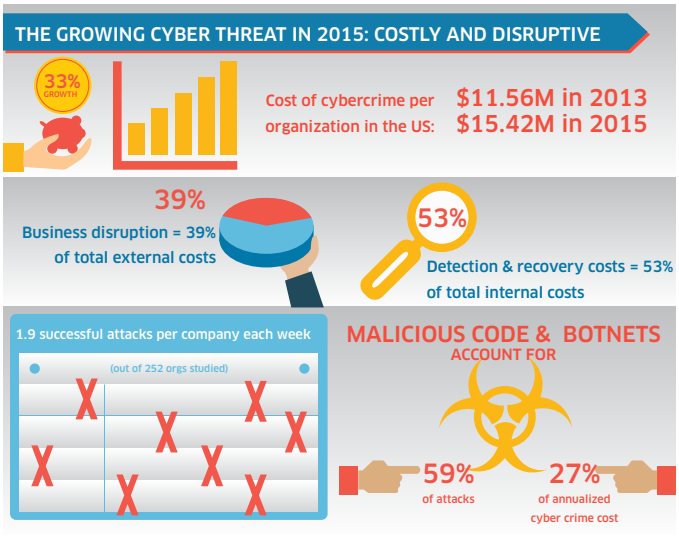
# SOFTWARE INTEGRITY TO SECURE NETWORK ASSETS

Alcatel·Lucent
Enterprise

Network hacks, data breaches, information theft, and other malicious network attacks are on the rise – and so is concern for overall network security strategy. Nearly one million malware threats are released worldwide every day, and it takes an average of 46 days to resolve a malicious attack which threatens critical operations, organizational reputations, and even the financial viability of many companies. Given the potential repercussions surrounding network attacks, it is crucial that organizations deploy a proactive, defense-in-depth strategy that addresses all layers of the network.

**Figure 1: The growing cyber threat in 2015: costly and disruptive**




Source: Ponemon Institute, 2015 Cost of Cyber Crime Study: Global

ALE, operating under the Alcatel-Lucent Enterprise brand, recognizes the importance of network level software integrity as a component of the larger network security ecosystem. ALE has taken an unprecedented step in the industry and partnered with LGS Innovations, a leader in cyber security, to offer CodeGuardian™, a technology that hardens network devices at both the software source code and binary executable levels to enhance overall network security.

In this partnership, the LGS CodeGuardian technology has been applied to the Alcatel-Lucent OmniSwitch® product family, adding extra protection to the portfolio.

# STAYING SECURE IN AN EVOLVING ENVIRONMENT

Cyber attack sophistication continues to evolve such that no single approach can guarantee the security of a company's digital assets. It is necessary to implement an in-depth defense with multiple layers of security, extending from the user device (with antivirus, passwords, encrypted connections), all the way to the network infrastructure, data center and firewall. Doing so will protect the traffic flowing between the corporation and the outside world, including the Internet.

The Alcatel-Lucent Enterprise solution supports multiple corporate IT areas for you:

- Network access control at both wired and wireless interfaces – enforcing role-based access and a quarantine process for unauthorized or non-compliant users
- Device health check to support a secure adoption of BYOD
- The comprehensive Alcatel-Lucent OmniVista® 2500 management system which offers multiple administrative roles, guaranteeing the right privileges to the right people
- Application analytics, using DPI technology, to identify in real time, applications traversing the network and potentially blocking the use of unsecured applications
- Smart analytics to detect anomalies and potential denial of service (DoS) attacks.
- Multiple embedded operating system techniques to mitigate or prevent attacks, including flood control gates, port scanning detection, task CPU usage monitor and control, etc.)

Modern day routers and switches are customized embedded computers, and the software running on them is not protected by traditional IT security mechanisms such as virus scanners. This leaves routers and switches susceptible to the introduction of malware and other attacks, potentially causing:

- Compromise of network connectivity (including rejecting or redirecting traffic)
- Opening of the network to further attacks by compromising security policy on the network
- Exposure of the network to theft of sensitive data
- Interruption or corruption of network traffic
- Blocking of all traffic by rendering the network hardware inoperable

The OmniSwitch product family adopts multiple operating system built-in techniques to mitigate or prevent attacks, including flood control gates, task CPU usage monitor and control. In order to further secure the operating system (AOS) running on the switches and routers, the OmniSwitch has adopted the LGS CodeGuardian technology. This technology mitigates larger enterprise risks at the source, enabling an enhanced security profile through:

- Independent verification and validation of OmniSwitch source code
- Software diversification of OmniSwitch object code to prevent exploitation
- Secure delivery of OmniSwitch software to customers

CodeGuardian protects networks from intrinsic vulnerabilities, code exploits, embedded malware, and potential back doors that could compromise mission-critical operations. CodeGuardian promotes a proactive, defense-in-depth approach toward network security. The CodeGuardian technology is continuously applied on every new AOS release, therefore it will addresses both current and future threats.

# A THREE-LAYER APPROACH TO SOFTWARE ASSURANCE

LGS' CodeGuardian technology hardens the OmniSwitch software through a combination of:

- Independent verification and validation (IV&V) and vulnerability analysis of switch source code
- Software diversification to prevent exploitation
- Secure delivery of software to customers

This three-layer approach not only ensures security, but chain of software custody control as well. The following sections describe each layer in more detail.

## INDEPENDENT VERIFICATION AND VALIDATION (IV&V) AND ANALYSIS OF SOURCE CODE

IV&V provides operational vulnerability scanning and analysis of switch software within the network equipment portfolio, reviewing the source code for:

- Equipment software vulnerabilities: Bugs and flaws contained in software
- System exploits: Concepts or code that take advantage of vulnerabilities to gain initial access to the operations of a system
- Embedded malware: Code loaded onto a system to inflict damage, collect data, change the functioning of the system, or launch attacks at other systems
- Back doors in software: Code intentionally designed into a system that bypasses normal authentication checks in order to give access or control. Examples include field debugging capabilities, secret key strokes, special login sequences, or hidden login user IDs.

CodeGuardian IV&V and vulnerability analysis addresses external interfaces such as:

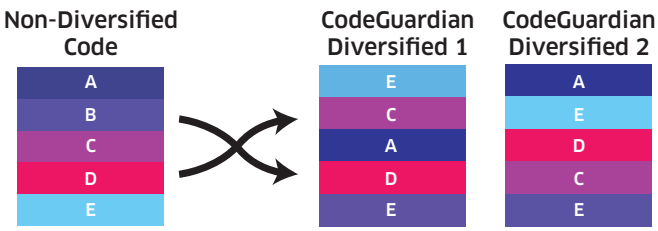
- HTTPS interface
- Login interface
- NTP interface
- Command Line Interface
- IP Port usage
- SNMP interface
- Data Packet interface

## SOFTWARE DIVERSIFICATION TO PREVENT EXPLOITATION

CodeGuardian technology also implements software diversification to randomize the executable program address space so that various instances of the same software, while functionally identical, are arranged differently on the binary level, making any address-dependent exploits ineffective on other diversified instances of the software. This prevents attackers from:

- Gaining access to information (data theft)
- Performing unauthorized actions or commands (privilege escalation)
- Preventing routine operation of a system (e.g., Denial-of-Service (DoS))

**Figure 2: CodeGuardian's diversification process**




In order to perform an exploit against a target, an attacker will typically take advantage of a vulnerability in a system, which often requires knowledge of the underlying address layout of an application. CodeGuardian's diversification process mitigates this risk by analyzing and modifying the position of application components, thereby reducing the effectiveness of attacks based on the address layout of a standard, non-diversified version of the software.

## SECURE DELIVERY OF SOFTWARE

From the time the switches leave the shipping facilities of ALE until it arrives at the customer premises, they can pass through multiple entities where ALE has no control. In order to minimize any chance of tampering with the AOS software, the customer receives with the hardware a welcome letter including credentials to securely access Alcatel-Lucent Enterprise web servers and download the appropriate secure AOS software. This process makes sure that the product is running the latest software version and includes all of the high-quality standards upheld by ALE's R&D.

# ALCATEL-LUCENT ENTERPRISE AND LGS INNOVATIONS
## PARTNERING FOR BEST-IN-CLASS NETWORK SECURITY

The OmniSwitch family is used and trusted by:

- Healthcare institutions
- Government agencies
- Information technology organizations
- Military operations
- Academic institutions

LGS INNOVATIONS
LISTEN · INNOVATE · DELIVER™

The OmniSwitch product family is changing the way government and commercial organizations work and communicate. The product family encompasses the most advanced line of switching and routing platforms that have the same feature set, are supported by a single operating system (AOS) and network management tool – the OmniVista 2500. The OmniSwitch line meets the most stringent and mission critical networking requirements for a network's access, distribution, core and data center.

LGS Innovations delivers solutions addressing the most complex networking and communications challenges facing the U.S. federal, state and local governments, critical infrastructure operators, and commercial enterprises worldwide. LGS offers groundbreaking research, development, and solutions in cyber security. To support CodeGuardian, LGS has formed an advisory committee that includes highly respected industry experts in cyber security, with current and past experiences from the #CyberUL project, "the L0pht" hacker think tank, DARPA, Google, national AFCEA Intelligence Committee.
By integrating LGS' CodeGuardian technology in the software development and delivery processes, ALE is committed to delivering the most secure software solutions within its switching equipment.

To learn more, visit http://enterprise.alcatel-lucent.com/?product=EnterpriseProducts&page=directory&active=8#Security



Alcatel·Lucent
Enterprise