MASERGY
Performance Beyond Expectations

CLOUD SECURITY

Unified Security Anywhere™

CLOUD GUARD™ – UNIFIED ENTERPRISE CLOUD SECURITY

Cloudy with a 90% Chance of Attacks

How secure is your cloud computing environment? If you've read the section in your customer service agreement that says you bear sole responsibility for the security of your content and applications in the cloud, you now realize that it's only as secure as you make it. Are you wondering what you should do next?

The answer is simple: Call Masergy®. Our Cloud Guard™ solution is the only security technology for cloud computing environments that utilizes an award-winning, industry-proven, unified architecture – one that's built from the ground up using network behavior analysis and correlation as the enabling technology – so you have visibility into pre-attack reconnaissance activity with earlier warnings of threats and alerts for security issues that other technology may not detect.

With a comprehensive, fully integrated suite of cloud security applications—patented network behavior analysis and correlation; PCI-enabled intrusion detection; vulnerability scanning and management; log management, analysis and monitoring; network access and policy monitoring; and comprehensive threat management for prioritized network, global and vendor threats and vulnerabilities – you benefit from a set of combined capabilities that can't be found anywhere else, including:

- The use of raw network packet data, IDS alerts, scans, logs, vendor threats, global threats and policy violations, so you have access to more data for analysis;
- Continuous correlation and analysis of information that can be tracked over significantly longer periods of time – rolling 14-30 days for raw packet data, up to six months for alerts, and up to two years for behavioral profiles;
- A learned intelligence capability that can predict behaviors and help you track developing threats; and
- The ability to deploy based upon your specific business requirements – whether you have a premise-based, cloud or hybrid network environment.

COST-EFFECTIVE, UNIFIED SECURITY ANYWHERE™

- Provides visibility into pre-attack reconnaissance activity, enabling earlier warnings of threats.
- Tracks developing threats before they can harm critical systems.
- Produces alerts for security issues not detectable by other technology.
- Provides virtually unlimited scalability.
- Ensures full regulatory compliance with industry and government standards.
- Utilizes 100% passive technology, ensuring zero network latency.
- Enables unified administration, monitoring and reporting with comprehensive compliance reports, weekly and summary reports, and an integrated network security ticketing system.
- Provides up to a 60% savings in security-related capital expenditures, training and staffing.
- Offers world-class Managed Services, including comprehensive alerting and incident response, compliance services for PCI, NERC CIP and HIPAA, vulnerability assessments, penetration testing, security audits, and more.

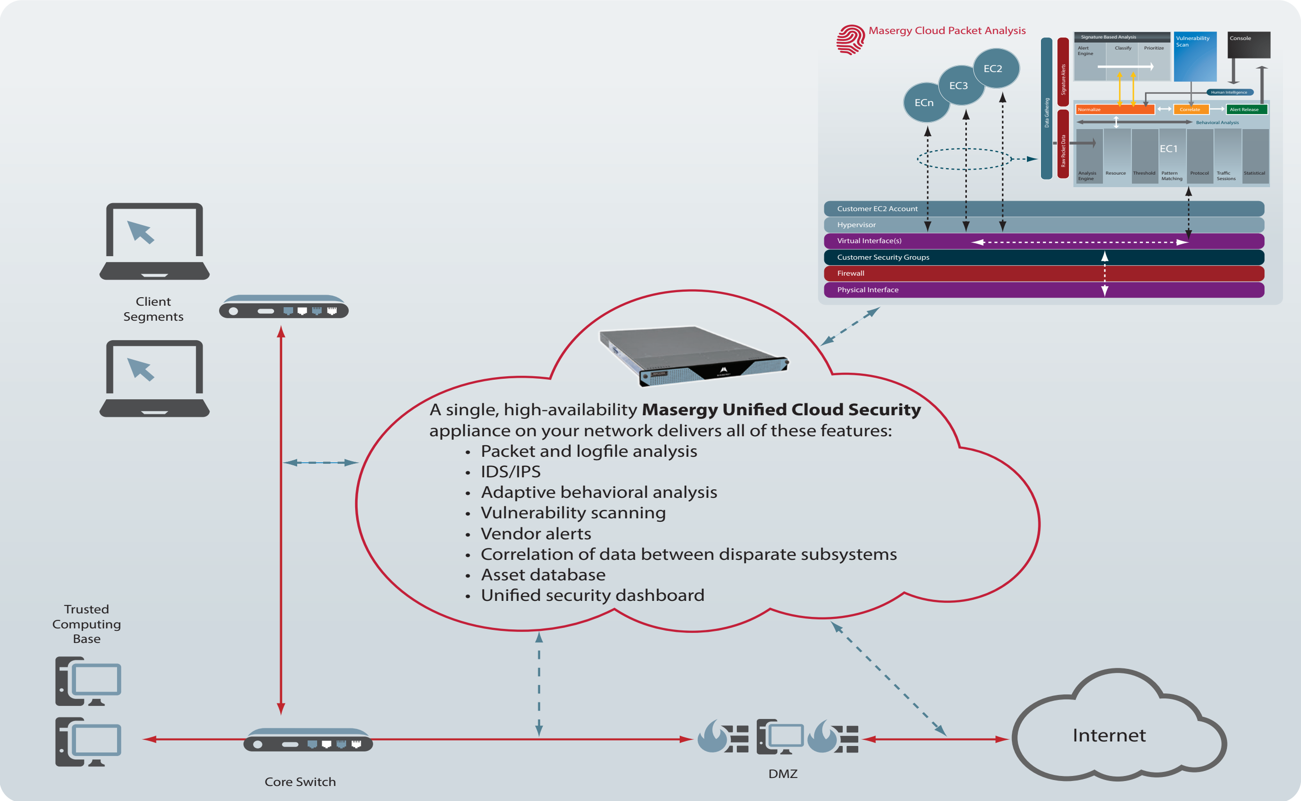
What's more, we back our technology with 24/7 managed security services to provide real-time visibility, control and oversight of your organization's entire security environment. This gives you immediate, turnkey access to one of the industry's leading Security Risk Management solutions – so you can protect your cloud applications and data wherever they reside.

Whether you need full-time support, nights, weekends or holidays, you can economically augment your IT staff and gain quick, easy access to actionable remediation information that can help you to prevent network security problems.

Need more proof? No problem. We've been delivering this same unified security architecture, along with industry-proven applications and world-class Managed and Professional Services, to Fortune 1000 companies on three continents since 2001. And our customer retention rate is well above 90% – quite an achievement in today's volatile market.

So give Masergy a call and let us show you how to make blue skies out of a cloudy day.

Masergy Unified Cloud Security Architecture



A single, high-availability **Masergy Unified Cloud Security** appliance on your network delivers all of these features:

- Packet and logfile analysis
- IDS/IPS
- Adaptive behavioral analysis
- Vulnerability scanning
- Vendor alerts
- Correlation of data between disparate subsystems
- Asset database
- Unified security dashboard

Within a hybrid deployment environment, the Masergy Virtual Detection + Prevention Module (DPM) connects to Master Control Unit (MCU) and Behavioral Correlation Module (BCM) for true unified network security.

CUSTOMIZED CLOUD SECURITY DESIGNED WITH YOUR BUSINESS IN MIND

Many organizations today are rushing to realize the advantage of cloud computing by implementing business critical applications in the cloud. While there are a multitude of service models used to deliver cloud applications, each has its own unique set of security challenges.

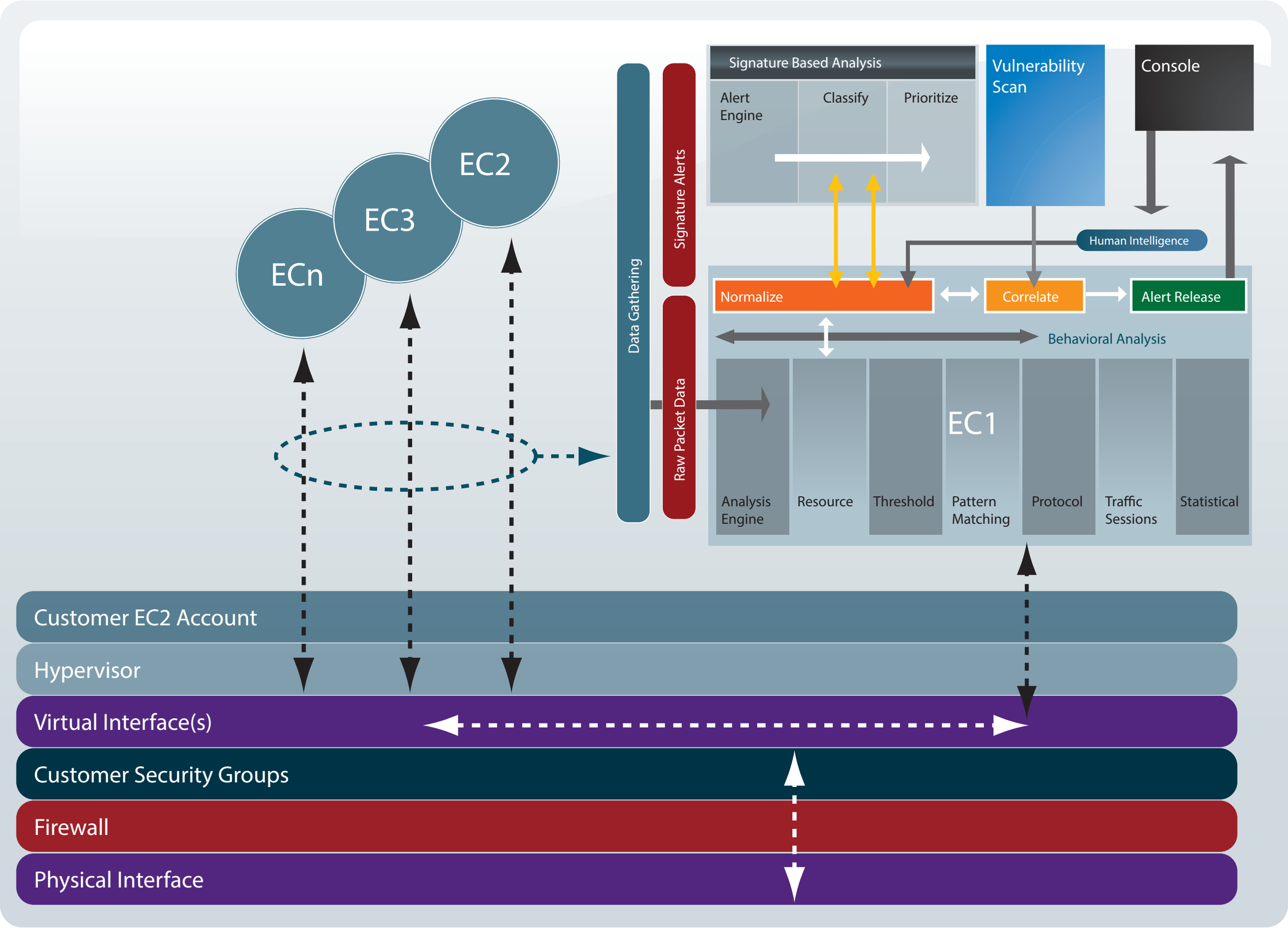
Beyond the basic firewall support provided with each cloud account, regulatory compliance still requires companies to monitor for hackers and malware, collect system log information, perform regular vulnerability tests, and remediate where necessary. Additionally, some regulatory compliance standards require network access, policy oversight and 24/7 network security monitoring.

These security requirements are further complicated by numerous restrictions placed on customers by cloud providers, including a customer's inability to deploy their own security appliances, a prohibition on vulnerability scanning, and the inability to monitor network packet information, even between instances within the same account.

Masergy's cloud technology has overcome these restrictions so that Cloud Guard modules can operate as an integrated system within each customer cloud account, providing signature intrusion detection, network behavior analysis (NBA) and correlation, vulnerability scanning, log management and monitoring, network access & policy management, and threat management to ensure full regulatory compliance.

Masergy's unified security architecture and plug-n-play modules allow you to customize your Unified Cloud Security solution to fit your unique cloud or hybrid environment as well as your IT budget. Customized Cloud Guard applications include:

Masergy's Cloud Packet Analysis Approach



Masergy's unique proprietary cloud technology overcomes EC2 restrictions to provide signature detection and network behavioral analysis (NBA) & correlation. In addition, Masergy Cloud Guard System Modules operate as EC2 instance(s) within each customer cloud account while the integrated Vulnerability Scanner ensures full regulatory compliance.

INTRUSION DETECTION

The Intrusion Detection module delivers requisite intrusion detection compliance for Cloud, CPE and Hybrid environments and is designed to run within each customer's virtual server instance(s) to detect malicious traffic, regardless of where applications and data physically reside. This 100% passive technology ensures zero network latency and:

- Supports PCI specific signatures and the latest malware signatures.
- Includes real-time custom signature development that enables tailored Data Leakage Protection (DLP).
- Detects, captures suspicious traffic for behavioral analysis and correlation.
- Provides automatic signature updates keep your system fully-optimized.
- Automatically correlates with Network Behavioral Analysis software to ensure coverage for stealth attacks, unloaded signatures, and zero hour attacks.
- Correlates with detected vulnerabilities to ensure that low priority events are properly classified when targeting known vulnerabilities.
- Provides a fully integrated ticketing and incident response system and is backed by
- Masergy's cost effective, 24/7 security monitoring services.

NETWORK BEHAVIORAL ANALYSIS AND CORRELATION

The Behavioral Correlation Module™ (BCM) is by far the best method for detecting reconnaissance activity leading up to an attack – especially low level or slow activity – as well as inside threats or abuse. Why it is better? Well, it's because this software continuously analyzes and correlates raw network packet data as well as stored behavioral profiles and signature alerts for quick identification of suspicious activity. It also:

- Gives you a safety net for the more than 95% of signatures and zero-hour attacks that aren't loaded into traditional IDS and IPS devices.
- Captures and continuously analyzes between 14 and 30 days of suspicious network traffic and up to two years of behavioral profiles and signature alerts in order to detect reconnaissance activity leading up to an attack.
- Includes a multi-tiered correlation capability that covers your entire network as well as global threats.
- Monitors suspicious activity for both external and internal traffic.
- Exceeds traditional frequency, threshold, and netflow-based detection.
- Vastly reduces false positives.
- Continuously adapts to each customer's unique network.

VULNERABILITY MANAGEMENT

As your virtual environment changes, the on-demand, virtual Vulnerability Scanner Module™ (VSM) helps you to keep pace by continuing to research potential security issues. The VSM provides custom scan schedules as well as extensive research capabilities. In addition, the VSM:

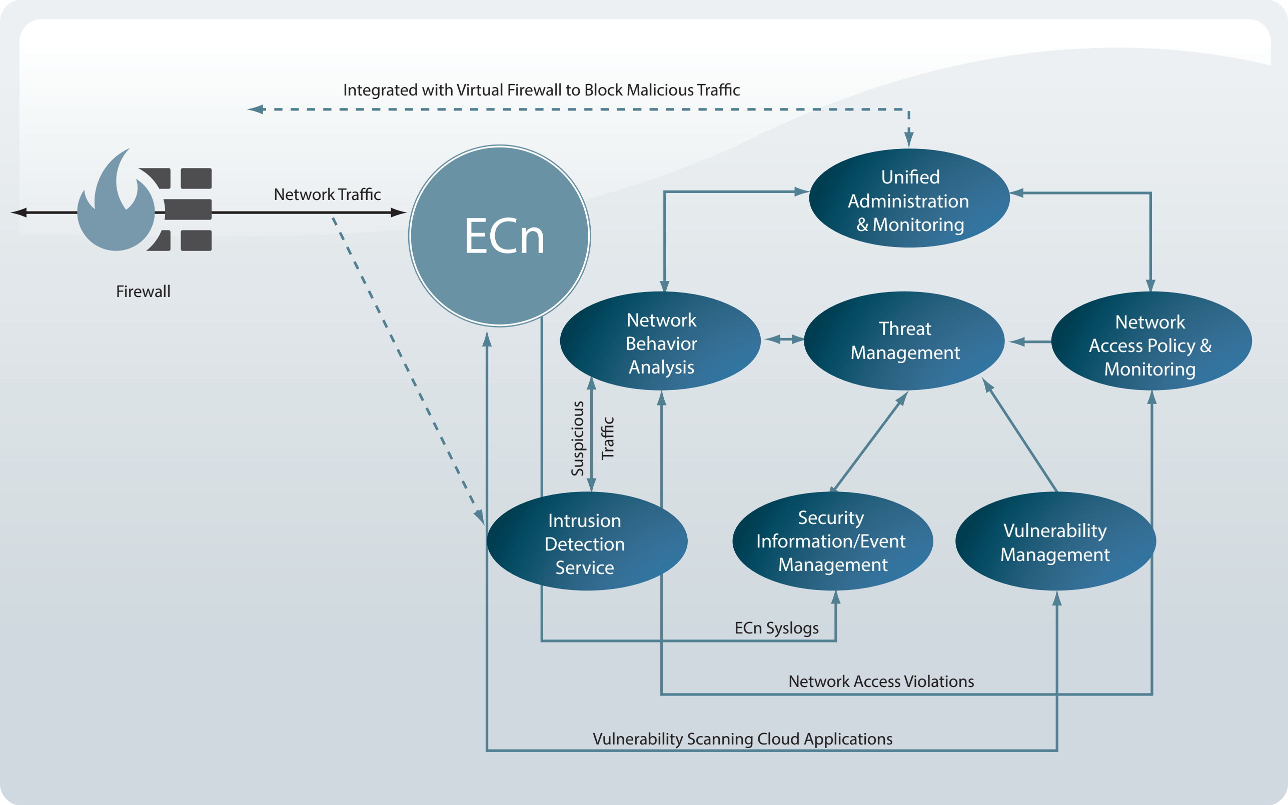
- Scans customer virtual machine images from within each customer account.
- Detects and reports PCI violations.
- Shares detected vulnerabilities with Intrusion Detection and Threat Management subsystems, which is unique to Masergy.
- Provides extensive reporting that includes individual vulnerability reports for each cloud virtual machine image (with associated risk levels and links to remediation steps) as well as summary and management reports for easier risk mitigation.

THREAT MANAGEMENT

The Security Dashboard Module™ (SDM) is designed to provide a simple, comprehensive rendering of your Cloud security posture, giving you immediate access to prioritized security threats and the underlying data that created them. The SDM automatically detects, correlates and prioritizes threats from multiple security, network and server sources within your Cloud instances, including network, global threats and posted vendor threats, as well as detected vulnerabilities. This allows you to identify the most critical threats, link threats to specific sources and targeted assets, determine the best remediation steps and appropriate patches, and gather data for forensic reporting. The SDM also:

- Tracks rolling 30-day threat remediation progress.
- Monitors and reports network access policy violations.
- Highlights primary attack types and vulnerability risk breakdowns.
- Identifies the geographic origin of an attacker via the global attack radar.

Masergy Unified Cloud Security Architecture


Integrated with Virtual Firewall to Block Malicious Traffic
Network Traffic
Firewall
ECn
Unified Administration & Monitoring
Network Behavior Analysis
Threat Management
Network Access Policy & Monitoring
Suspicious
Traffic
Intrusion Detection Service
Security Information/Event Management
Vulnerability Management
ECn Syslogs
Network Access Violations
Vulnerability Scanning Cloud Applications

Masergy's Unified Cloud Security is based on a modular systemic architecture that utilizes 100% passive technology and is hybrid Cloud/CPE enabled.

NETWORK ACCESS POLICY AND MONITORING

The Network Security Zones™ module (NSZ) is designed to establish, manage and monitor access policies for Cloud applications and is a cloud-ready alternative to Network Access Control and Identity & Access Management solutions. This 100% behaviorally-based solution supports DHCP (Dynamic Host Configuration Protocol) environments where it's necessary to track individual users or hosts independent of their IP addresses.

The NSZ module also requires no host agent software in order to define and enforce your corporate network security posture. Further, the NSZ software:

- Automatically generates access policy violations to the unified monitoring console and threat management dashboard for analysis, ticketing, and incident response.
- Enables continuous monitoring of secure relationships between specific network resources and users for specific time intervals.

LOG MANAGEMENT AND MONITORING

The ability to collect, analyze, respond to and retain log information is crucial to detecting potential security breaches, providing forensic capabilities, ensuring PCI compliance and enabling corporate accountability across your company's cloud and/or hybrid enterprise environment. Masergy's log management and monitoring software enables all log files to be continuously analyzed by customer-specific rule sets and then retained for reporting and forensics. Detected policy violations or activities of interest result in alerts on the unified management console for further analysis, incident response and ticketing. In addition, this module:

- Captures and analyzes logs from firewalls and syslog-producing applications. Collects and archives at least one year of syslog and/or Windows Event Logs for all Cloud applications.
- Establishes complex policies and monitors events for compliance.
- Includes an extensive policy-based rules processing capability.
- Policy enforcement capable
- Supports automatic or on-demand blocking at virtual Firewalls to block harmful network traffic (based on Cloud provider firewall policies).
- Integrates and correlates with other subsystem data.
- Supports a minimum of 1.5 Terabyte NAS in the cloud.
- Provides custom reports to meet your specific audit requirements.

FIREWALL MANAGEMENT AND MONITORING SERVICES

Masergy supports your cloud provider's virtual firewall and any other application or system syslog feed with unlimited changes to the existing firewall configuration and any required firewall maintenance updates. In addition, our trained security analysts can perform the following customer requested changes by the end of the next business day:

- Changes to the firewall rule base.
- Changes to security group definitions.
- Changes to the account authentication configuration established at the user, client, and session levels.

CERTIFIED COMPLIANCE IN THE CLOUD

Now that your cloud solution is up and running, you may be asking yourself, "how can I confirm that my cloud environment meets government and/or industry standards for compliance?" With Masergy on your team, you can be confident that it is. We understand that maintaining compliance in the cloud depends on a number of critical factors. That's why we've taken a holistic approach to our CloudCheck™ Certification Program. This comprehensive process is designed to provide you with a clear path to ensuring that your company is certified in the cloud. The CloudCheck seal lets your customers know that their sensitive personal information – and your company's confidential data – is protected. For more information, ask for a copy of the CloudCheck Certification Program Brochure and Checklist.

CloudCheck™
CERTIFIED

COMPREHENSIVE COMPLIANCE REPORTING

VULNERABILITY SCAN REPORTS **REPORTS BY VULNERABILITY, INCLUDING DETAILED DESCRIPTIONS, CONSEQUENCES, RISK FACTORS, REMEDIATION STEPS, AND LINKS TO CVES, PATCHES, AND MORE.**	
• Current Risk Report • Current Risk Summary • Ignored Vulnerabilities Report	• Vulnerability Escalation Report • Vulnerability History Report
VULNERABILITY MANAGEMENT REPORTS **LINKS THREATS WITH THREAT SOURCES, PORTS, PROTOCOLS, AND TARGETED ASSETS, AND PROVIDED REQUIRED REMEDIATION |STEPS & PATCHES**	
• Prioritized Vendor Threats • Prioritized Network Threats • Prioritized Global Threats • Prioritized Vulnerabilities	• Prioritized Threat List (all) • Rolling 30-day Threat Remediation Report • Network Access Policy Violation Report • Geographic origin of attackers.
OPEN SERVICES REPORTS **IDENTIFIES AND DOCUMENTS EXTERNAL USAGE OF ENTERPRISE SERVICES AND RESOURCES, AS WELL AS INTERNAL USAGE OF EXTERNAL SERVICES AND RESOURCES.**	
•Web Usage • Encrypted Web Usage • SMTP Mail Usage • Encrypted SMTP Mail Usage (SSL) • POP3 Mail Usage • Encrypted POP (SSL) Usage • IMAP Mail Usage • Encrypted IMAP Mail Usage • FTP Usage •Telnet Usage	• SSH Usage • LDAP Usage • Socks Usage • News Usage • Encrypted News Usage (SSL) •Windows Share Usage (netbios-ssn) • Napster Usage • IM Usage • Proprietary (other)

FLEXIBLE MANAGED SERVICES FOR YOUR CLOUD COMPUTING NEEDS

Once you have the CloudCheck seal, you can keep your Cloud Guard solution operating at peak efficiency with our world-class 24/7 managed or co-managed services. With or without a contract, you can cost-effectively allocate your internal resources and outsource network security requirements based on your company's specific needs.

Finally, industry-proven cloud security backed by comprehensive managed services – it's everything you need to help your company stay ahead of potential network security problems and save a bundle in capital expenditures, training and staffing.

CONTACT MASERGY TODAY

For more information regarding our Unified Enterprise Security solutions, contact us at 1 (866) 588-5885 or visit us online at www.masergy.com

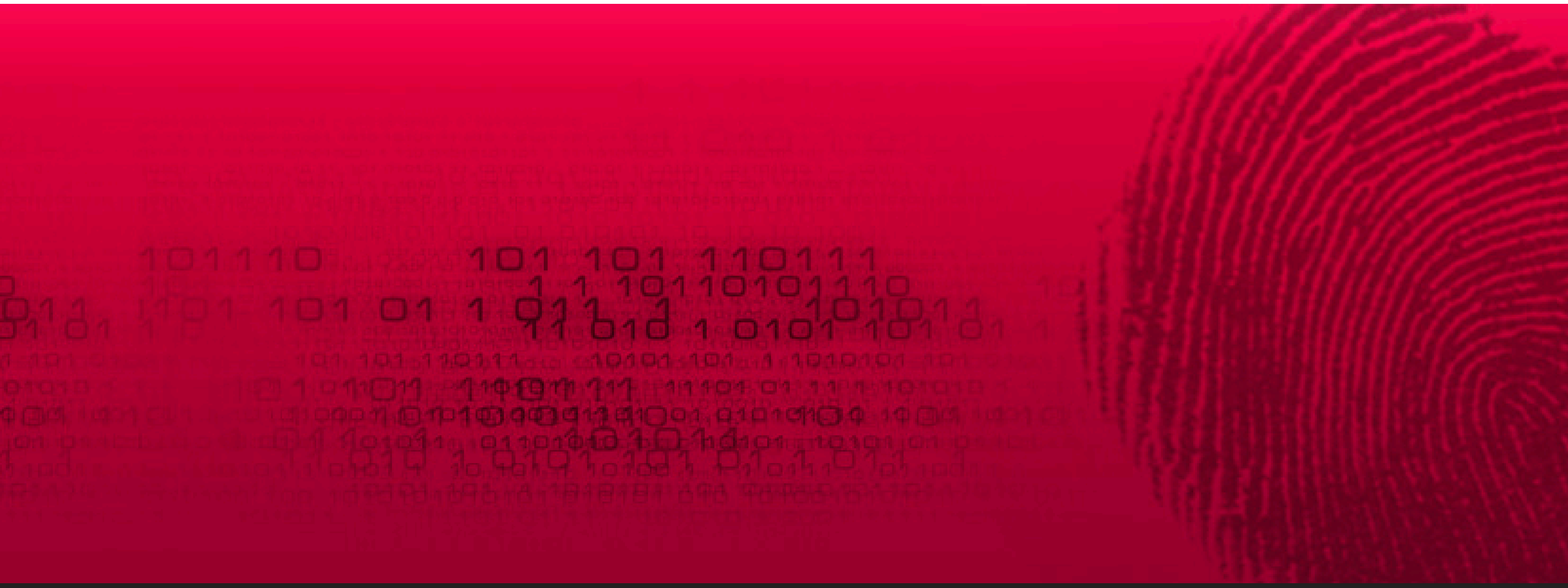
2009 Best Products & Services – Reader's Trust Award
Network Products Guide has awarded Masergy the 2009 Best Products and Services - Readers' Trust Award for Unified Security.

2009 Global Product Excellence - Customer Trust Award
Masergy is a winner of the 2009 Global Product Excellence Customer Trust Award for Integrated Security from Info Security Products Guide.

2009 Product Innovation Award
Masergy's Enterprise UTM++ and All-n-One Security Module for Enterprise UTM have received 2008 and 2009 Product Innovation awards for unified security from Network Products Guide.

2009 'Tomorrow's Technology Today' Award
Masergy is a winner of 2006, 2007, 2008 and 2009 'Tomorrow's Technology Today' awards from Info Security Products Guide.

2009 Best Deployment Scenario Award
Info Security Products Guide has named Masergy a winner of the 2009 Best Deployment Scenario Award for Managed Security Services.



Corporate Headquarters (USA):

2740 North Dallas Parkway, Suite 260, Plano, TX 75093 USA
Phone: +1 (214) 442-5700
Fax: +1 (214) 442-5756

MASERGY

Performance Beyond Expectations