

The Path to Ubiquitous Network and
Information Protection
A Stratecast Partners Excerpt



“Partnering with clients to create innovative growth strategies”

The Path to Ubiquitous Network and Information Protection

Protecting enterprise networks and information is moving to a new stage. Several technical and business developments are demonstrating that the enterprise network perimeter is disappearing and the value of traditional perimeter defenses is no longer sufficient; more is required. At the same time, the penalties for inadequate security are on the rise such that complacency in addressing this heightened risk is unacceptable for enterprises, particularly those with a close correlation between their security trustworthiness and their business objectives. However, equally unacceptable for enterprises is a continuous escalation in security expenditures. Bottom line, enterprises demand new approaches to network and information protection that are highly adaptable and effective in mitigating today's threats and in the evolution of threats in the future. In addition, these same solutions need to support the enterprise's business objectives, not be an obstruction.

For these reasons, a new set of security solutions is beginning to emerge that offer heightened breadth and depth in threat identification, more pervasive enforcement of security decisions throughout the enterprise network (i.e., not just at the perimeter), create operational synergies across multiple security domains, and provide enhanced protection of sensitive enterprise information.

Shown in the next two pages is Stratecast Partners' assessment of Mirage Networks.

Michael Suby
Program Manager, Business Market Strategies
msuby@stratecast.com

Mirage Networks

Focused extensively on protecting the interior of enterprise networks, 4-year old Mirage Networks offers a network-based endpoint control solution named NAC (Network Access Control). Situated out-of-band (i.e., deployed on a switch port), Mirage NAC appliances continuously compare network activity to the behavioral patterns of common attack methods (e.g., threat propagation, bad packets, spoofing, mail-related, and reconnaissance). Rather than rely on signatures to define the threatening or suspicious behavioral patterns, Mirage combines rules that represent 16 types of network communication traits to define these patterns. The company also collects information on assigned and unassigned IP addresses referred to by the company as or dark IPs (i.e., where the communication is coming from and going to) to further augment its detection effectiveness. With this approach Mirage states its solution is more effective (fewer false positives, identifies zero-day attacks) and more efficient (zero added latency) in detecting threatening activity than signature or heuristic-based detection methods.

Once threatening behavior has been detected, NAC will utilize its knowledge of devices on the enterprise network to mitigate threats through the following techniques:

- Attack Deception - misdirect attacks through snaring and virtual decoys, and
- Attack Mitigation - contain threats through surgical quarantining offending devices.

To be noted, all detection and mitigation functions are accomplished without the deployment of endpoint software agents or upgrades to the network infrastructure. The out-of-the-box functionality of NAC appliances have been shown to be effective in identifying and blocking threats in as little as 15 minutes after installation.

In the company's short history, Mirage has gained several prominent customers and OEM relationships. As an OEM partner, Mirage technology is embedded in SBC's (now AT&T) PremierSERV Managed Intrusion Prevention Service (IPS) and in a major network equipment vendor's security appliances. The company reports they now have over 100 customers, over 600 units have been sold, and the number of channel partners, currently over 50, is growing. Mirage's early attention to sales channel through the development of its early 2005 introduction of ChannelFirst Program has been a significant contributor to the company's growth.

Solution Attribute	Description
Breadth and depth in identifying and assessing security threats	<p>With Mirage Networks' focus on identifying internal threats through analysis of suspicious network behaviors, it is not positioned as a comprehensive security solution addressing all forms of attacks (e.g., DDoS) and protecting all points of vulnerability (e.g., unpatched laptop or desktop OS). Nevertheless, the company's dedicated focus on internal threats; the fact that NAC overcomes numerous limitations in perimeter and host-based security solutions; and has zero impact on the enterprise network infrastructure and traffic processing, positions Mirage NAC as a natural and immediate complement to an enterprise's existing and future perimeter and host-based security deployments.</p> <p>This complementary point notwithstanding, the company is actively branching out into additional security arenas. This is most evident with the January 2006 introduction of Mirage's "NAC-in-the-Box" solution, version 3 of Mirage NAC, which adds agentless vulnerability scanning to the previous version. Policy-controlled scanning of devices is conditional, not always on. For example in pre-admission, a scan is initiated when a user is entering a sensitive area of the enterprise network. In a post-admission scenario, a scan is initiated when a violation of a Mirage NAC behavioral rule has occurred. Mirage NAC delivers lightweight scanning and uses integrations with third parties to provide additional in-depth scans as well as patch management and antivirus updates.</p>
Pervasive enforcement of security policy decisions	<p>The deception and mitigation technologies incorporated into Mirage NAC permit enforcement of security policy decisions at a very granular level – on a per device basis. Mirage NAC enforcement is entirely completed within the device itself, not in network infrastructure or on agents deployed on endpoint devices (i.e., laptops, desktops, and servers).</p>
Support synergies across multiple security domains	<p>A technical engagement with McAfee is the most prominent example of cross-domain synergies; other integrations exist with offerings from netForensics, Infoblox and Qualys. Future integrations are in development. All told, these integrations allow the company's NAC solution to collaborate with additional third-parties, providing its customers with network access control plus functionality including:</p> <ul style="list-style-type: none"> • Patch management to reduce remediation time and administration oversight, • Perimeter IPS and firewalls to amend their settings to block incoming attacks detected by Mirage NAC, • Event correlation to provide broader identification of threatening network activity, and • Compliance reporting.

About Stratecast Partners

Stratecast Partners directly assists clients in achieving their objectives by providing critical, objective and accurate strategic insight, in a variety of forms, via an access-and-industry-expertise-based strategic intelligence solution. Stratecast provides communications industry insight superior to a management consultancy, yet priced like a market research firm. Stratecast Partners' product line includes: Monthly Analysis Services [Convergence Strategies & Network Architectures (CSNA), OSS Competitive Strategies (OSSCS), Network Professional Services Strategies (NPSS), Consumer Market Strategies (CMS), and Business Market Strategies (BMS)]. Weekly Analysis Service [Stratecast Partners Insight for Executives (SPIE)], Standalone Research, and Business Strategy Consulting.

About Frost & Sullivan

Frost & Sullivan, a global growth consulting company founded in 1961, partners with clients to create value through innovative growth strategies. The foundation of this partnership approach is our Growth Partnership Services platform, whereby we provide industry research, marketing strategies, consulting and training to our clients to help grow their business. A key benefit that Frost & Sullivan brings to its clients is a global perspective on a broad range of industries, markets, technologies, econometrics, and demographics. With a client list that includes Global 1000 companies, emerging companies, as well as the investment community, Frost & Sullivan has evolved into one of the premier growth consulting companies in the world.