Stratecast A Division of FROST & SULLIVAN

Stratecast Perspectives & Insights for Executives

SPIE 7-26 – July 20, 2007

Laptop's Newest Peripheral: Security on a Stick

Introduction[1]

As enterprises and their information workers embrace mobility as a standard business practice, the enterprise's ***at risk*** level grows in multiple dimensions. Most notably,

- **Data is at risk** – The fluid exchange of data is essential to a growing number of business operations. Data fluidity without sufficient protection and control elevates the risk of data becoming lost, stolen, misused, and compromised. Furthermore, the negative implications to the enterprise of a data breach rise with the sensitivity and non-public nature of the data.
- **Worker productivity is at risk** – Reliability and availability of mobile devices is critical to mobile workers. Cyber infections will compete for device processing and bandwidth capacities. The same contention can occur with mis-configured devices and user abuse (e.g., installation and use of unauthorized applications). Cyber defenses hosted on users' devices (e.g., anti-virus, anti-spam, and IDS) also take a slice of processing and bandwidth capacities. In a worst case scenario, a lost or stolen device places the worker in an out-of-commission state. Regardless of the cause, returning the worker to his/her optimal or previous operating state can be a significantly time-consuming and costly effort.
- **The enterprise network is at risk** – Despite best efforts to protect users' mobile devices from cyber infections, few enterprises would claim that the host protections resident on user devices are as robust in protection as their network perimeter defenses. Furthermore, as these mobile devices connect to the enterprise network, either remotely or when re-docking, there is risk to the enterprise network. In addition, the physical security at enterprise locations, such as ID badges, card readers, and co-worker proximity, represent a layer of defense in controlling access to the enterprise network that is not automatic with mobile and remote workers (i.e., how to validate who they say they are – authentication).
- **The enterprise brand is at risk** – An enterprise's brand is always on display and, at the same time, at risk. A catch-22 situation, worker mobility contributes to business agility and responsiveness. Yet these same business improvements also establish a new bar in customer

---

[1] In preparing this report, Stratecast conducted interviews with representatives of the following companies:

- Alcatel-Lucent – Dor Skuler, General Manager, Mobile Security Solutions, Enterprise Solutions
- SanDisk - Yariv Fishman, Head of Product Management - Enterprise Solutions
- Yoggie Security Systems – Shlomo Touboul, Founder & CEO

Please note that the insights and opinions expressed in this assessment are those of Stratecast and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

and partner expectations that the aforementioned dimensions place at risk. More specifically, information breaches will not only damage the trust relationship between affected parties and the enterprise but also the trust level that non-affected parties associate with the enterprise.

- **Costs are at risk** – Reducing these *at risk* dimensions is not easy or inexpensive. Purchasing and/or licensing security technologies; installation, management, and maintenance of security technologies; and administrative tasks add to the overall cost of reducing risk. Moreover, lack of user transparency in the operation of security is also a cost consideration. Unbalanced focus on reducing risk without consideration of the user impact can be counter-productive, that is, there is less risk but users are productivity-constrained. In the end, the enterprise must weigh the benefits of reducing risk versus the costs.

These ***at risk*** dimensions are not new. The risks associated with mobility began with the first laptop and the advent of electronic tele-working. With increased dependency on laptops over desktops, broadening of wireless access alternatives, miniaturization of removable storage media, and increasing sophistication of cyber threats, the risk level has steadily grown and so has the cost to mitigate this risk.

A new security product category has emerged to address this heightened mobility risk. We will refer to this category as Security on a Stick (SoaS) as a common product attribute is the security technology residing in a separate device that attaches to the user's laptop. There are, however, important variations within this SoaS product category. Similar to other security product categories, especially new ones, there is no one-size-fits-all.

In this bulletin, Stratecast will describe three representative SoaS products and highlight their distinctive attributes, product directions (in part based on Stratecast projections), and go-to-market strategies. The representative vendors and SoaS products include:

- Alcatel-Lucent OmniAccess 3500 Non-stop Laptop Guardian,
- SanDisk® TrustWatch™, and
- Yoggie Security Systems PICO™.

Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian

Although a lengthy product name, it is very descriptive on the security it delivers. Stratecast first covered the Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian (NLG) in June's analysis on Network Access Control (NAC) entitled *"Why Pre-admission Network Access Control is Not THE Solution"* (BMS 2-9), June 2007.[2] The study excerpt that follows provides a basic description of NLG.[3] After the excerpt, we will describe other capabilities of the NLG and Alcatel-Lucent's product direction and go-to-market strategy.

[2] For information on obtaining this full study, please contact Stratecast at 877-463-7678 or inquiries@stratecast.com.

[3] In a NAC scenario, the NLG ensures that the security state of corporate-owned laptops is continuously maintained relative to policy. In this manner, the health checking of a NLG-equipped device upon network connection, remote or in-office docking station, is non-essential. A NAC-initiated health check would merely confirm what is already known about the connecting laptop.

Excerpt

Currently available in a broadband wireless card form factor for laptops, the NLG is a mini-computer equipped with a 3G wireless modem, rechargeable battery, self-contained hardened operating system, and flash memory. This combination of functions can be remotely controlled by IT as an independent staging area to launch several data and device management tasks when the user's laptop boots up, such as:

- automatically establishing VPN connections (no additional VPN client software required),
- operating system patching,
- application software upgrading,
- checking for and correcting non-compliant security defenses,
- conducting over-the-air data backups (can be accomplished when device is powered off), and
- GPS tracking.

In addition, the NLG can serve as a factor in a multi-factor authentication scheme and can be a vault for encryption keys used in hard drive or file encryption.

Since the communication channel and access to and control of the NLG can be reserved to IT organizations, device users cannot interfere or tamper with its operations. Moreover, this solution assists IT departments in standardizing configurations of corporate-owned laptops through broadcasting of configuration changes to all NLG-equipped devices with a single command. Because the NLG has its own processor, battery, and communication channel, conflicts with user-initiated activities are virtually eliminated.

A recently added capability to the NLG is a 1 gigabyte slot for a SD (Secure Digital) Memory Card. Requested by one of Alcatel-Lucent's beta customers in the financial services vertical, the removable storage card insulates stored and encrypted data from the security vulnerabilities that can exist in the laptop's operating system.[4] As previously described, keys used for encryption on the SD Memory Card or the laptop's hard drive are stored and updated on the NLG device. The company's expansion in data leakage protection is consistent with a growing enterprise demand.[5] In addition, we anticipate that Alcatel-Lucent, similar to other SoaS vendors outlined in this report, will continue down the path of enhancing data-at-rest protection. Currently, Alcatel-Lucent utilizes technology from SafeBoot for data-at-rest encryption. NLG's current technology partners also include: PatchLink and Microsoft SMS for patch management, EMC for back-up, and Absolute Software for laptop recovery.

As described previously, the NLG form factor is now a PCIMIA wireless card. We anticipate that as the wireless industry evolves, NLG will follow its trend in having a smaller footprint and eventually

[4] NLG currently supports Windows XP.

[5] See "*Mobile Data Protection Sector Assessment*" (BMS 2-1), January 2007, for additional analysis on data-at-rest protection.

be available as an embedded component.[6] For now, however, the PCIMIA form factor aligns well with the company's go-to-market strategy.

Alcatel-Lucent's primary go-to-market strategy is through wireless carriers. Already announced, Alltel, Sprint-Nextel, and Verizon Wireless are at various stages of business development with Alcatel-Lucent. For each party, there are strategic advantages. For wireless carriers, assisting enterprises in using mobile communication securely lowers adoption barriers. In addition, positioned as an IT tool for managing and maintaining corporate laptops without requiring physical touch, the NLG benefits users (less inconvenience) and IT (improved scalability in servicing laptops and in ensuring standardization) and, as a potential outcome, strengthens the internal enterprise business case to equip more laptops with broadband wireless cards. Correlated with this last point, wireless carriers are hungry for opportunities to deepen their customer relationships by expanding into device management. The independent and plug-in nature of NLG supports this initiative without placing carriers at risk of having to respond to customer helpdesk calls on user device issues with which that they, the carriers, have no involvement. With the NLG, carriers have a clear demarcation on where their management service starts and ends. For Alcatel-Lucent, wireless carriers bring a base of enterprise customers that already have broadband wireless cards in use. With a coordinated and concerted marketing plan by the carriers and Alcatel-Lucent to upgrade these same customers to NLG-enabled wireless cards, Alcatel-Lucent is well position to drive rapid sales growth.

SanDisk TrustWatch

A leading supplier of flash memory storage devices, SanDisk introduced TrustWatch in February 2007. TrustWatch represents a continuation of the company's movement into the enterprise segment with solutions that not only offer mobile, convenient, and high-capacity storage through USB flash drives (UFD) but also support life-cycle management of the stored material. In support of this strategic push into the enterprise segment, the company in November 2006 acquired msystems™ Ltd., a flash storage vendor and creator of mTrust (now called CMC by SanDisk), an enterprise management system for UFDs.[7]

TrustWatch is a solution suite consisting of multiple components that transform UFDs into trusted storage devices and enables secure remote access to enterprise applications.[8] As described by the company, the operations of each TrustWatch component are:

- **TrustWatch Access** – Provides security on the UFD, including password protection. Integrates a secure browser, email client, spyware scanner, Citrix ICA Web client, optional VPN client, and data storage. Also creates an activity log tracking all data moving to and from approved UFDs.

[6] The prospect of embedded security in mobile devices and how this will materialized in the market is outlined in "*Embedded Security in a Wireless World*" (SPIE 7-16), April 2007.

[7] mTrust was introduced by msystems in the second quarter of 2006.

[8] Stratecast believes that a future direction of the TrustWatch solution is in developing and emphasizing premium integration with the company's enterprise version of Cruzer® USB flash drives over non-SanDisk UFDs as this direction drives sales of two of the company's assets: CMC management software and hardware storage technologies. Cruzer Enterprise includes hardware-based encryption.

- **TrustWatch Vault** – Establishes FIPS 140-2 certified encryption on the UFD, sufficient for HIPPA, SOX, and other compliance regulations.
- **TrustWatch Manager** – Offers a browser-based centralized console for IT administrators, allowing them to remotely deploy, update, track, and disable thousands of UFDs.

In addition, TrustWatch in collaboration with several port protection solutions can limit port use to only approved devices, define allowable operations of USB- approved devices, and log all USB activities.

SanDisk followed an ecosystem model in the creation of TrustWatch. For example, TrustWatch was co-developed with RedCannon Security and includes security technologies from several third-party vendors: RSA (authentication), SecureWave (endpoint information leakage), and Safend (endpoint information leakage). In addition to the life-cycle data storage management technology acquired from msystems, the company incorporated home-grown technologies: CruzerSync® (data/file synchronization and back up), TrustedFlash™ (partitioned secure storage), and TrustedSignins™ (one time password) into TrustWatch.

With the compact size, storage capacity (in gigabits), mobility, and universality (plugs into any USB port) of UFDs, TrustWatch supports an enterprise need to permit sensitive data to move with its workers among computing devices of varying trust levels (e.g., from the high trust level of enterprise owned desktop PCs to the low trust level of home PCs and public Internet kiosks) with a heightened level of confidence that the risk of data leakage is addressed and data privacy regulations are satisfied. Combined with the secure access applications integrated into TrustWatch (e.g., secure browser, two-factor authentication, and optional VPN client), these same users can securely access enterprise applications from any device without leaving any trace of user activity on the host device.

Support of secure access from any device (trusted or untrusted) by TrustWatch parallels a key value proposition of SSL VPNs.[9] But, as seen in the early stage of its evolution, SSL VPN could consistently support access only to simple web applications from Internet-connected devices. To expand access to a broader range of applications including highly sophisticated and dynamic web applications, SSL VPN client-side software must run on the host or user device. Depending on the restrictions on the host device to receive and run SSL VPN host software, the range of application access will vary from one host device to another. This SSL VPN limitation presents a business opportunity for SanDisk to develop customized versions of TrustWatch for SSL VPNs. By maintaining the SSL VPN software on a TrustWatch-enabled UFD, users accessing enterprise applications through an SSL VPN gateway can consistently access any application from any host device, trusted or untrusted. In addition, this business opportunity expands the SanDisk sales channel to include the direct sales, resellers, and VARs of SSL VPN products.

A similar business opportunity exists for WAN optimization and application acceleration soft clients. This client software is designed to replicate the WAN optimization and application acceleration technologies and user benefits available in symmetrically deployed premise-based appliances, but on user devices. To avoid the burden or overcome the inability to install the soft client on the

[9] See "*SSL VPN Evolution & Transformation Continues"* (BMS 2-4), April 2005 for Stratecast recent analysis on SSL VPN.

computing and communication devices the user has at his/her disposal, a TrustWatch-enabled UFD could make WAN optimization and application acceleration as universal as UFDs.

These two business opportunities with SSL VPN and WAN optimization vendors follow a similar path as the recently announced co-development agreement with Microsoft.[10] In this agreement, Microsoft will develop software and SanDisk hardware to allow mobile users to carry their Microsoft computing environment, not just files, with them as they move from one Windows XP or Vista device to another. The initial version of this co-developed product is not expected until the second half of 2008. Stratecast anticipates that the business opportunities with SSL VPN and WAN optimization and application acceleration vendors will materialize more quickly.

Yoggie Security Systems PICO

Start-up Yoggie Security Systems has developed two free-standing security solutions that elevate the cyber defenses of laptops such that the level of protection for remote laptops is the same as when these same laptops are inside the enterprise network. The logic of Yoggie's solution is that laptops when remote have only one line of cyber defense consisting of software security applications. Comparatively in an on-network setting, these same laptops are more thoroughly insulated from cyber threats because they have double the defense: (1) integrated hardware and software solutions deployed at the network perimeter, and (2) the security software applications on the user's device.

Yoggie's solution to this "less secure when remote" problem is to place similar multithread network perimeter defenses on a hardened and independent computing device that plugs into a laptop USB port. The company offers two version of this solution: (1) PICO, for single device use, and (2) Gateway, for shared use among multiple devices (e.g., small office and home networks).

As a device operating independent of the user's laptop (own operating system and processor), the PICO and Gateway function as a constant filter and gateway between the user device and the Internet (untrusted network). All traffic to and from the user device and the Internet is processed through the PICO or Gateway. In practice following the installation of Yoggie's Window drivers at first use, users' network connections regardless of type (e.g., WiFi, Ethernet, and Bluetooth) are blocked unless the PICO or Gateway is plugged in.

Focusing on the single device solution PICO, the PICO is a full Linux 520 MHz computer miniaturized to the size of a USB Flash Drive and weighs 18 grams. The security applications that operate within the PICO environment currently include:

- URL filtering, parental controls,
- Anti-SPAM,
- Anti-phishing,
- Anti-spyware,
- Anti-virus,

[10] See the joint press release by Microsoft and SanDisk entitled "Microsoft and SanDisk Join Forces to Create New Experience for USB Flash Drives and Flash Memory Cards" posted on May 11, 2007.

- L8 and MLA agents,
- HTTP, FTP, SMTP, and POP3 proxies,
- IPS/IDS,
- VPN, and
- Firewall.

Updates to policies, rules, and signatures are securely, automatically, and transparently to the user fetched by the PICO every five minutes.

Because risk level of a laptop is dynamic based on user activity (e.g., web sites visited) and emails received, PICO has the ability to assess the changing risk level and modify security policy settings automatically. This is accomplished with Yoggie's patented pending Adaptive Security™.

The PICO is offered in two models, Personal for consumers and PRO for businesses. Retail list price is $179 for Personal and $199 for PRO for the first year subscription (includes updates). In subsequently years, the annual subscription fee is $30 and $40, respectively. The Yoggie Management Server (an appliance) has a list price of $5,000.

As a young start-up, sales distribution is in a formative state. Online sales now and retail stores starting this summer is how the company will reach consumers. Security distributors, resellers, and VARs are used to reach enterprise buyers.

The PICO is an innovative example of computer miniaturization. And through this miniaturization, PICO users gain a one-two punch of improved cyber threat protection and the reclaiming of laptop processing capacity for other applications running on their laptops. These benefits notwithstanding, we view Yoggie as more challenged to succeed in the SoaS market than Alcatel-Lucent and SanDisk. Certainly, the size, industry relationships, brands, existing sales channels and customer bases, and financial backing of these two companies far exceed those of a start-up. From a product comparison, Yoggie PICO and Gatekeeper do not currently support data-at-rest protection, a prominent capability of Alcatel-Lucent NLG and SanDisk Trustwatch and a growing enterprise need. Last, there are other approaches to strengthening cyber threat defense for laptops when operating outside perimeter defenses. Network-based security services as offered by Network Service Providers (e.g., AT&T and Verizon) and Internet access aggregators (e.g., iPass) are alternatives to PICO and Gateway. Yet, PICO's range of security applications is significant and the PICO price is highly competitive to the prices for network-based security services and even the cost of purchasing and subscribing to host-based security software.

Stratecast
The Last Word

SoaS (Security on a Stick) presents enterprises with a new alternative to addressing the growing problem of protecting their mobile assets – worker productivity, devices, and information. In addition, SoaS solutions highlight the potential and advantages of driving security technologies and non-security technologies (e.g., WAN optimization and application acceleration) down to the device level without having to engage directly in the device environment. This separation from the device environment serves to accelerate SoaS product development cycles (e.g., less compatibility testing with operating systems and their versions), reclaiming of laptop processing, and reducing contention between IT desktop support and enterprise security organizations as each will have their own environment to operate in.

These favorable attributes notwithstanding, long-term market success for SoaS products in our view will follow those vendors that can:

- **Go long in capabilities** – Successful SoaS product must be comprehensive in security applications. Partial solutions that require the enterprise to combine solutions from multiple suppliers add to IT cost and complexity and contribute to gaps in security.
- **Deliver administrative ease-of-use** – Easy to want but hard to deliver especially with SoaS products that are an ecosystem of technologies from several suppliers, as most will be. In addition, intuitive, comprehensive, and flexible alerting and reporting capabilities are critical as substantiation of regulatory, industry, and company policy compliance is a growing enterprise need.
- **Support scalability, platform extensibility, and form factor diversity** – The number and diversity of mobile devices (not just laptops but also smartphones) will continue to increase. SoaS products with high levels of device scalability and platform support will win over solutions that are not as broad. In addition, offering the SoaS solution in multiple form factors (e.g., USB plug-in versus a laptop component installed during order fulfillment) will serve to expand market potential.
- **Guarantee user transparency** – Users are a forceful constituent base that, on average, is more concerned about how well their mobile devices serve their needs and preferences than security. If SoaS is not user transparent in its operations, users will protest and slow adoption.

Michael Suby

Research Program Director

Stratecast (a Division of Frost & Sullivan)

msuby@stratecast.com

About Stratecast

Stratecast 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's 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 Perspectives and 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.

CONTACT US

For more information, visit www.stratecast.com, dial 877-463-7678, or email inquiries@stratecast.com.