

The Array SPX Series provides a complete End-Point Security solution that integrates the Symantec On-Demand Agent (SODA) to prevent the compromise of corporate data (such as company financials, customer information and intellectual property) caused by network access through public and unmanaged devices including kiosks, home computers and guest laptops.

■ Data-Leakage Prevention

The Array End-Point Security solution (with integrated SODA software) mitigates possible resource exposure by delivering an on-demand agent (does not require pre-installation) that adapts its policies to suit changing environments.

For instance, administrators can define host-checking security policies that adapt specifically to managed and unmanaged devices. Should the on-demand agent detect a company-issued device, the user is provided with the full range of resources for which he or she is authorized; should the same user connect over a personal laptop, kiosk or public

workstation, he or she may be provided with a subset of authorized resources depending on the security environment of the unmanaged device (virus scan, personal firewall, etc.). In the instance of connections from unmanaged devices, cache cleaning may be enabled to wipe devices of sensitive data at the end of a session, or secure desktop may be implemented for a further level of security - creating a fully secure sandbox in which local actions are locked down.

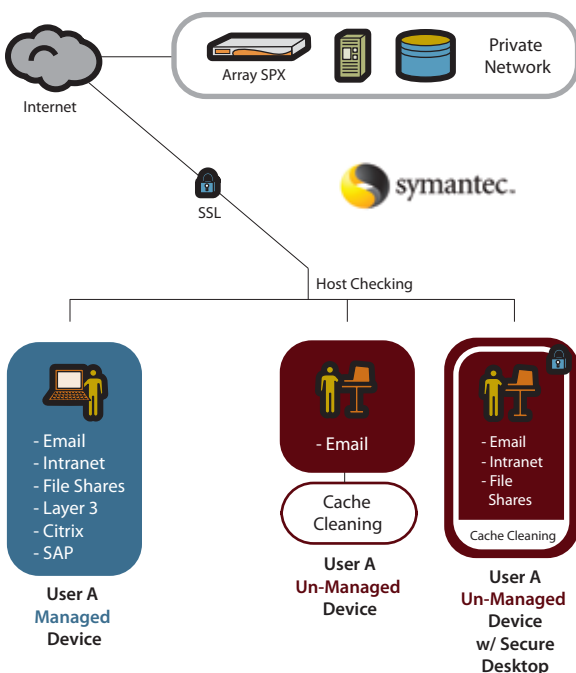
■ Integrated Management

Symantec On-Demand Agent software is fully integrated with Array SPX Series platforms - with configuration performed from the SPX WebUI in a series of carefully-designed and

SODA End-Point Highlights

- **Determines the identity and health of client devices** prior to authentication and network admission
- **Comprehensive scan including anti-virus, personal firewalls, service packs, patches, certificates and MAC addresses**
- **Denies admission or provides limited access based** on client security posture and access environment
- **Completely erases browser cache upon session termination** ensuring sensitive data does not remain on public or un-managed devices
- **Optional secure desktop virtualizes entire session in an encrypted vault** eliminating potential for data leakage
- **Symantec On-Demand Agent (SODA)**

■ How It Works



■ Array End-Point Security Features

Host Checking – prevents corporate networks and data from being compromised by non-compliant unmanaged devices. The Host Checking module verifies that unmanaged devices accessing confidential data are secured by antivirus software with updated virus definitions, anti-spyware, personal firewalls, critical service packs, and patches. Array Network's subscription service ensures that host integrity rules are updated with the latest pre-configured security checks.

Adaptive Policies – ensures that the appropriate policy is applied to users accessing networks and data. The Array On-Demand Agent has the ability to adapt security policies based on identification of the specific network locations and the type of network device (managed vs. unmanaged) to ensure that all confidential data is protected without affecting the productivity of the user. For example, a compliant corporate laptop accessing Webmail would not be required to download the Secure Desktop because their computer is secure, while a sales person accessing that same Webmail server would have a Secure Desktop downloaded automatically to protect the session in that dangerous environment.

Cache Cleaner – ensures that Web browser information, such as cookies, history, auto-complete, stored passwords, and temporary files, are erased or removed upon termination of the session, inactivity timeout, or closing of the browser. Cache Cleaner works either by itself for all supported operating systems or in conjunction with Secure Desktop to clean the browser cache on additional operating systems such as Mac OS X, Linux, and Windows (98,ME), or as a standalone module.

Secure Desktop – protects confidential data by creating an environment that secures all data involved in the network session by virtualizing the desktop, file system, registry, printing, saving to removable media and network drives, and copy/paste functions. All data is encrypted on the fly and optionally erased upon session termination. The Secure Desktop can be configured to allow users to switch between the normal desktop and Secure Desktop, as well as remain persistent on the unmanaged device between sessions with a password.

On-Demand Agent – is delivered at the time of network connection from Array's SPX series of SSL VPN Gateways: the SPX 1800, 2800, 4800, 5800 and 6800. On-Demand Agent is delivered using a lightweight Java-based delivery mechanism that ranges in size between 250-500K and can install without administrative rights, Active X disabled, and browser security on high. On-Demand Agent's lightweight and universal delivery enables widespread usage across multiple operating systems and Web browsers, on slow connections, and on locked down devices.