Lancope.
### Network Performance + Security Monitoring™

WHAT'S NEW IN STEALTHWATCH® SYSTEM 6.2

Lancope's StealthWatch® System unifies security and network performance monitoring to provide end-to-end visibility for dramatically improved network troubleshooting and risk posture. By conducting sophisticated behavioral analysis on flow data from existing infrastructure, the system cost-effectively enhances network security and performance across physical and virtual environments.

StealthWatch 6.2 includes a wide range of new features designed to help customers embrace next-generation technologies, and address increasing infrastructure demands resulting from trends such as IT consumerization, bring-your-own-device (BYOD), virtualization and rapidly-evolving cyber attacks.

Highlights

- Integration with the Cisco Identity Services Engine (ISE) for Enhanced Mobile Security and Identity Awareness
- New Virtual Deployment Options
- Advanced Application Monitoring
- Integration with Palo Alto Networks' Enterprise Firewall
- Support for IPFIX
- New FIPS Capabilities
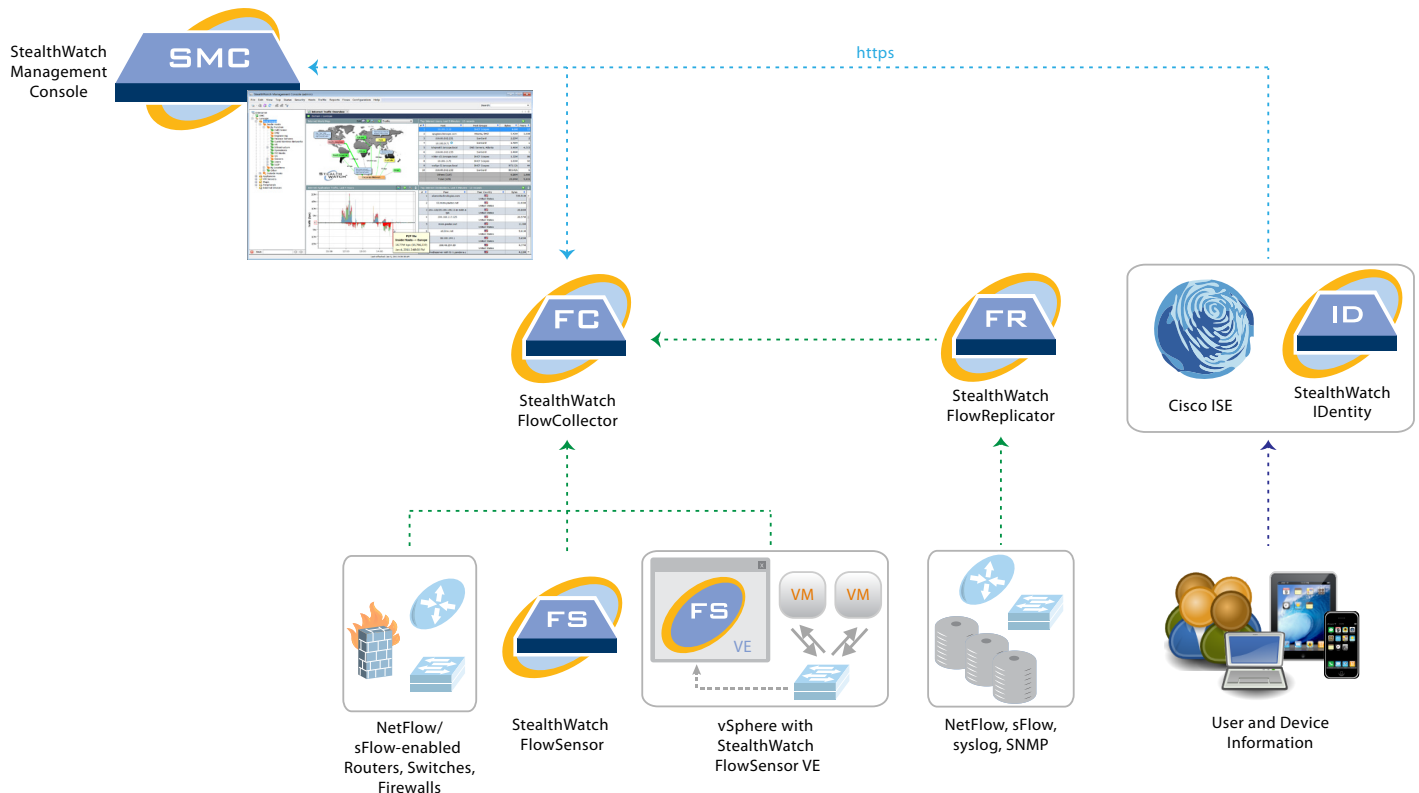
StealthWatch 6.2 enables customers to continue embracing next-generation technologies to address emerging trends.

Integration with the Cisco Identity Services Engine (ISE)

In the wake of IT consumerization and BYOD environments, the network perimeter has vanished. Today's enterprises require a more effective, seamless means of monitoring and controlling users' access to the network and sensitive resources. StealthWatch version 6.2 now integrates with the Cisco Identity Services Engine (ISE) to extend critical network visibility and security across the internal and external network.

Cisco's ISE is a next-generation network admission control system built on the 802.1x standard, which provides customized access to corporate resources based on user/endpoint identity. It is a key element of Cisco's SecureX context-based security architecture for Borderless Networks, and Cisco's TrustSec solution for intelligent access control. The ISE adds to the identity data available for analysis through StealthWatch, including valuable information on the types of devices being used to obtain network access, and where the device is physically located on the network.

| Start Active Time	Alarm	Source	Source User Name	Source Device Type	Details
Dec 9, 2011 3:28:00 PM (1 day 18 hours 3 minutes ago)	Host Lock Violation	10.201.	Bob. Smith	Apple-iPhone	Rule #8 Botnet Communications Source Host is using http (80/tcp) as client to 208.73. (Double–click for details)
Dec 9, 2011 3:30:00 PM (1 day 18 hours 1 minute ago)	Suspect Data Loss	10.201.	John. Doe	Microsoft-Workstation	Observed 131.68M bytes. Expected 14.28M bytes, tolerance of 50 allows up to 81.64M bytes.

Integration with Cisco's ISE increases the amount and types of identity data available for analysis through StealthWatch.

Through integration with StealthWatch, Cisco ISE users can expand their security and compliance strategies by continuously monitoring user behavior on the network. StealthWatch aggregates identity data from the ISE with key network and security data from flow-enabled devices to deliver a single, comprehensive view into network activity for more effective troubleshooting.

Mobile Device Security for BYOD Environments

According to data from Aberdeen, 75 percent of companies currently allow employee-owned smartphones and/or tablets to be used at work.[1] Meanwhile, Gartner has predicted that 90 percent of organizations will support corporate applications on personal devices by 2014.[2] BYOD has significant productivity, convenience and cost benefits, but it is leading to serious challenges for IT administrators.

Unfortunately, mobile users often circumvent corporate security policies and safeguards, and it is too cumbersome – and often impossible – to install and manage security software on every new device. StealthWatch solves this problem by delivering in-depth internal security monitoring that proactively detects issues stemming from any device on the network, without having to install additional software or deploy expensive probes.
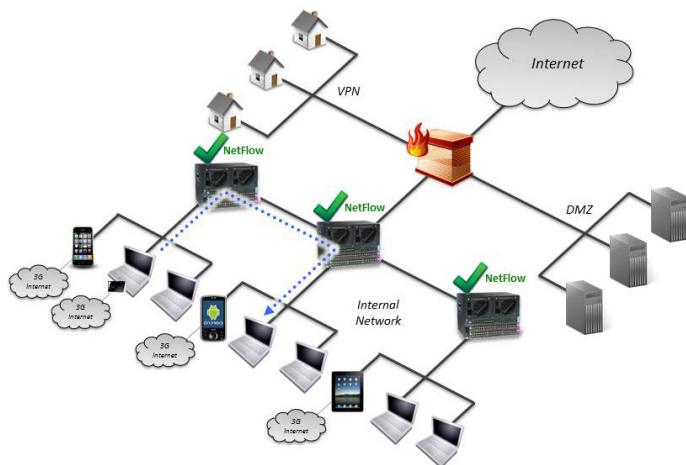
Increasingly complex enterprise networks demand a higher level of mobile security.

1 – ZDNet, "75% of Enterprises Have 'Bring Your Own Device' Policies. What That Means," March 29, 2011, http://www.zdnet.com/blog/sybase/75-of-enterprises-have-bring-your-own-device-policies-what-that-means-charts/1025
2 – Gartner, "Gartner Reveals Top Predictions for IT Organizations and Users for 2011 and Beyond," November 30, 2010, http://www.gartner.com/it/page.jsp?id=1480514

By integrating with the ISE, StealthWatch can now incorporate additional device and identity data from Cisco into its overall view of network activity to further advance mobile security. With mobile devices set to outship personal computers by more than 2 to 1 in 2012, all enterprises must now develop a solid mobile strategy in order to survive.[3]

Advanced Identity Awareness

With the growing complexity of enterprise networks, it is getting increasingly difficult for IT administrators to efficiently mitigate issues. One capability that can enhance network and security troubleshooting is identity data. Since 2006, Lancope has offered the StealthWatch IDentity™ appliance to help organizations track the root cause of security and performance issues all the way down to the exact user responsible.

Through integration with the ISE, Lancope leverages Cisco's identity-aware infrastructure to expand upon the user data available for analysis in StealthWatch. With advanced identity data, administrators can more easily address issues without negatively impacting high-level users or traffic.

New Virtual Deployment Options

StealthWatch 6.2 introduces new virtualized deployment options for the StealthWatch Management Console (SMC) and StealthWatch FlowCollector, enabling users to further embrace the movement towards cloud computing. By virtualizing more components of the StealthWatch platform, Lancope allows for the monitoring of both physical and virtual infrastructure using virtual appliances.

Virtualization delivers many benefits, including but not limited to:

▶ lower hardware, maintenance and energy costs

▶ recovered data center floor space

▶ higher availability

▶ reduced disaster recovery costs

▶ faster server deployments

▶ optimized server capacity

Enhanced Application Monitoring

Version 6.2 also advances application performance monitoring by providing URL information in flow records generated by the StealthWatch FlowSensor. URL data, which has previously been unavailable from most flow sources, enables administrators to differentiate between applications to more easily determine which ones are causing performance or security problems. Users can now identify both the hostname of the server, as well as any error messages within the flow, to further aid troubleshooting and forensic investigations.

Client Host ⇅	Client Host Groups ⇅	Client Application Det... ⇅	Server Host ⇅	Server Host Groups ⇅	RTT... ⇅	SRT... ⇅
10.201.	Desktops, VLAN201, Los Angeles	GET http://na3.salesforce.com/00Q5000000ZSz11	204.14.	Salesforce, United States	19ms	2086ms
10.201.	Desktops, VLAN201, Los Angeles	GET http://www.salesforce.com/	204.14.	Salesforce, United States	18ms	85ms

New URL data from StealthWatch helps distinguish which applications are causing security or performance issues.

---

3 – IDC, "IDC Predictions 2012: Competing for 2020," December 2011, http://www.idgglobalsolutions.com/think-tech/idg-knowledge-hub/idc-top-10-2012-predictions

Intelligence from Palo Alto Networks' Enterprise Firewall

In StealthWatch 6.1, Lancope introduced the ability to combine internal and external monitoring by extending behavioral-based flow analysis to data from perimeter devices such as firewalls. In addition to collecting and analyzing flow data from the Cisco ASA 5500 Series, StealthWatch 6.2 now also consumes data from Palo Alto Networks' Next-Generation Enterprise Firewalls. By incorporating analysis of external flow data with intelligence from the internal network, StealthWatch increases the contextual awareness needed to combat today's advanced threats.

Support for IPFIX

Lancope continues to embrace advanced flow data protocols to enhance the analysis capabilities of StealthWatch. Version 6.2 incorporates new support for IPFIX, a standardized flow protocol built on NetFlow v9 that features variable length fields as well as several other upgrades. As flow data protocols continue to progress, Lancope will remain dedicated to expanding its support to include next-generation data for advanced usages.

FIPS Capabilities

FIPS 140-2 Inside

Federal Information Processing Standards (FIPS) are U.S. computer security standards developed to protect information transmitted by government agencies and contractors. Lancope now provides FIPS capabilities for inter-device communication to help government entities preserve the confidentiality and integrity of data collected and analyzed by the StealthWatch System. StealthWatch 6.2 supports FIPS 140-2 by using RSA BSAFE Crypto-J, a validated FIPS 140-2 cryptographic module.*

To learn more or request a demo, contact sales@lancope.com.

About Lancope, Inc.

Lancope®, Inc. is a leading provider of flow-based monitoring to ensure high-performing and secure networks for global enterprises. Unifying critical network performance and security information for borderless network visibility, Lancope provides actionable insight that reduces the time between problem identification and resolution. Enterprises rely on Lancope to make better network decisions, respond faster to network problem areas and avoid costly outages and downtime — at a fraction of the cost of conventional network monitoring solutions.

Lancope Headquarters

3650 Brookside Parkway
Suite 400
Alpharetta, GA 30022

U.S. Sales
+1.770.225.6500
888.419.1462

International Sales
+44 (0)560 344 8075

Website: www.lancope.com
E-mail: sales@lancope.com

DSV802162012

*RSA BSAFE Crypto-J provides FIPS 140 security level 1 overall, level 2 for roles, services and authentication, and level 3 for design assurance for a connected device configuration (CDC) only.