In today’s technology environment, advanced persistent threats (APTs) and other sophisticated attacks are overpowering traditional security tools. Trends like IT consumerization, globalization and virtualization are diminishing the network perimeter, while cyber criminals are becoming more skilled and stealthy. At the same time, IT teams are having to do more with fewer resources. Technologies including SIEM, AV, firewalls and IDS/IPS still play a valuable role in enterprise architecture. However, additional network visibility is now required to efficiently combat the full realm of advanced threats facing today’s organizations. More and more, the worlds of network operations and security operations are colliding, and security teams are benefiting from having access to both types of data to improve contextual awareness.

StealthWatch Provides End-to-End Visibility for Advanced Network and Security Monitoring

Lancope’s StealthWatch® flow-based monitoring solution delivers complete, real-time visibility into all hosts and traffic on the network, providing actionable insight for addressing a wide variety of network and security issues. StealthWatch leverages NetFlow and other flow data from existing routers and switches to cost-effectively unify security, network and application performance monitoring for more comprehensive protection and less downtime.

The system enables IT teams to quickly pinpoint the root cause of issues all the way down to the exact application and user – dramatically reducing the time from problem onset to resolution. StealthWatch is scalable to meet the needs of even the largest networks, and can also monitor and protect virtual environments.

Key Capabilities of StealthWatch

- **Flow-based monitoring** for continuous, comprehensive visibility across the internal and external network
- **Behavioral-based anomaly detection** for fast troubleshooting of APTs and other attacks without requiring signature updates
- **Automatic threat prioritization and mitigation** for expedited incident response
- **Application awareness** to quickly pinpoint application issues and ensure secure, reliable delivery
- **Identity awareness** to uncover users responsible for, and affected by, network and security issues
- **Network forensic data** for conducting incident investigations
- **Advanced reporting capabilities** to enable users to retrieve the exact information and level of detail required
- **Massive scalability** to meet the needs of even the largest networks
StealthWatch and SIEM

SIEM (Security Information and Event Management) tools record and report on security incidents that take place on the network by aggregating log information from a variety of sources. The value of SIEM data, however, is reliant upon the technologies from which it is collected, typically including AV, firewall and IDS/IPS systems. While these systems do provide valuable data surrounding specific security events, they lack the 24/7 visibility and network performance statistics provided by flow-based technologies like StealthWatch.

Based on behavioral analysis versus signature updates, StealthWatch detects advanced persistent threats and other zero-day attacks that bypass perimeter defenses, as well as insider threats such as network misuse, unauthorized access, device misconfigurations and data leakage. In addition to providing in-depth intelligence on the internal network, StealthWatch can also conduct behavioral analytics on data from perimeter devices such as firewalls, delivering even greater situational awareness. StealthWatch also provides functionality for automated threat prioritization and mitigation for more effective troubleshooting.

By augmenting traditional sources of SIEM data with flow-based information, administrators can see deeper into the network, reducing the cost and complexity of incident resolution and improving overall security measures. In addition, StealthWatch goes above and beyond these security capabilities to:

1) support compliance initiatives,
2) enhance network forensics for incident investigation, and
3) significantly improve network and application availability and performance.
## Customer Use Cases - NetFlow and SIEM

### Enhanced network visibility

A stock exchange in Asia is utilizing StealthWatch alongside its SIEM. StealthWatch data is accessed from the SIEM via an API to provide greater context surrounding events than can be achieved with traditional security tools. With SIEM and NetFlow, this organization has achieved enhanced network visibility, an improved security posture, greater network performance and better troubleshooting and forensics capabilities to support its high volume of financial transactions.

### Protection against advanced persistent threats (APTs)

As a highly sensitive and targeted entity, a U.S. federal government organization knew it needed more than just traditional network and security tools to adequately safeguard its infrastructure from advanced persistent threats. The organization therefore uses StealthWatch in correlation with its SIEM to obtain more comprehensive visibility into network traffic. This deeper level of visibility enables administrators to fully qualify and better respond to security events, streamline incident response and improve forensic investigation.

### Situational & contextual awareness

A large pharmaceutical company turned to StealthWatch to supplement its SIEM and fill in the missing pieces of its network audit trail. To achieve 100% visibility, the company enhances its SIEM deployment with flow data from StealthWatch, which is available 24/7/365 from routers and switches, providing an end-to-end account of all communications on the network even in the absence of other log data.

### Streamlined network & security operations

A powerful player in the nuclear power industry sought a means of intuitively viewing network traffic in real time to improve both security and network operations. The company implemented StealthWatch to obtain 100% visibility across its entire network without requiring signatures. StealthWatch data is sent to the company's SIEM along with information from other sources, enabling the organization to easily baseline traffic and trigger alerts on behavioral changes, as well as obtain simple access to all flow logs for forensic analysis.

### Better network forensics

A high-profile media and entertainment company sought the ability to see which services and applications were traversing its network, and also needed a cost-effective tool to assist with network forensics. By deploying StealthWatch in addition to its SIEM, the company has obtained round-the-clock, end-to-end network visibility, reducing the time from problem onset to resolution for both network performance and security issues.

---

To learn more or request a demo, contact [sales@lancope.com](mailto:sales@lancope.com).