

# Network and Application Deep Flow Monitoring

## Deep-Dive

### Analysis

Take a deep-dive into packet flows to assess network performance and understand specific applications transactions.

## Packet-Level

### Forensics

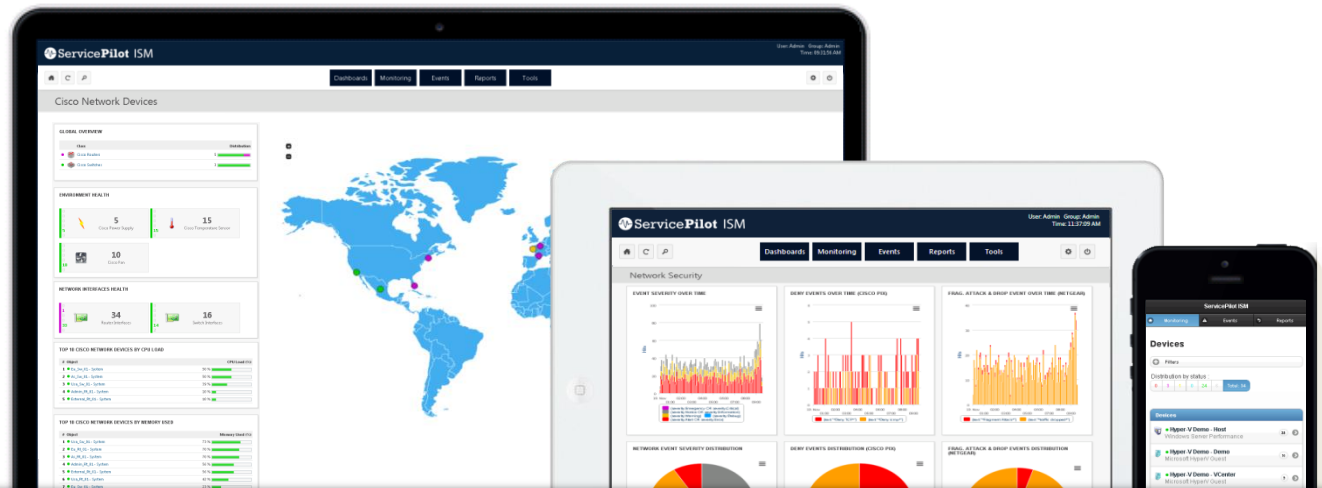
Get a deep-packet visibility and a detailed historical retro-analysis to resolve service delivery and security problems.

## Security

### Enhancement

Make sure that security corporate policies are respected at every level and leverage the effectiveness of your existing security tools.

Resiliency  
Robustness  
Reliability



Contact Us

Americas: +1 (954) 446-9010

Europe: +33 2 40 60 13 30

[www.servicepilot.com](http://www.servicepilot.com)

## Network and Application Deep Flow Monitoring

### Windows, Linux/Unix & IBM z/OS Servers

#### Remote Packet Capture

- Collect, store and decode packets from your servers and rapidly identify network performance issues by analyzing the response time of all active applications.
- Get a total visibility into server events to understand security alerts

#### Network Software Probe

- Collect, store and decode packet data that has been transferred over the network from any source and to any destination.

### Quality of Service

- Get full control over the corporate bandwidth, and make sure that key applications get bandwidth in priority over undesirable applications

### Scalability

- Our powerful software probe can monitor up to 5Gb/s and 96.000 sessions. This will allow you to handle and index massive data volumes generated by your IT systems and infrastructure from any location, source and format.

### NetFlow Software Probe

- Collect and analyze data from continuous flows of network traffic and get operational charts and tables that show precisely who uses the corporate network, how and for what purpose.

### Application Identification

- Detect applications running on standard or non-standard ports and identify the application and protocol behind an IP flow thanks to our Deep Packet Inspection technology.

### Search & Report

- Benefit from our NoSQL advanced search engine and convert the results of your queries into easy-to-interpret PDF reports which will give you a clear and complete view of network and application performance.

### Alerting

- Set alerts to identify when thresholds are exceeded. Rules can be established to trigger automated actions in response to certain conditions, such as sending traps ,Syslog and email notifications.

### Metadata Extraction

- Go beyond application identification and extract application metadata to get a full understanding of network transactions and user behavior.

### Statistics

- Extract crucial statistics embedded in metadata such as the volume of traffic per application and per user, application performance, identifiers to implement security rules and content inspection.

### Check out our other solutions for VoIP, network, server, applications and databases

- Routers, Switches, Firewalls, Load Balancers, Wi-Fi Access Points
- VoIP monitoring with all the associated infrastructure (trunks, gateways, etc.)
- Servers: Windows, \*Nix, IBM, Cisco UCS
- Virtualization: VMware vCenter, VMware ESX/ESXi, Microsoft Hyper-V
- Applications: DHCP, DNS, Web, TCP, Microsoft Active Directory, Microsoft Exchange, IBM Lotus Domino, BlackBerry
- Databases: SQL, MySQL, Oracle SQL, Microsoft SQL Server, PostgreSQL