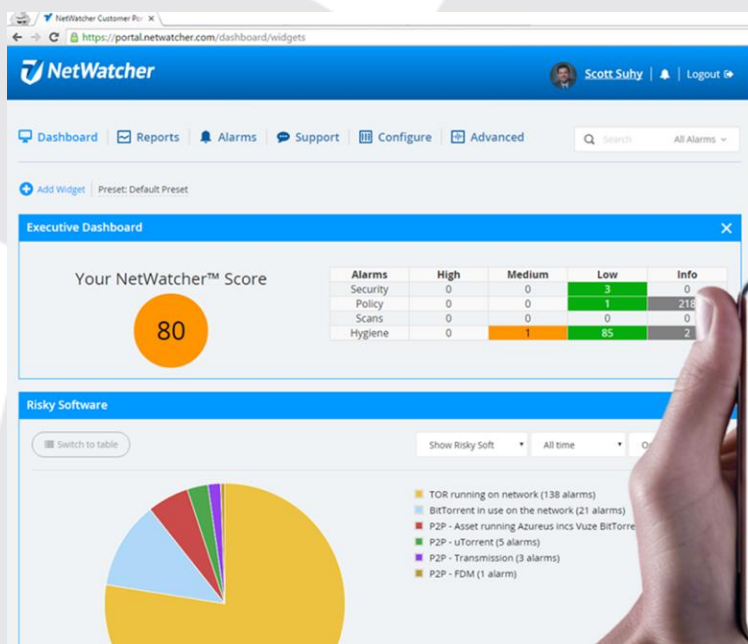


Using NetWatcher for Situational Awareness of your Networks Security

What is NetWatcher?

NetWatcher is a Security-as-a-Service platform that enables customers to have a cost-effective 24 x 7 security service monitoring their networks for vulnerabilities and exploits. Many government and industry compliance requirements, and security best practices, outline the need for continuous monitoring, intrusion detection, active scanning, log monitoring, net-flow analysis, event management and endpoint integration. NetWatcher enables customers to immediately deploy these services and take advantage of a fully-staffed Security Operations Center (SOC). This means superior security that is easy to use, accurate and affordable.

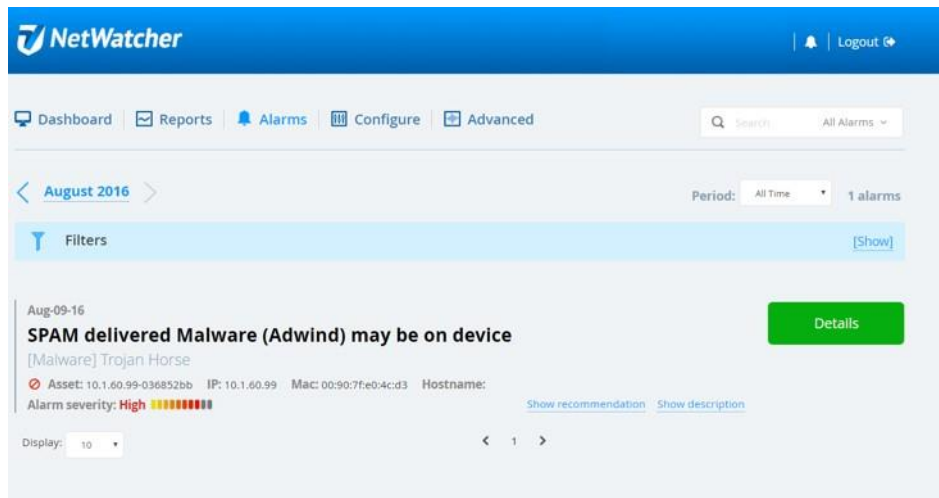
Your Network Security Health Score



One of NetWatcher's powerful features is its ability to devise a numerical score that gives a quick sense of how many issues you need to deal with today!

Monitoring for Exploits

NetWatcher will immediately warn you of an exploit via email, text message or via reports (depending on how you configure alerting). The service will explain the issue to you in easy to understand language, tell you what asset has been exploited, how serious the issue is and what to do about the issue.



Monitoring your Security Hygiene

What is security hygiene? It is essentially how well you are managing your network security and the activities your employees are doing on a day to day basis that may compromise the security of your network, opening your company/agency up to exploit.

Employees Activities

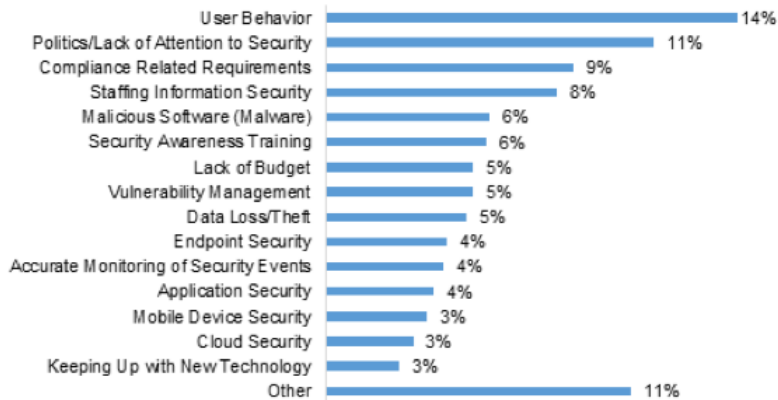
Most exploits occur due to non-malicious users letting bad actors into the enterprise unknowingly... The security industry calls this the *Unintentional Insider Threat* problem ([more here](#)).

Some examples are:

- Employees running old vulnerable software such as Flash or Java versions that are littered with exploitable problems. ([here](#) is a good article on what the FTC thinks of Java). [Here](#) is another example how an old version of Flash might exploit the enterprise.
- Employees running risky software such as BitTorrent and Tor.
- Employees sending Personally Identifiable Information (PII) data such as passwords or credit card numbers over the internet in clear text.
- Employees going to nefarious websites. Employees clicking on phishing messages.

Top Internal Security Pain Points

What do you consider your top internal information security pain point within your organization for the last 90 days?



As you can see from the latest 451 Research study User Behavior is the leading internal IT security pain point.



With NetWatcher each week by default (configurable) all users get an email with the security posture of the network. The email has the widget, seen in figure 1, that provides you a score (out of 100, normalized over the number of assets on the network), and how many violations have resulted in open alarms, of various priorities, over the last 2 weeks. Executives like this email because it can tell them very quickly if their score is going up or down and what is driving the score in one direction or the other. They can also click on each item in the grid to see the exact issue and what user/asset on the network is causing the potential risk.



If you navigate over to the NetWatcher dashboard you can also install many widgets like the two you see in figure 2 related to the number of users running risky software or vulnerable software.

It's important to deal with these hygiene issues as they arise. You can either:

1. Upgrade the software if necessary
2. Remove the software if it is too risky
3. Train the user on why the activity or software they are using exposes them and the company to exploit
4. Update employee policy documents to include what a user can and cannot do on the network
5. Block the software at the firewall/router &/or use web gateways to block the users for visiting bad sites &/or use email phishing services to force users to be smart about what they are clicking

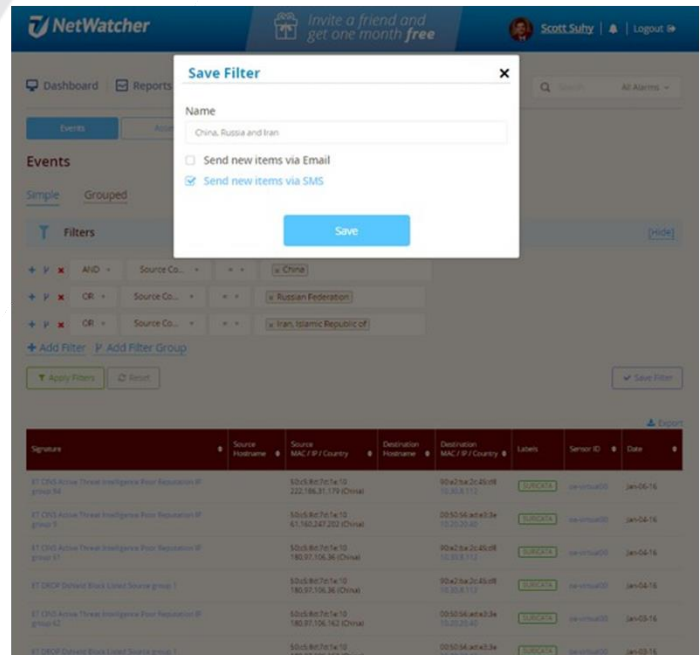
Network Security



You also want to keep an eye on what's getting through your firewall, especially from countries like Iran, China and Russia. With NetWatcher, one of the widgets we provide is to show you all the countries that have triggered anomalous events once they made it through the firewall. If you click on any country in the widget in figure 3 you will be taken to the corresponding events and can review all the detail including downloading the 'pcap' or look at related events by the hour or day that occurred on the same asset allowing you to see if the bad actor may be migrating.

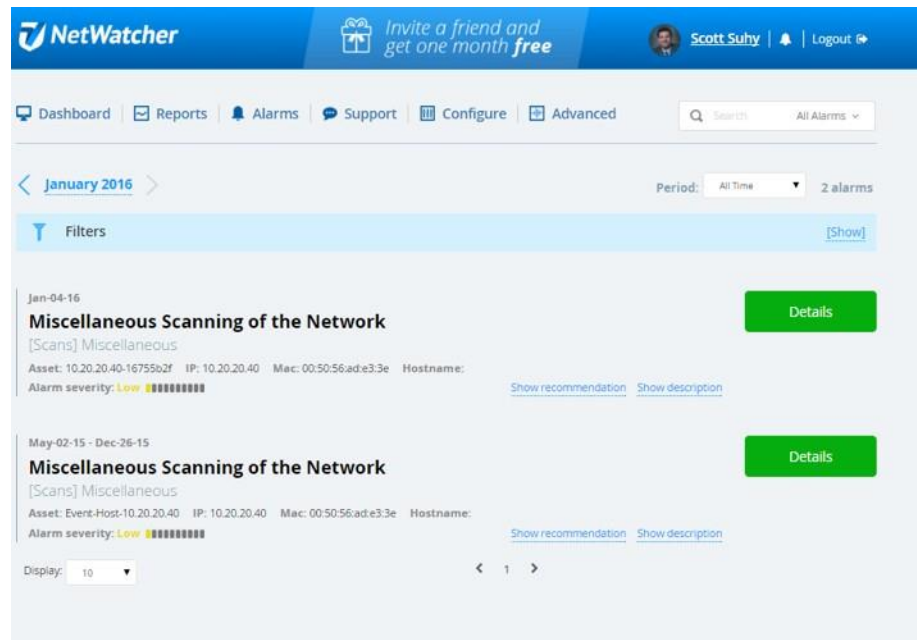
You can even set "Trip Wires" to send you an SMS message if one of these events (or any other event for that matter) occurs.

For example, here is a SMS trip wire set for any event from China, Iran or Russia.



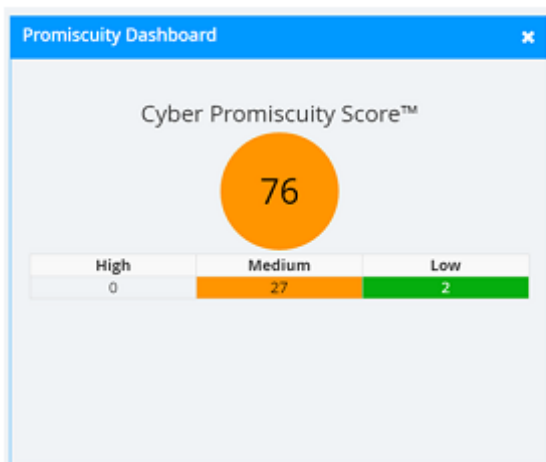
Signature	Source Hostname	Source MAC / IP / Country	Destination Hostname	Destination MAC / IP / Country	Labels	Server ID	Date
ET DNS Active Threat Intelligence Feed Response IP group 14	82.42.194.21	222.186.21.175 China	82.42.194.21	10.20.2.1	Malware	netwatch02	Jan-05-16
ET DNS Active Threat Intelligence Feed Response IP group 15	82.42.194.21	82.180.247.202 China	20.50.56.100	10.20.2.40	Malware	netwatch02	Jan-05-16
ET DNS Active Threat Intelligence Feed Response IP group 17	82.42.194.21	180.87.106.36 China	82.42.194.21	10.20.2.1	Malware	netwatch02	Jan-05-16
ET DROP Default Block Listed Source group 1	82.42.194.21	180.87.106.36 China	82.42.194.21	10.20.2.1	Malware	netwatch02	Jan-05-16
ET DNS Active Threat Intelligence Feed Response IP group 12	82.42.194.21	180.87.106.162 China	20.50.56.100	10.20.2.40	Malware	netwatch02	Jan-05-16
ET DROP Default Block Listed Source group 1	82.42.194.21	180.87.106.162 China	20.50.56.100	10.20.2.40	Malware	netwatch02	Jan-05-16

You also need to keep a close eye on what network “Scanning” is making it through your firewall. NetWatcher provides, widgets for this as well. Here is an example of multiple scans taking place on 2 different corporate assets.



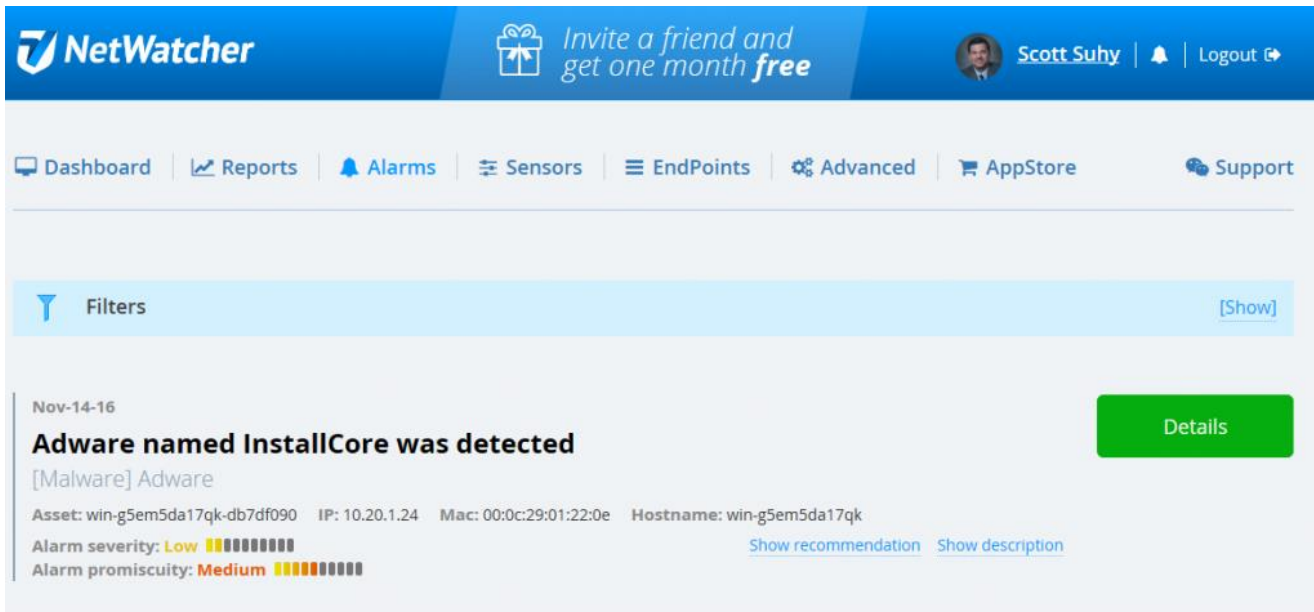
With all of these Security Hygiene items it is up to you to determine if they are normal and safe or do you need to blacklist IP addresses or entire countries at the firewall/router so they can never enter the organization. Do your users do business in those countries? Do your users do business with the organizations that own the IP address of those scanning you? These are just a couple of the questions you will need to ask to determine the steps you need to take to take the action necessary to increase your organizations security posture.

Your Network Cyber Promiscuity Score™



The Cyber Promiscuity Score (CPS) helps customers understand how much the activity going on in the organization exposes them to future compromise.

You will also see that each Alarm has a severity for both Health and Promiscuity Score:



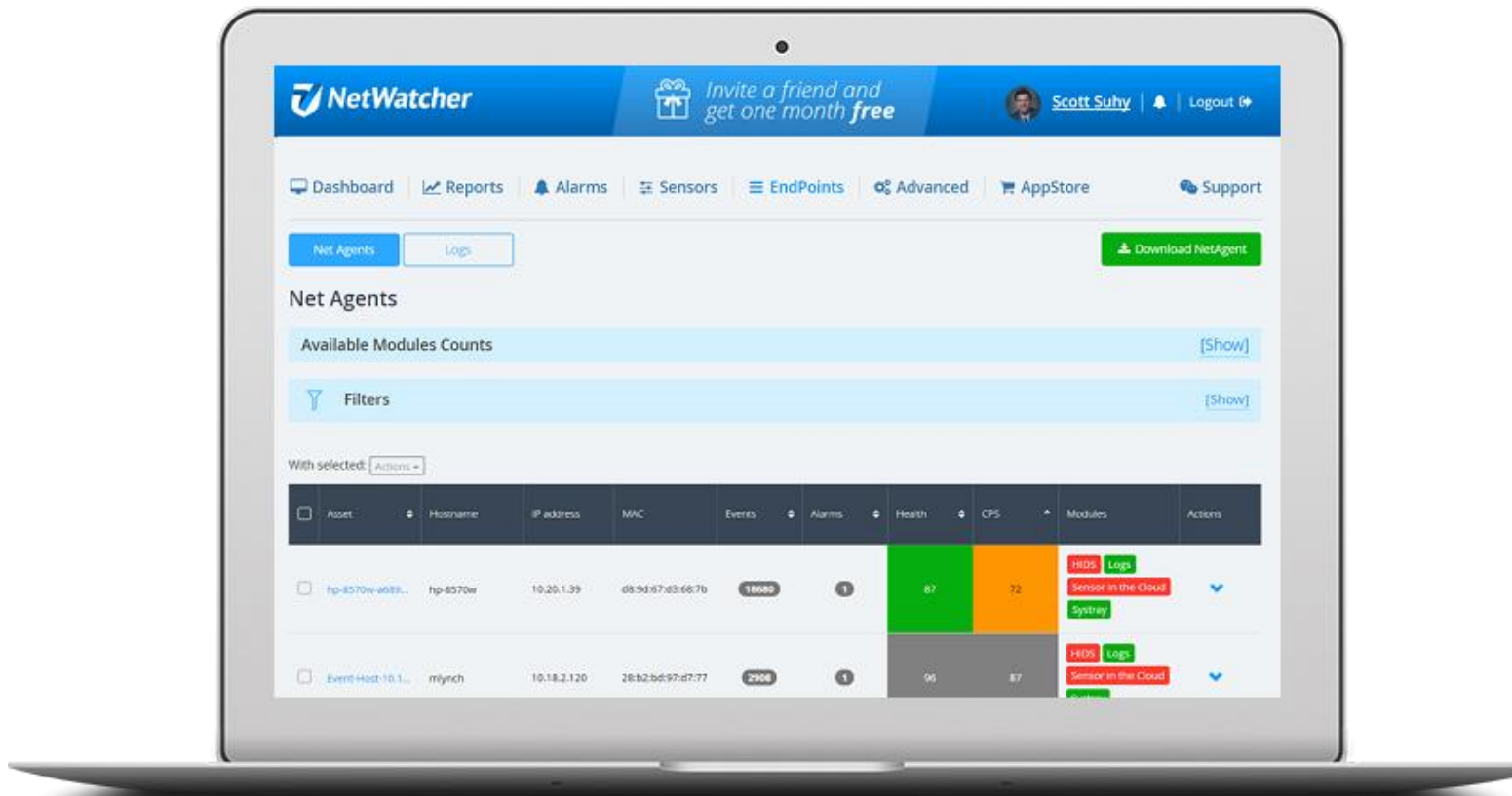
The screenshot shows the NetWatcher dashboard interface. At the top, there's a blue header with the NetWatcher logo, a promotional banner for inviting a friend, and a user profile for Scott Suhy with a logout button. Below the header is a navigation bar with links to Dashboard, Reports, Alarms, Sensors, EndPoints, Advanced, AppStore, and Support. A light blue filter bar is visible above the main content area. The main content area displays an alarm for 'Nov-14-16' with the title 'Adware named InstallCore was detected'. Below the title, it says '[Malware] Adware'. The asset information is listed as 'Asset: win-g5em5da17qk-db7df090', 'IP: 10.20.1.24', 'Mac: 00:0c:29:01:22:0e', and 'Hostname: win-g5em5da17qk'. The alarm severity is 'Low' (indicated by 1 yellow bar and 7 empty bars) and the alarm promiscuity is 'Medium' (indicated by 4 yellow bars and 4 empty bars). There are links for 'Show recommendation' and 'Show description'. A green 'Details' button is located to the right of the alarm information.

The Variables that drive the Cyber Promiscuity Score are:

- *Length of time alarms are open*
- *Percent of corporate assets with open alarms*
- *Promiscuity Rating of the alarms*

Now managers in the organization can quickly see (real time) how much risk they have of a serious cyber security exploit.

The NetWatcher Cloud Endpoint



Managers in the organization can also see where the risk is coming from in their organization because this new Cyber Promiscuity Score and Cyber Health Score is also applied to each asset in the organization that is running the NetWatcher Cloud Endpoint service.

HOST Intrusion Detection (HIDS)

The NetWatcher Cloud Endpoint has modules that you can load for different functions. The HIDS module enables file integrity monitoring, root-check, and process monitoring.

LOGS

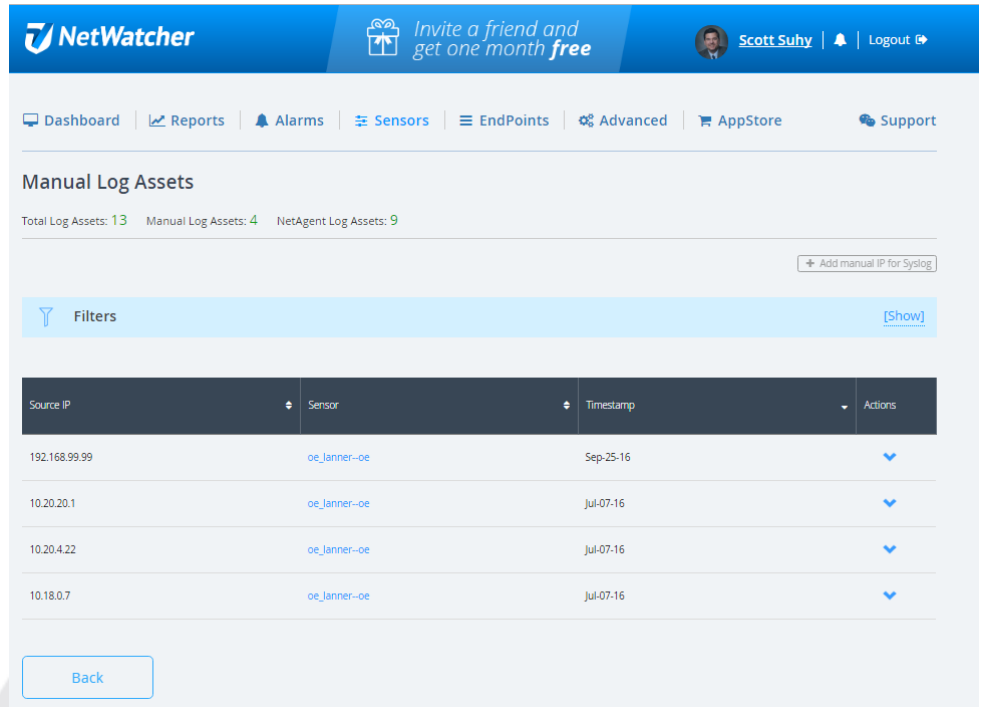
The LOGS module sends the endpoint's logs to the sensor for correlation. This is especially handy for server logs.

Sensor-in-the-Cloud

The NetWatcher Sensor-in-the-Cloud module provides a secure Virtual Private Network (VPN) and utilizes a cloud sensor when the user is not on the corporate network

Security Information and Event Management (SIEM)

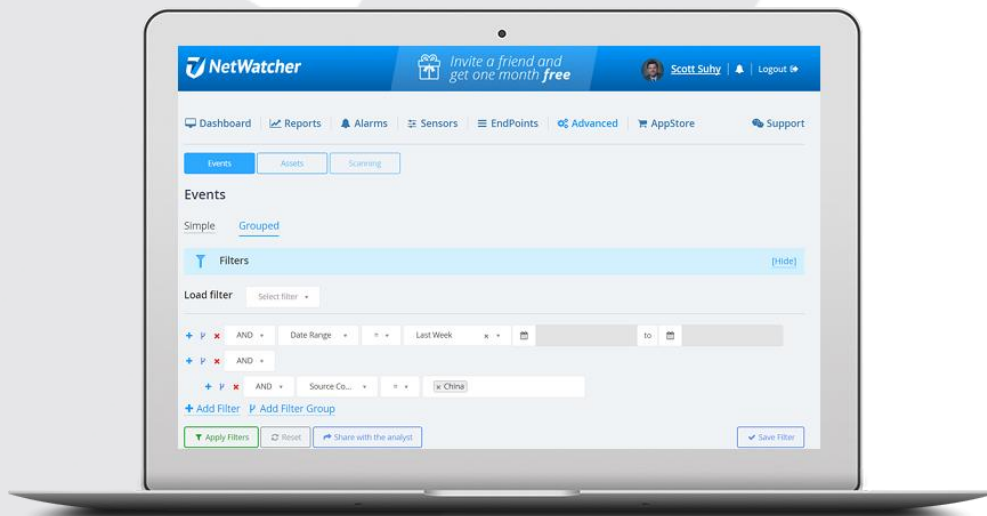
NetWatcher also operates as a SIEM where it gathers both logs from endpoints as well as SYSLOGs that are pointed to it. The sensor uses these logs for anomaly purposes and report them to the cloud service for advanced correlation over time.



The screenshot shows the 'Manual Log Assets' page in the NetWatcher interface. The top navigation bar includes the NetWatcher logo, a promotional banner for a free trial, and user information for Scott Suhly. The main navigation menu contains links for Dashboard, Reports, Alarms, Sensors, EndPoints, Advanced, AppStore, and Support. The page title is 'Manual Log Assets', and it displays statistics: Total Log Assets: 13, Manual Log Assets: 4, and NetAgent Log Assets: 9. A button 'Add manual IP for Syslog' is visible. Below a 'Filters' section, a table lists log assets with columns for Source IP, Sensor, Timestamp, and Actions. The table contains four entries, all from sensor 'oe_lanner-oe'. A 'Back' button is at the bottom.

Source IP	Sensor	Timestamp	Actions
192.168.99.99	oe_lanner-oe	Sep-25-16	▼
10.20.20.1	oe_lanner-oe	Jul-07-16	▼
10.20.4.22	oe_lanner-oe	Jul-07-16	▼
10.18.0.7	oe_lanner-oe	Jul-07-16	▼

Users can do report on anomalous behavior pre (events) or post (alarms) correlation and set tripwires that can be valuable for noticing unique behavior as soon as it occurs.



The screenshot shows the 'Events' page in the NetWatcher interface. The top navigation bar is identical to the previous screenshot. The main navigation menu includes 'Events', 'Assets', and 'Scanning'. The 'Events' section is active, with 'Simple' and 'Grouped' tabs. Below a 'Filters' section, there is a 'Load filter' dropdown and a complex filter builder. The filter builder shows a sequence of conditions: 'Date Range' (Last Week), 'Source Co...' (China), and 'Add Filter Group'. Buttons for 'Apply Filter', 'Reset', 'Share with the analyst', and 'Save Filter' are at the bottom.

We hope you enjoy the NetWatcher service. We've designed the service to be useful for managers, help desk techs and for advanced security analysts. We've tried to make the User Interface (UI) intuitive and easy to use as well as powerful. If you have any questions don't hesitate to contact us at info@netwatcher.com

Follow us on Twitter @netwatcher.

<https://netwatcher.com>