NetWatcher

Comparing the NetWatcher® Managed Detection & Response Service to the AlienVault USM™

Several companies find themselves comparing NetWatcher to AlienVault during the sales process. This paper is meant to outline some of the similarities and differences. The biggest difference between the two companies is that NetWatcher is a service where AlienVault is primarily a product so at the end of the day it is comparing Apples and Oranges. However, we know that customers are faced with this choice — Managed Detection and Response with NetWatcher or buying a platform like AlienVault.

Did you ever hear the saying “Fast, good or affordable? Pick two.” Known as the Project Management Triangle. I don’t think it applies here–In this case I think you can have all 3.….

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.

What is AlienVault USM?

AlienVault offers a paid security platform, called Unified Security Management, that integrates threat detection, incident response, and compliance management into one solution. Threat applications are offered via hardware, virtual machines and as a cloud service. (from here).

AlienVault versus NetWatcher – Pricing

(NetWatcher is AFFORDABLE and no security analysts required)

AlienVault's pricing is on their Website but you can also find it here and here. The big deal here is not the pricing of the platform (as both are comparable in price) but the price of the user of the platform. Many mid-market companies do not have security engineers and the AlienVault tool really requires this level of engineering proficiency–hence a dilemma. NetWatcher does not require you to have a team of very expensive security analysts (>100k/year) because we do the heavy lifting for you in our Security Operations Center (SOC). Which brings me to points 'setup' and 'ease of use' below. Also, keep in mind that buying software is a CAPEX versus OPEX event –your CFO will be happier.

> "(ISC)2, a provider of education products, career services, and credentials to IT security pros, estimates that by 2019 there will be a need for 6 million security professionals, but only 4.5 million will have the necessary qualifications for those jobs. The burgeoning growth of demand for security pros has transformed the career path from a narrow field to a broad one." -TechBeacon

AlienVault versus NetWatcher – Setup

(NetWatcher is FAST & EASY to Setup)

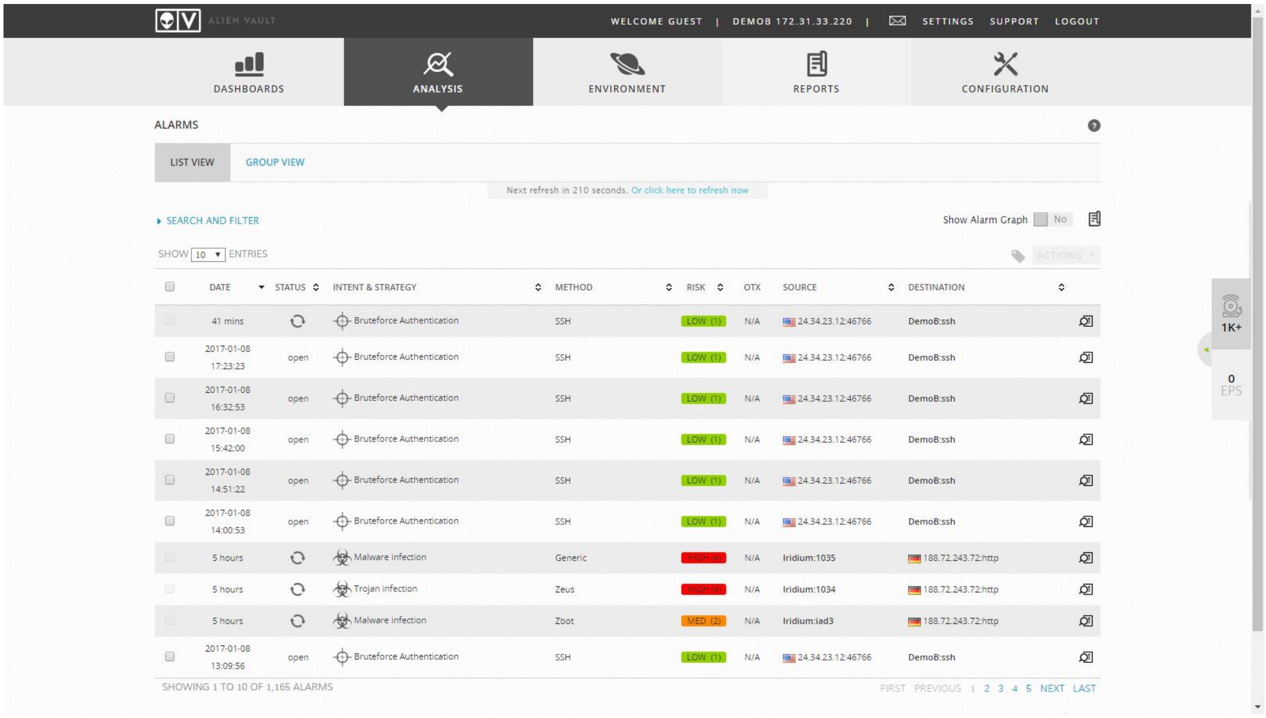
The AlienVault tool requires you to really understand Linux and systems administration. You can see it right in their 247 page deployment guide --it's hard to setup. They offer some great 'paid' training that is quite pricey if you want to help turn your IT engineer into a Security Analyst. In contrast the NetWatcher appliance (or Virtual Machine) is very easy to setup — just create a mirror port on your router or switch and hook us into it… If you want to install the NetAgent on endpoints you can but it's not required (but recommended) and you can also point all your SYSLOGs to the sensor as well for ingestion and advanced correlation.

AlienVault versus NetWatcher – Ease of Use

(NetWatcher is FAST)

This is where things bifurcate. If you are in IT and have no advanced security expertise AlienVault is a stretch and is really going to require you to either hire a person that is qualified to use it, learn it yourself by going to training and dedicating a lot of time to understanding security or hiring a third party MSP or MSSP to manage it for you.

As an example, will your IT guys know what to do with any of these Alarms?



ALARMS

LIST VIEW | GROUP VIEW

Next refresh in 210 seconds. Or click here to refresh now

▸ SEARCH AND FILTER

Show Alarm Graph No

SHOW 10 ENTRIES

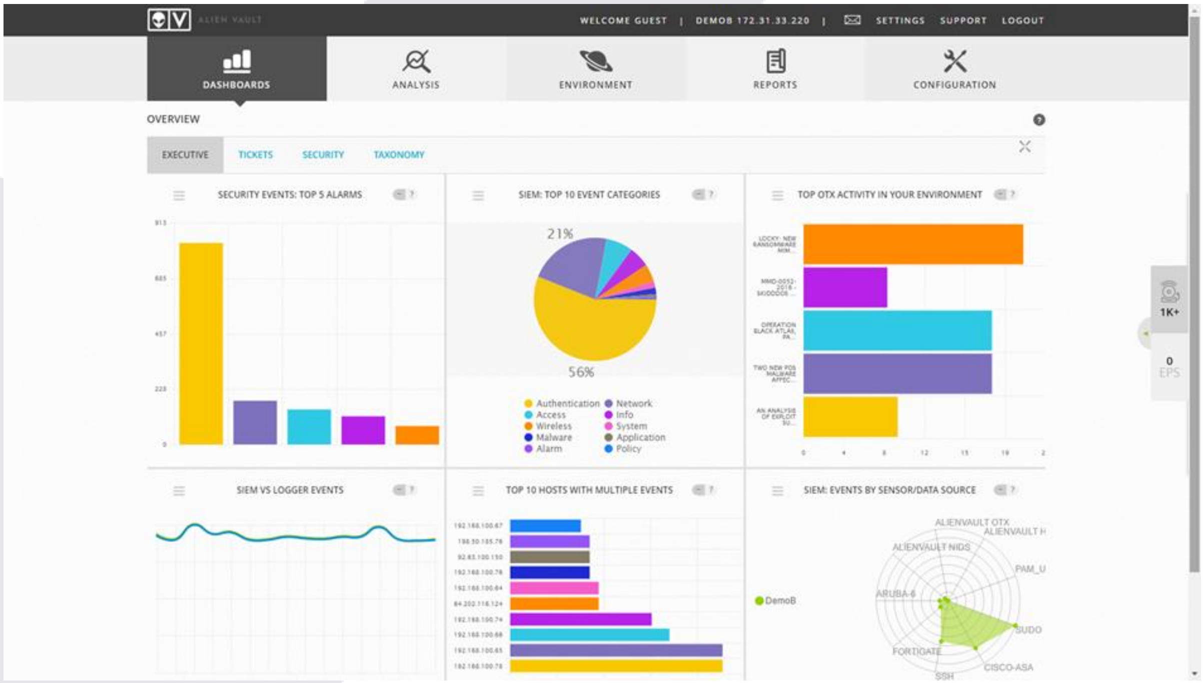
ACTIONS

□	DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION
□	41 mins		Bruteforce Authentication	SSH	LOW (1)	N/A	24.34.23.12:46766	DemoB:ssh
□	2017-01-08 17:23:23	open	Bruteforce Authentication	SSH	LOW (1)	N/A	24.34.23.12:46766	DemoB:ssh
□	2017-01-08 16:32:53	open	Bruteforce Authentication	SSH	LOW (1)	N/A	24.34.23.12:46766	DemoB:ssh
□	2017-01-08 15:42:00	open	Bruteforce Authentication	SSH	LOW (1)	N/A	24.34.23.12:46766	DemoB:ssh
□	2017-01-08 14:51:22	open	Bruteforce Authentication	SSH	LOW (1)	N/A	24.34.23.12:46766	DemoB:ssh
□	2017-01-08 14:00:53	open	Bruteforce Authentication	SSH	LOW (1)	N/A	24.34.23.12:46766	DemoB:ssh
□	5 hours		Malware infection	Generic	HIGH (4)	N/A	Iridium:1035	188.72.243.72:http
□	5 hours		Trojan infection	Zeus	HIGH (4)	N/A	Iridium:1034	188.72.243.72:http
□	5 hours		Malware infection	Zbot	MED (2)	N/A	Iridium:iad3	188.72.243.72:http
□	2017-01-08 13:09:56	open	Bruteforce Authentication	SSH	LOW (1)	N/A	24.34.23.12:46766	DemoB:ssh

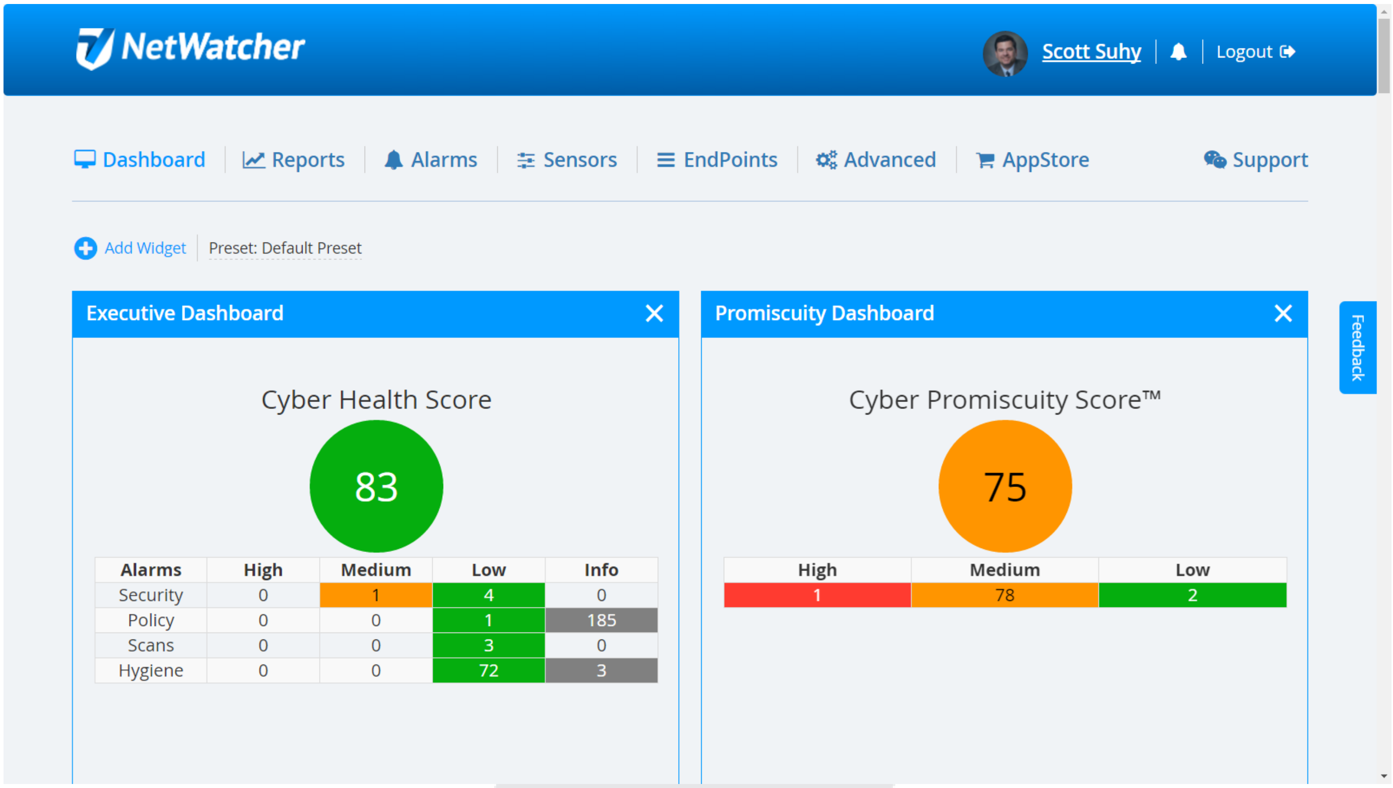
SHOWING 1 TO 10 OF 1,165 ALARMS

FIRST PREVIOUS 1 2 3 4 5 NEXT LAST

And what is the value of any of these widgets on the AlienVault dashboard? Do your IT guys know what to do with SIEM Top 10 Event Categories? It looks good but what value is it?



If you use NetWatcher you get a real time Security Health Score — what's at risk now! …and a Cyber Promiscuity Score (CPS) –what's my probability of attack in the future.   Not only that, if you load the NetWatcher netagent on the endpoints you can get these scores for each endpoint in the organization.



Executive Dashboard

Cyber Health Score

83

Alarms	High	Medium	Low	Info
Security	0	1	4	0
Policy	0	0	1	185
Scans	0	0	3	0
Hygiene	0	0	72	3

Promiscuity Dashboard

Cyber Promiscuity Score™

75

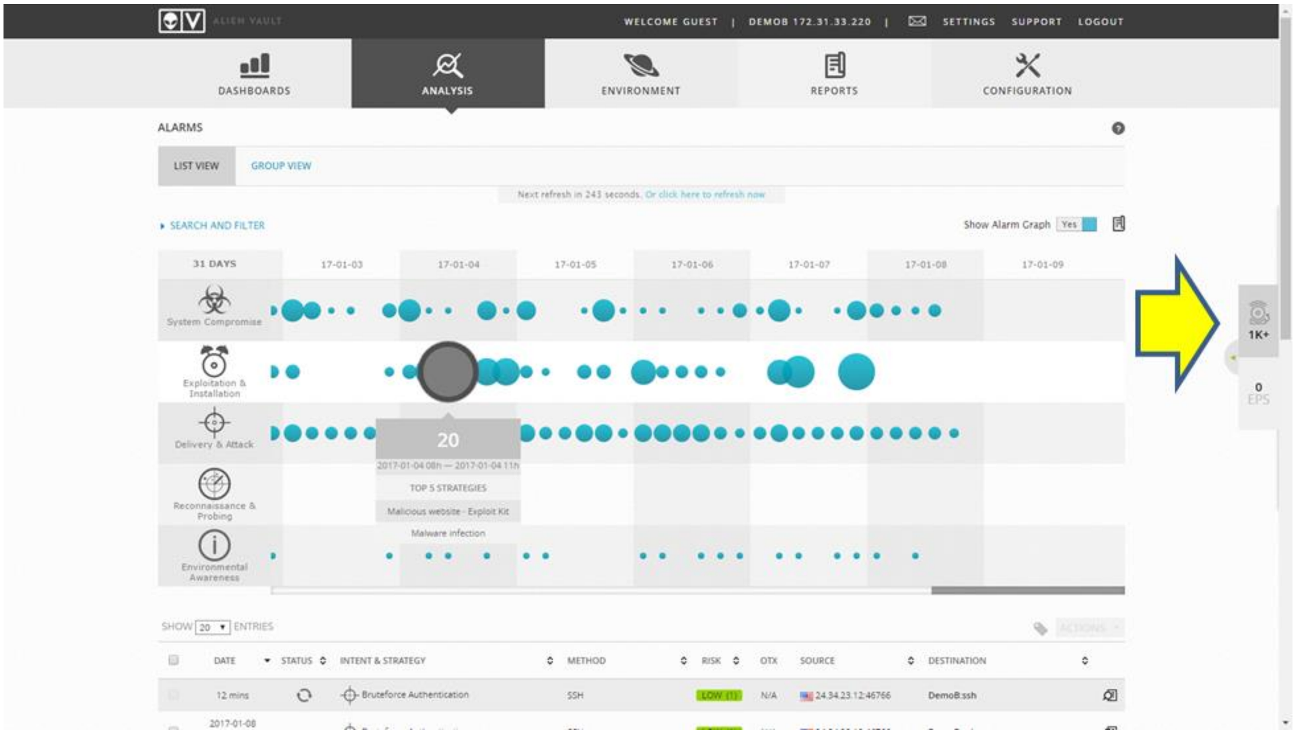
High	Medium	Low
1	78	2

Know exactly what needs fixed and your probability of attack and what asset in your organization is most likely to cause you an issue.

AlienVault versus NetWatcher – Usefulness of Information

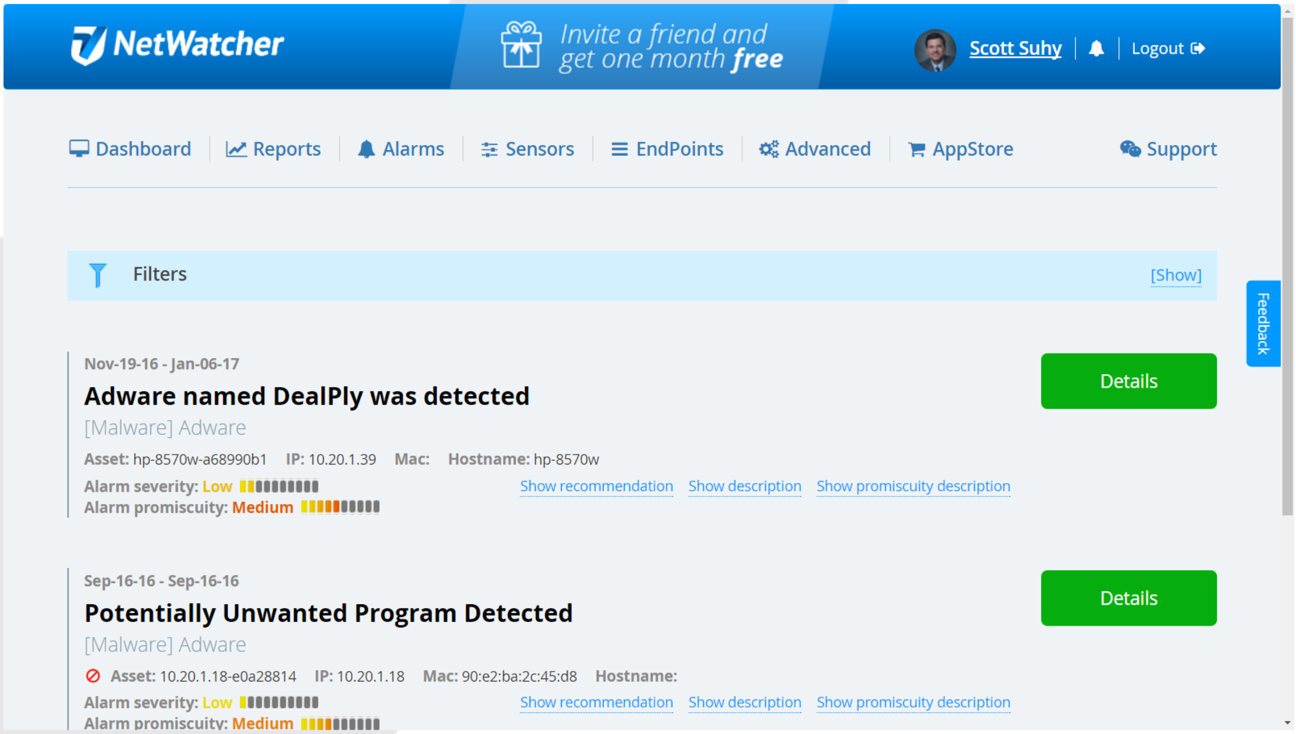
(NetWatcher is GREAT)

If you are a security analyst the AlienVault information is useful and understandable.   However, in contrast the NetWatcher information is very clear and concise and we only tell you about an Alarm once and age it over a two-week period whereas AlienVault tells you about the Alarm over and over and over and over.… Just in the demo they have online there are over 1000 open Alarms mostly for the same issues.   If you want event fatigue you will get it with AlienVault.



	DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION
□	12 mins		Bruteforce Authentication	SSH	LOW (1)	N/A	24.34.23.12:46766	DemoB:ssh
□	2017-01-08							

In contrast, with NetWatcher you have Easy to understand Alarms with Easy to understand remediation guidance.



Nov-19-16 - Jan-06-17

Adware named DealPly was detected

[Malware] Adware

Asset: hp-8570w-a68990b1 **IP:** 10.20.1.39 **Mac:** **Hostname:** hp-8570w

Alarm severity: Low

Alarm promiscuity: Medium

Show recommendation Show description Show promiscuity description

Sep-16-16 - Sep-16-16

Potentially Unwanted Program Detected

[Malware] Adware

Asset: 10.20.1.18-e0a28814 **IP:** 10.20.1.18 **Mac:** 90:e2:ba:2c:45:d8 **Hostname:**

Alarm severity: Low

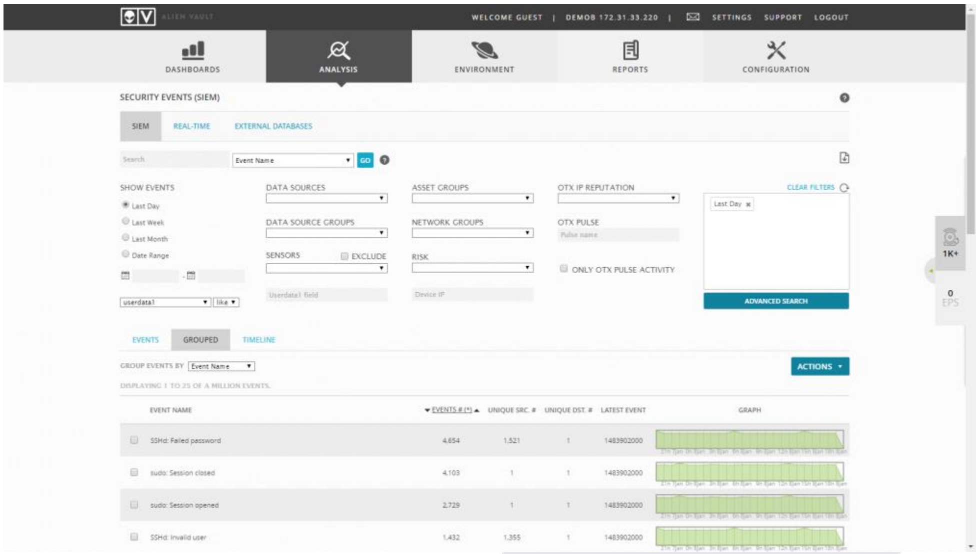
Alarm promiscuity: Medium

Show recommendation Show description Show promiscuity description

AlienVault versus NetWatcher – Usefulness to Security Analysts

(NetWatcher is GREAT for Security Analysts Too)

Both the AlienVault tool and the NetWatcher service are great for security analysts. You can get at all the same data but the NetWatcher interface is just a lot easier to use. With NetWatcher you can also easily setup tripwires to alert you via SMS or email if that bad actor you have been looking for has been poking around. But–it's important for me to point out here–there is a team of Security Analysts in the NetWatcher Secure Operations Center (SOC) doing this for you….



SECURITY EVENTS (SIEM)

Search: Event Name

SHOW EVENTS: ● Last Day ○ Last Week ○ Last Month ○ Date Range

userdata1 like

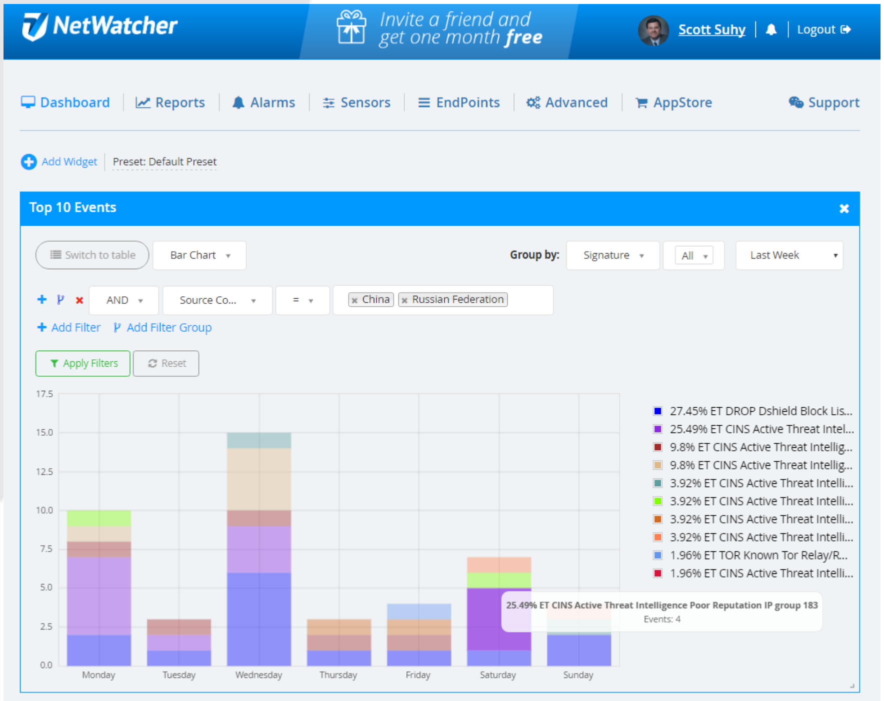
DATA SOURCES · DATA SOURCE GROUPS · SENSORS □ EXCLUDE · ASSET GROUPS · NETWORK GROUPS · RISK · OTX IP REPUTATION · OTX PULSE · □ ONLY OTX PULSE ACTIVITY

CLEAR FILTERS: Last Day ×

GROUP EVENTS BY Event Name

DISPLAYING 1 TO 25 OF A MILLION EVENTS.

	EVENT NAME	EVENTS # (*)	UNIQUE SRC. #	UNIQUE DST. #	LATEST EVENT	GRAPH
□	SSHd: Failed password	4,654	1,521	1	1483902000	
□	sudo: Session closed	4,103	1	1	1483902000	
□	sudo: Session opened	2,729	1	1	1483902000	
□	SSHd: Invalid user	1,432	1,355	1	1483902000	


NetWatcher
Invite a friend and get one month free
Scott Suhy
Logout
Dashboard
Reports
Alarms
Sensors
EndPoints
Advanced
AppStore
Support
Add Widget
Switch to table
Add Filter
Add Filter Group
Apply Filters
Reset
17.5
15.0
12.5
10.0
7.5
5.0
2.5
0.0
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
27.45% ET DROP Dshield Block Lis...
25.49% ET CINS Active Threat Intel...
9.8% ET CINS Active Threat Intellig...
9.8% ET CINS Active Threat Intellig...
3.92% ET CINS Active Threat Intelli...
3.92% ET CINS Active Threat Intelli...
3.92% ET CINS Active Threat Intelli...
3.92% ET CINS Active Threat Intelli...
1.96% ET TOR Known Tor Relay/R...
1.96% ET CINS Active Threat Intelli...
25.49% ET CINS Active Threat Intelligence Poor Reputation IP group 183
Events: 4

Preset: Default Preset

Top 10 Events

Bar Chart

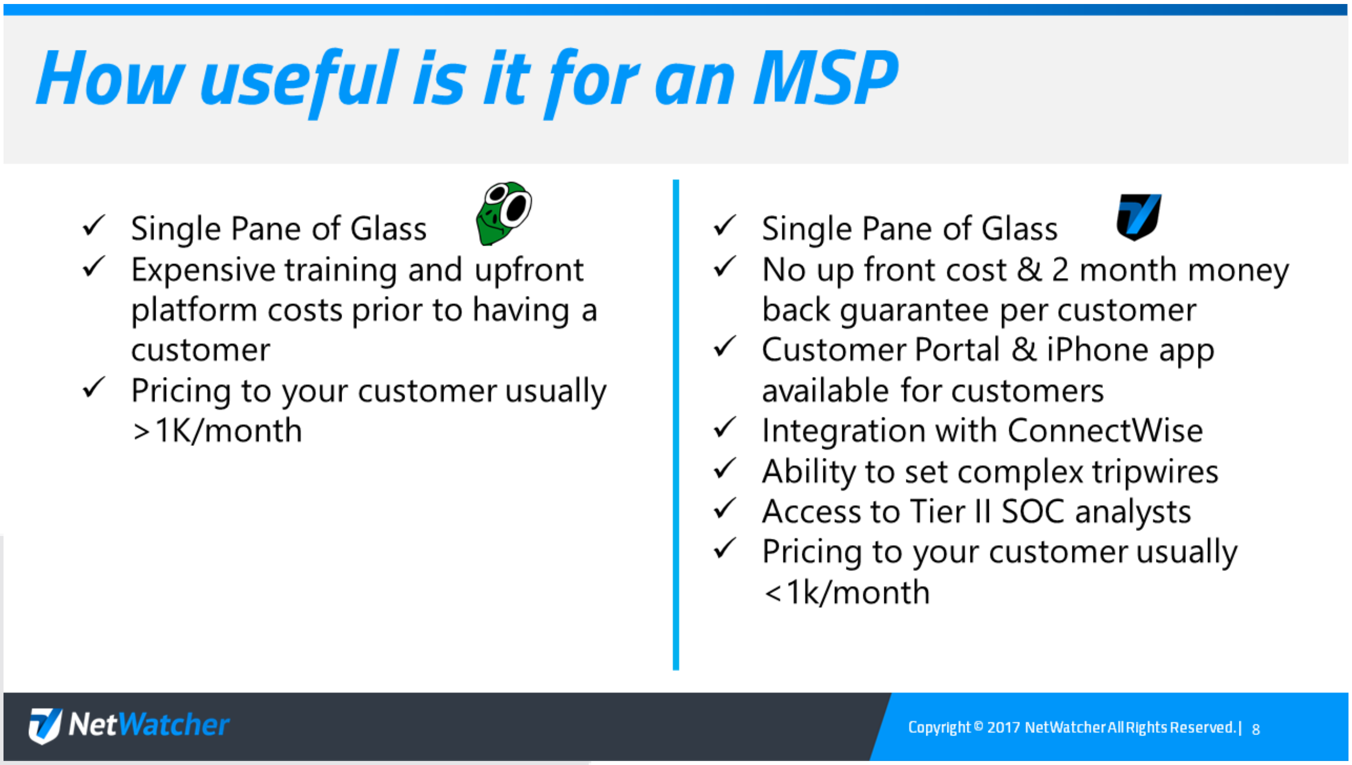
Group by: Signature · All · Last Week

AND · Source Co... · = · × China × Russian Federation

AlienVault versus NetWatcher – Usefulness to the Managed Services Provider ‘MSP’

(NetWatcher is GREAT)

This is where the NetWatcher tool really shines. Most MSPs customers can’t afford an MSP’s service fees once they invest in AlienVault or tools like it. However, with NetWatcher the MSP does not have to pay any money until they sign a customer and make money and start the service. NetWatcher is the MSP’s tier II support and their SOC. NetWatcher analysts teach the MSP how to become a great MSSP along the way and there is no outlay of cash up front.



How useful is it for an MSP

- ✓ Single Pane of Glass
- ✓ Expensive training and upfront platform costs prior to having a customer
- ✓ Pricing to your customer usually >1K/month

- ✓ Single Pane of Glass
- ✓ No up front cost & 2 month money back guarantee per customer
- ✓ Customer Portal & iPhone app available for customers
- ✓ Integration with ConnectWise
- ✓ Ability to set complex tripwires
- ✓ Access to Tier II SOC analysts
- ✓ Pricing to your customer usually <1k/month

Copyright © 2017 NetWatcher All Rights Reserved. | 8

AlienVault versus NetWatcher – Overall Comparison

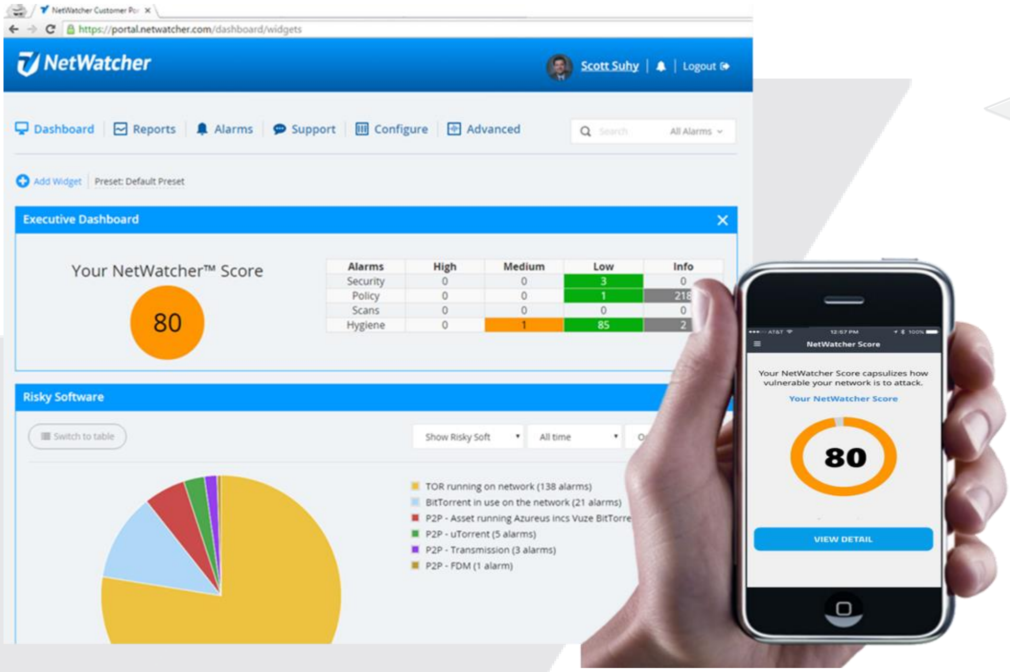
(FAST, GOOD and AFFORDABLE)

		NetWatcher	AlienVault
Security Analyst Support	Analysts in the NetWatcher SoC reviewing your data helping you understand complex issues	YES	NO
Easy to setup	No knowledge of complex Linux deployment required	YES	NO
	Deployed as a service	YES	NO
Easy to use	No required security experience	YES	NO
	Easy to understand user interface	YES	NO
Affordable	Does NOT require you to have security experience	YES	NO
	2 Month Money Back Guarantee	YES	NO
	Affordable Pricing	YES	YES
Advanced Correlation		YES	YES
Log Aggregation (SIEM)		YES	YES
Asset Discovery		YES	YES
Behavioral Monitoring		YES	YES
Intrusion Detection		YES	YES
Vulnerability Assessment		YES	YES
Sensor-in-the-Cloud	Security when asset leaves the network	YES	NO
MSP Friendly	No upfront Investment	YES	NO
	No required security experience	YES	NO
	ConnectWise Integration	YES	NO

Oh yea… there is this other cool little feature we should tell you about with NetWatcher… it's our Sensor-in-the-Cloud. If you don't want to deploy a sensor locally you don't have to… your endpoints can use our Sensor-in-the-Cloud option. This is also great to turn on for endpoints that are on the network sometimes and off others (mobile workers). You want to know if your CXO let their kids play Minecraft and download unsafe JAR files on their corporate laptop while they were on vacation long before that asset ever hits the corp net…

So I think you can have all three with NetWatcher-Fast, Good and AFFORDABLE!

More on NetWatcher



Your NetWatcher™ Score

80

Alarms	High	Medium	Low	Info
Security	0	0	3	0
Policy	0	0	1	218
Scans	0	0	0	0
Hygiene	0	1	85	2

Your NetWatcher Score capsulizes how vulnerable your network is to attack.

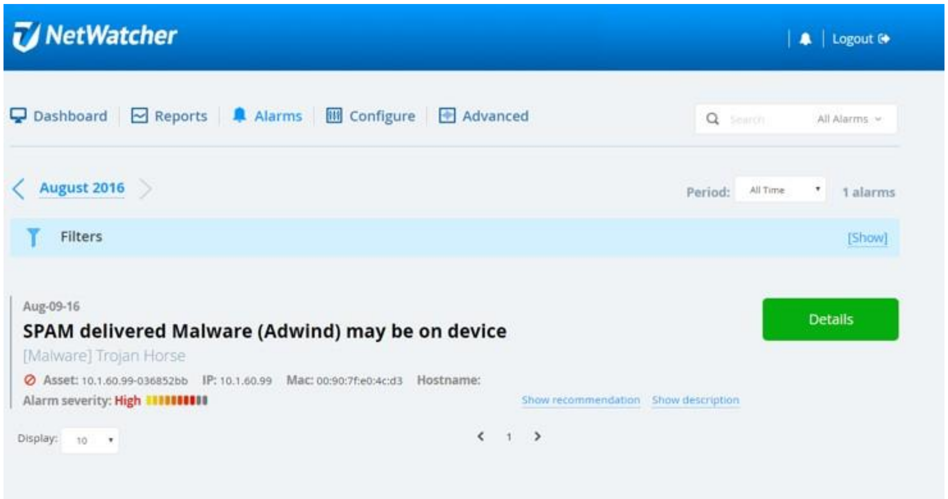
Your NetWatcher Score

80

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.



Period: All Time 1 alarms

Aug-09-16

SPAM delivered Malware (Adwind) may be on device

[Malware] Trojan Horse

Asset: 10.1.60.99-036852bb IP: 10.1.60.99 Mac: 00:90:7f:e0:4c:d3 Hostname:

Alarm severity: High

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.

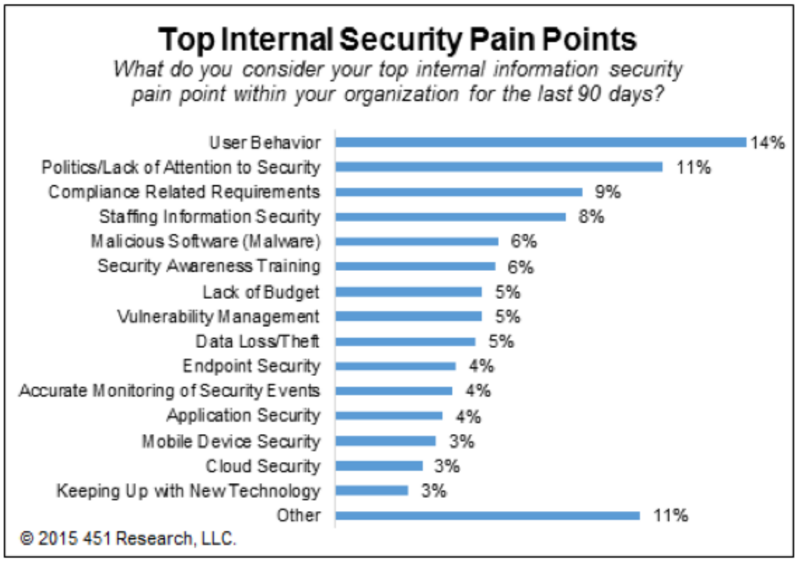
Employees Activities

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).

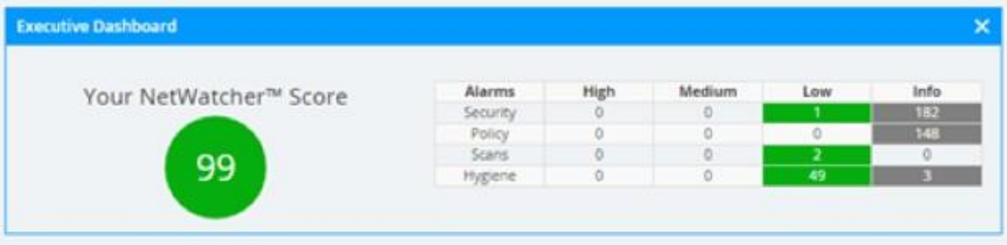
Some examples are:

- 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.

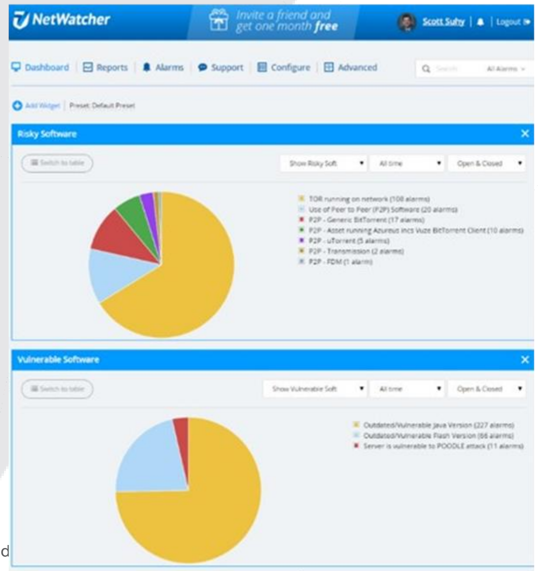


As you can see from the latest 451 Research study User Behavior is the leading internal IT security pain point.



Alarms	High	Medium	Low	Info
Security	0	0	1	182
Policy	0	0	0	148
Scans	0	0	2	0
Hygiene	0	0	49	3

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.

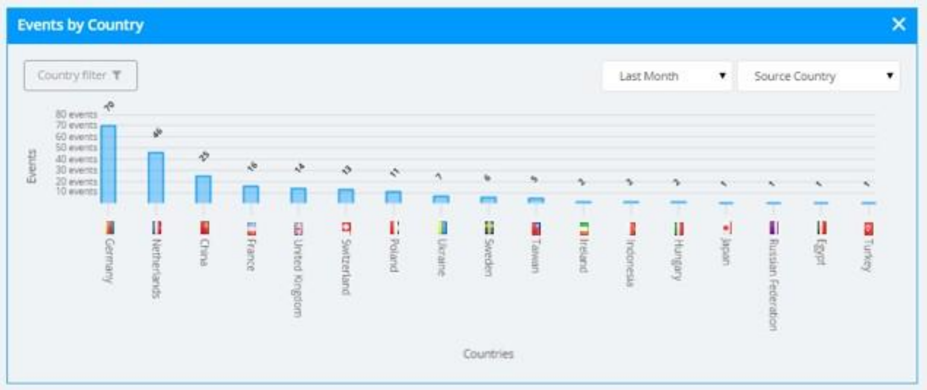

NetWatcher
Invite a friend and get one month free
Scott Sufty | Logout
Dashboard | Reports | Alarms | Support | Configure | Advanced
Search
All Alarms
Add Widget | Preset: Default Preset
Risky Software
Switch to table
Show Risky Soft
All time
Open & Closed
TOR running on network (108 alarms)
Use of Peer to Peer (P2P) Software (20 alarms)
P2P - Generic BitTorrent (17 alarms)
P2P - Asset running Azureus incs Vuze BitTorrent Client (10 alarms)
P2P - uTorrent (5 alarms)
P2P - Transmission (2 alarms)
P2P - FDM (1 alarm)
Vulnerable Software
Switch to table
Show Vulnerable Soft
All time
Open & Closed
Outdated/Vulnerable Java Version (227 alarms)
Outdated/Vulnerable Flash Version (66 alarms)
Server is vulnerable to POODLE attack (11 alarms)

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

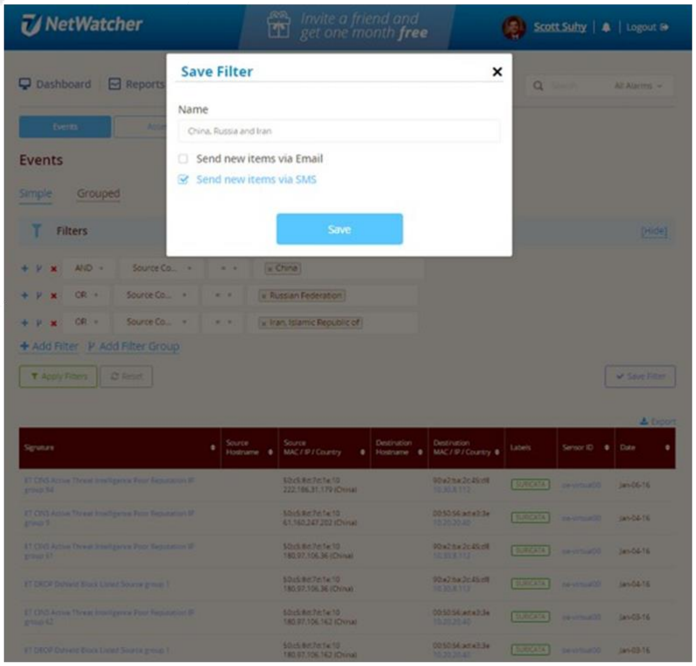
Network Security



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.



Save Filter

Name: China, Russia and Iran

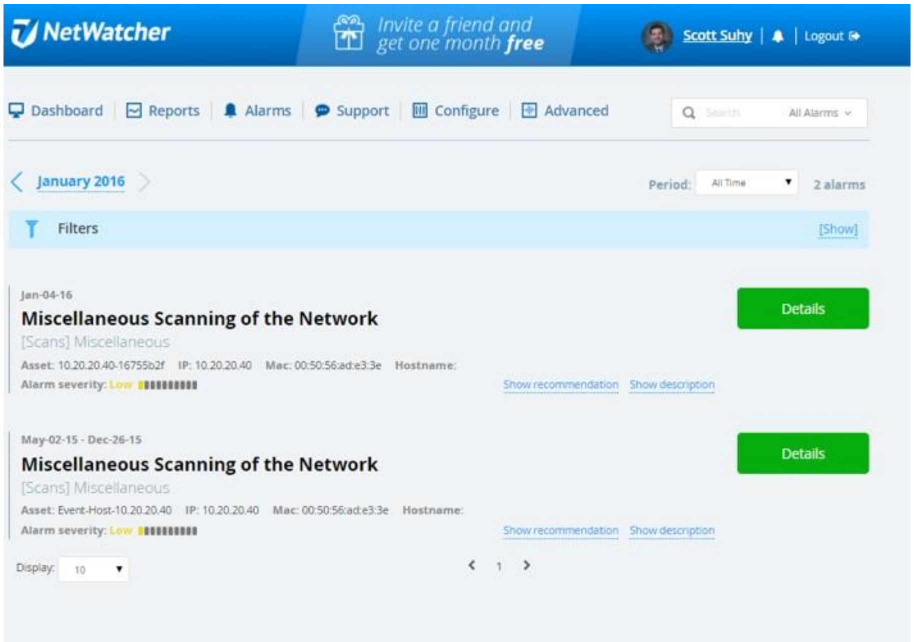
☐ Send new items via Email
☑ Send new items via SMS

Save

AND	Source Co...		China
OR	Source Co...		Russian Federation
OR	Source Co...		Iran, Islamic Republic of

Signature	Source Hostname	Source MAC / IP / Country	Destination Hostname	Destination MAC / IP / Country	Labels	Sensor ID	Date
ET CINS Active Threat Intelligence Poor Reputation IP group 54		50:c5:8d:7d:1e:10 222.186.31.179 (China)		90:a2:ba:2c:45:d8 10.30.8.112	SURICATA	ne-virtual00	Jan-06-16
ET CINS Active Threat Intelligence Poor Reputation IP group 5		50:c5:8d:7d:1e:10 61.160.247.202 (China)		00:50:56:ad:e3:3e 10.20.20.40	SURICATA	ne-virtual00	Jan-04-16
ET CINS Active Threat Intelligence Poor Reputation IP group 61		50:c5:8d:7d:1e:10 180.97.106.36 (China)		90:a2:ba:2c:45:d8 10.30.8.112	SURICATA	ne-virtual00	Jan-04-16
ET DROP Dshield Block Listed Source group 1		50:c5:8d:7d:1e:10 180.97.106.36 (China)		90:a2:ba:2c:45:d8 10.30.8.112	SURICATA	ne-virtual00	Jan-04-16
ET CINS Active Threat Intelligence Poor Reputation IP group 62		50:c5:8d:7d:1e:10 180.97.106.162 (China)		00:50:56:ad:e3:3e 10.20.20.40	SURICATA	ne-virtual00	Jan-03-16
ET DROP Dshield Block Listed Source group 1		50:c5:8d:7d:1e:10 180.97.106.162 (China)		00:50:56:ad:e3:3e 10.20.20.40	SURICATA	ne-virtual00	Jan-03-16

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.



January 2016

Period: All Time

2 alarms

Jan-04-16

Miscellaneous Scanning of the Network

[Scans] Miscellaneous

Asset: 10.20.20.40-16755b2f IP: 10.20.20.40 Mac: 00:50:56:ad:e3:3e Hostname:

Alarm severity: Low

May-02-15 - Dec-26-15

Miscellaneous Scanning of the Network

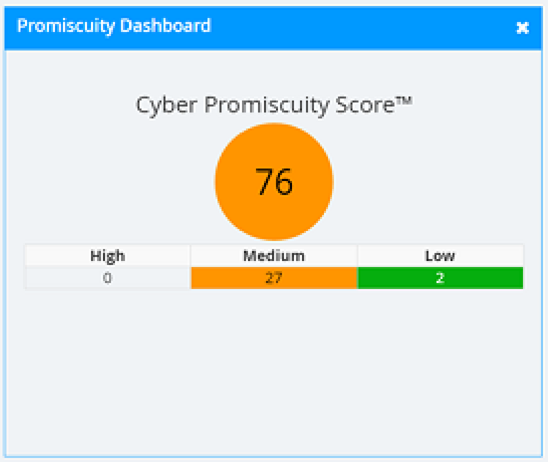
[Scans] Miscellaneous

Asset: Event-Host-10.20.20.40 IP: 10.20.20.40 Mac: 00:50:56:ad:e3:3e Hostname:

Alarm severity: Low

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™



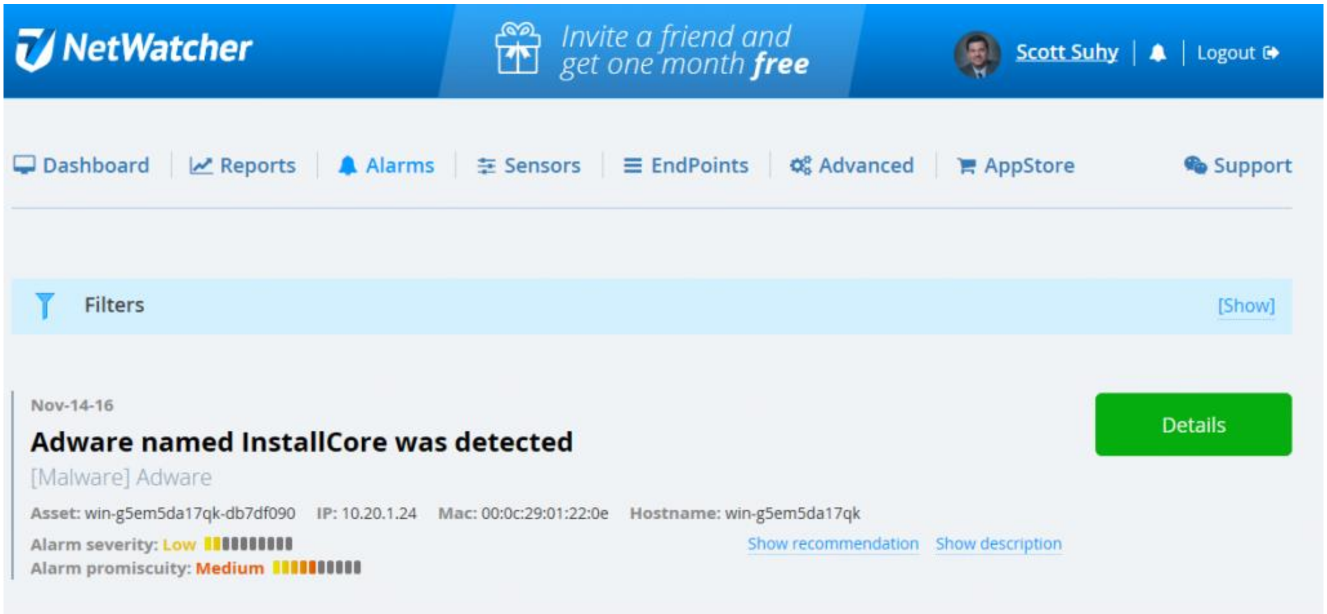
Cyber Promiscuity Score™

76

High	Medium	Low
0	27	2

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:



Nov-14-16

Adware named InstallCore was detected

[Malware] Adware

Asset: win-g5em5da17qk-db7df090 IP: 10.20.1.24 Mac: 00:0c:29:01:22:0e Hostname: win-g5em5da17qk

Alarm severity: Low

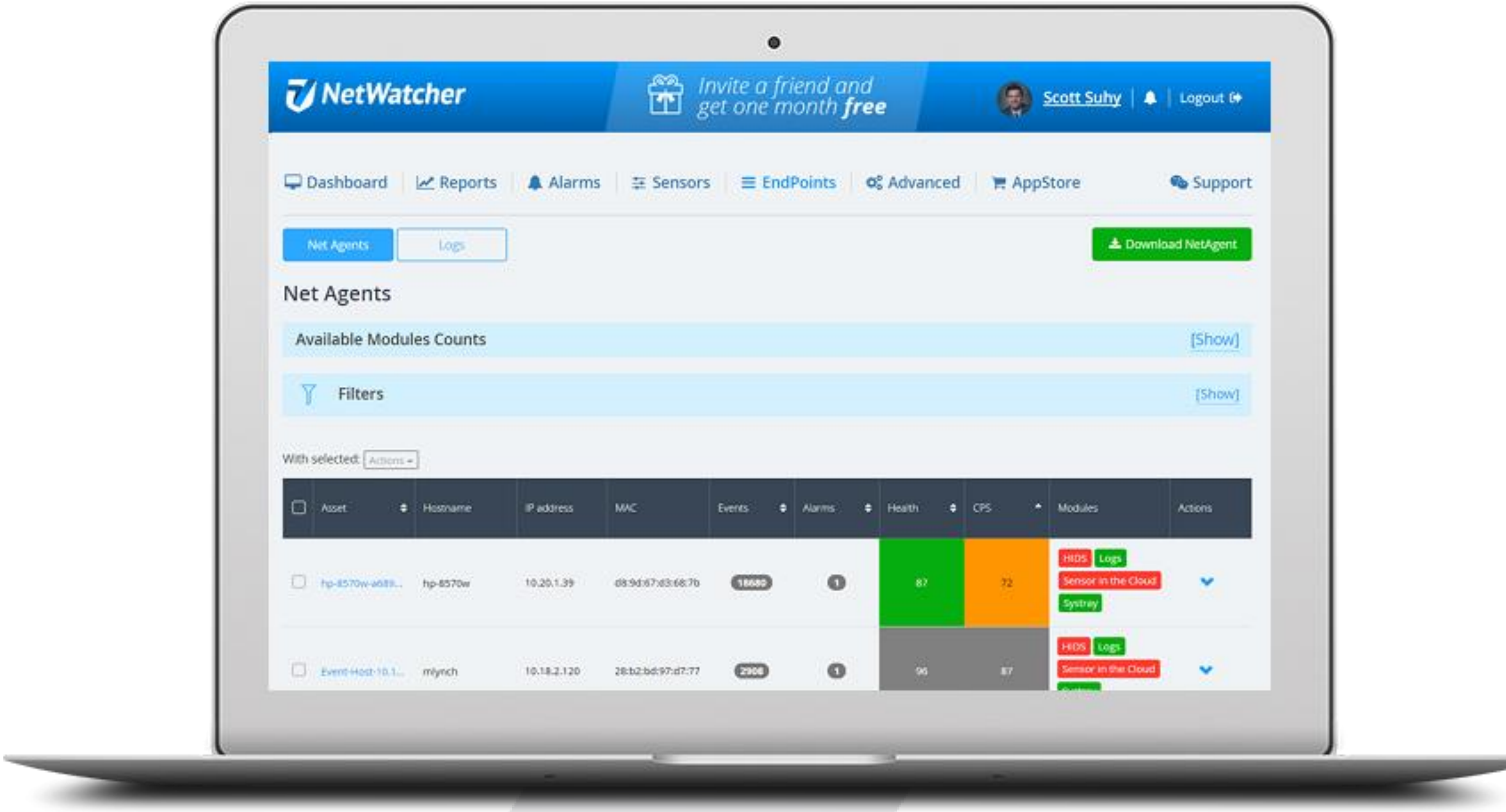
Alarm promiscuity: Medium

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



Net Agents

Available Modules Counts [Show]

Filters [Show]

With selected: Actions

□	Asset	Hostname	IP address	MAC	Events	Alarms	Health	CPS	Modules	Actions
□	hp-8570w-a689...	hp-8570w	10.20.1.39	d8:9d:67:d3:68:7b	18680	1	87	72	HIDS Logs Sensor in the Cloud Systray	⌄
□	Event-Host-10.1...	mlynch	10.18.2.120	28:b2:bd:97:d7:77	2908	1	96	87	HIDS Logs Sensor in the Cloud	⌄

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

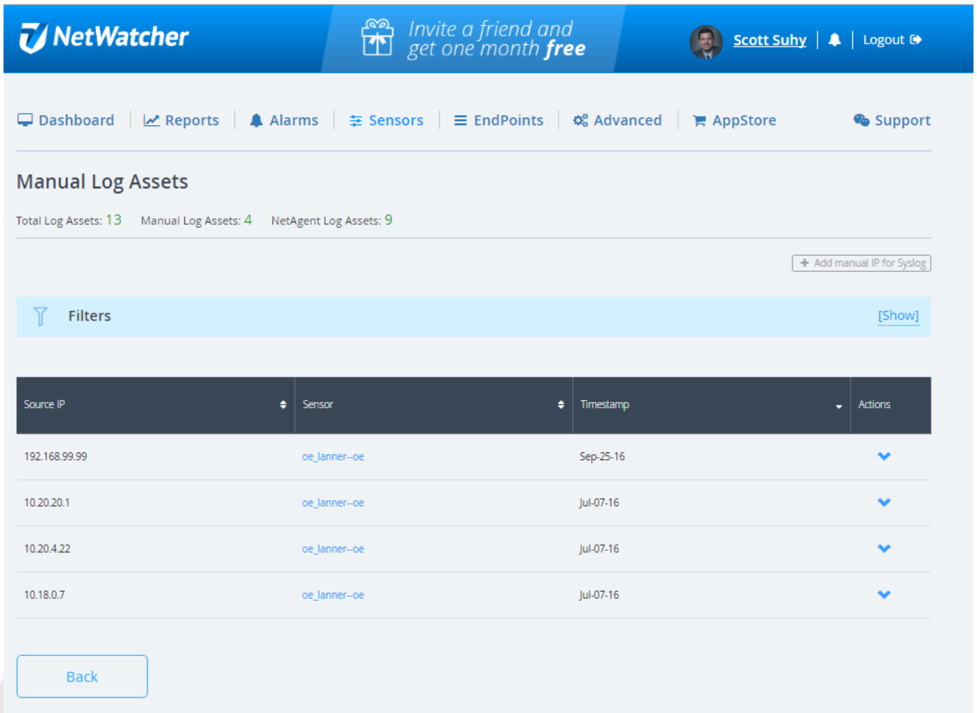
The LOGS module sends the endpoint's logs to the sensor for correlation. This is especially handy for server logs.

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.

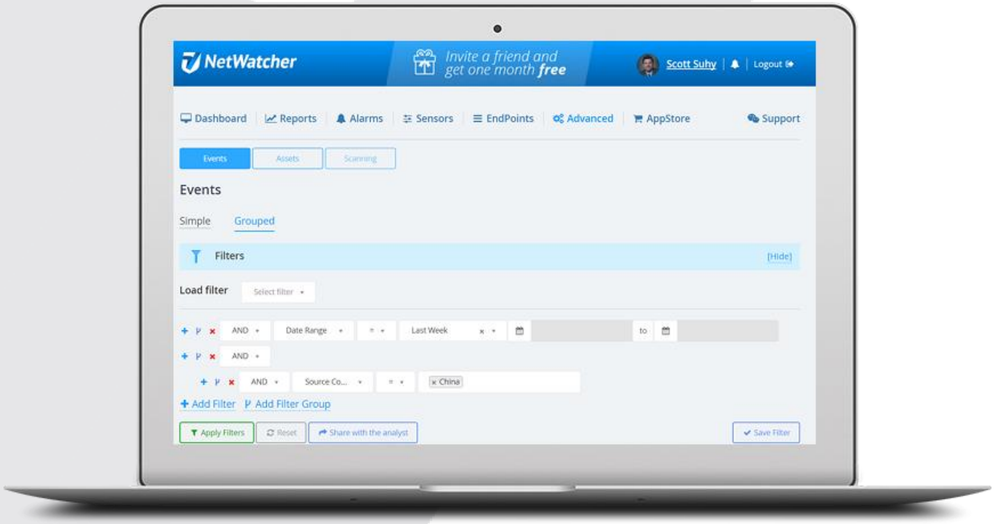


Manual Log Assets

Total Log Assets: 13   Manual Log Assets: 4   NetAgent Log Assets: 9

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.



Events

Load filter: Select filter

AND · Date Range · = · Last Week · to

AND

AND · Source Co... · = · China

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