# Review on Intrusion Detection and Intrusion Prevention Systems

# What is an Intrusion Detection System?

IDS is a system that monitors traffic for suspicious activities. It issues alerts on detecting suspicious system behavior. Any malicious program or lines of code get reported to the admin using an existing set of data. Although IDS triggers alerts for suspicious activities, it often gets exposed to false threats. It is the reason why an IT firm needs to fine-tune IDS when it installs the software.

## How Does An IDS System Differ From IPS?

An intrusion detection system assesses network traffic and inspects signs of possible cyber-attacks. Intrusion prevention systems (aka IPS) inspect encrypted data packets. It can stop data packets from getting delivered based on the nature of network traffic.

The main difference between IPS and IDS is that the former is a control system. IDS is a system used for monitoring data traffic. IDS compares network activity to an existing threat database. IDS takes help from an individual to look at the data traffic.

# What Are The Types Of IDS Systems?

- NIDS (aka network detection system) gets installed at checkpoints. NIDS monitors data traffic from all devices localized on the network.
- HIDS (aka host detection system) gets installed on multiple hosts or servers across the network. HIDS detects traffic from the specific device and alerts the system admin to detect suspicious activities.
- APIDS (aka protocol-based detection system) is an agent that resides on a pool of servers. It monitors data traffic by interpreting communication on app-based protocols.
- CIDS (aka Hybrid detection system) is the resultant combination of one or more IDS systems. It needs system admins to configure host agents with network protocols to get a complete view of the system.

# Intrusion Detection Systems (IDS) Vs. Intrusion Prevention Systems (IPS)

Sr.No.	Intrus	sion Detecti	on System	Intrusion Prevention System				
1.	Intrusion	detection	systems	are	An intrusion prevention system is a			
	monitoring	and detecti	on tools.	prevention control system.				

2.	The tools of the Intrusion Detection System don't take action on their own.	The control system of IPS accepts and rejects the packets based on a certain ruleset.
3.	An intrusion detection system requires human intervention or another system to look at the results.	Intrusion prevention system requires regular updating of the new possible data threats.
4.	An intrusion detection system is not inline so traffic doesn't require to flow through it.	Intrusion Prevention System is inline where traffic needs to flow through it.
5.	There are two types of IDS: Network Intrusion Detection System (NIDS) and Host-based IDS (HIDS).	There are 4 types of IPS: Network- based IPS (NIPS), Wireless IPS (WIPS), Host-based IPS (HIPS) and Behavior IPS.

# How to Choose the Best Intrusion Detection System?

There is numerous intrusion detection system available in the market but to choose the best among all the available system requires a lot of research. Here we have explained various factors you need to keep in mind while choosing the best intrusion detection system. These are mentioned as follows:

- First, try to research out your business needs and systems that are available.
- Is the IDS system going to support the current network?
- Consider the budget for both IDS/IPS systems.
- Wireless/Wired network support
- What happens If something goes wrong with the current system
- Whether the system can be scaled to bigger with the existing system
- Interoperability
- Timely updates to new or modified signature for prevention/detection of threats.

# List of the Best Intrusion Detection Software

Here is the top 10 list of best intrusion detection software explained in a detailed manner as follows:

#### 1. SolarWinds Security Event Manager

SolarWinds Security Event Manager is an IDS that runs on a windows server platform. It is best for clients who are having large businesses.

ode Health - Activity det by last activity (last update: 4 minutes ago)	1	All Events - Last 12 hours All Events in Last 12 hours (last update: a few seconds ago)	1	All Events by Event Type An Events by EventType Cast update: a few tectority appl
lame	Last Event + *	1400	654 d Events	769 UserLogon
vpar-alk-test2	Never	1200 M MM		312 UserLogoff
/IN-DGT4OU7C1EA.swdey.local	10 months a	1000	001	222 MachineLogon
ab-checkpoint2200	9 months as	100	- www	222 MachineLogotf
nartin-PC.swdey.local	8 months aj	400		83 FileDataWrite
ng-brn-lem-05	8 months aj			10 Internalinfo
MnodeWin2016.engineering.lab.brno	7 months aj	02'00 08'00 09'00	12:00	7 ServiceStart
MnodeWin2016.engineering.lab.brno	7 months ap	Real Provide State		
min-PC.swdev.local	6 months aj	User Logon by User	Logon Failures by Source Machine	Logon Failures by User
N-83297LT64QL.swdev.local	ő months aj	User Logons by Destination Account (ast update: 5 minutes agh)	Falled Logons by Destination/Machine Cast update: 5 minutes ago	Failed Logons by Destination Account fast update. 5 minutes agai
SKTOP-Q185883.engineering.lab.brno	ő months aj			4
B-SSAK-2016-1.swdev.local	5 months aj	253 Administrator	AUSF501.tul.solarwinds.net	jadrandal atomicza Salesboard
g-aus-sys-350	5 months aj	STE administrator	The DCUT, tut solar winds het	Sam City
rg-aus-sys-354	5 months ag	and outprovers	110 aus-dev-dc-02 survey local	justri doharty
ng-aus-sys-351	4 months at	2000 75 ANONYMOUS LO		Distance of the second se
		57 ORIONITS	trm-dev-dc-01.swdev.local	oleksiy maktiyna
1 2 3 4 5 3 1-100	0 of 444 100 👻	53 mark.dorney	0RKGF501 tul solarwinds net	Enc Colum 5 80 100 180 200 280
les Fired by Rule Name	as ago)	Firewall Events by Type All Frenal Events by EventType (ast update: 5 minutes app)	Traffic by Destination Port     Hitsesson Traffic by DestinationPort (last update: 5 minutes april	All Events by Connector Name At Electric by TopMist Tetrupdate & minuter agol
	Iter during migrat	DataBaseAccess		THES Windows Security
	t-rule-with-mail-a	ApplicationDeni	1500	FIM File and Directory
42 integration-tes	t-rule-with-mail-a	32 ApplicationAcce		13 Windows System 10 ManagerMonitor
42 integration-tes 42 userLogon	t-rule-with-mail-a	699 6 UserAuthAudit	1000 Cohers	TriGes
42 integration-tes	t-rule-with-mail.a		400	

**Source:** https://cdn.networkmanagementsoftware.com/wp-content/uploads/5-security-event-manager-main-dashboard.jpg

#### Features:

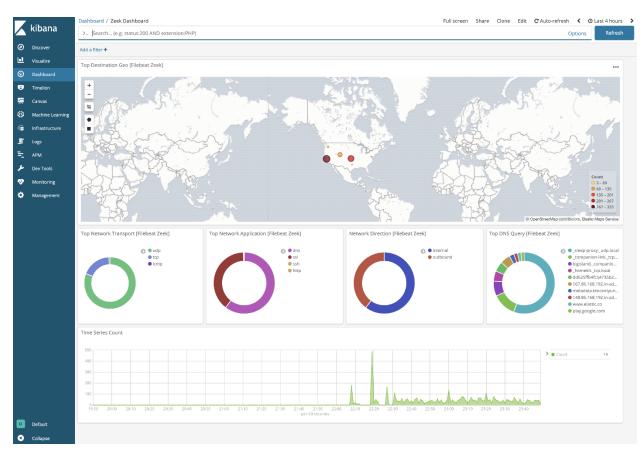
- Real-Time Monitoring
- Compliance Tracking
- Data Visualization
- User Activity Monitoring

Website: https://www.solarwinds.com/security-event-manager

Pricing: Pricing starts from \$2613 as a one-time payment with 30 days free trial.

#### Zeek

Zeek is also known as Bro which is a network-based intrusion detection system (NIDS) that operates on live traffic data. This tool can be installed freely on UNIX, Linux and Macintosh OS platforms.



Source: https://www.elastic.co/guide/en/beats/filebeat/current/images/kibana-zeek.png

#### Features:

- Open Source with a BSD License
- Analysis of Real-Time Data
- Standard Interface
- IPv6 Support

#### Website: <u>https://zeek.org/</u>

Pricing: Zeek is open-source which is available free to use.

#### OSSEC

OSSEC is an open-source Host-based Intrusion detection system that is free for usage. It can be run on UNIX, Windows, Macintosh OS and Linux platforms but doesn't have a user interface.

	Discover Visualize Dashb	oard Setti	ngs		Last 7 days 🤆
•				Q D D	a d C 💿
AJ	erts Over Time			✗ ★ Top 10 Alerts	
	00			Legend Ø • Count	Legend C 1002
	40				<ul> <li>5501</li> <li>5502</li> <li>5710</li> </ul>
	2015-09-16 17:00 201	15-09-18 05:00	2015-0	9-19 17:00 2015-09-21 05:00	9 591
		@time	stamp per 3	3 hours	• 5503
			^	^	•
	ert Details			« 1 2 3 4 58 »	
	Time +	Alert_Level	Rule	« 1 2 3 4 58 » Details	Description
		Alert_Level	<b>Rule</b> 5502		
•	Time 🗸	3		Details	Description
	Time - September 22nd 2015, 16:40:40.390	3	5502	Details Sep 22 16:38:41 r5-9-29 sshd[10262]: pam_unix(sshd:session): session closed for user vic Sep 22 16:20:42 r5-9-29 sshd[10262]: Accepted publickey for vic from 10.30.172.28 port 58888	Login session closed.
	Time - September 22nd 2015, 16:40:40.390 September 22nd 2015, 16:22:44.407	3 3 3	5502 5715	Details           Sep 22 16:38:41 r5-9-29 sshd[10262]: pam_unix(sshd:session): session closed for user vic           Sep 22 16:20:42 r5-9-29 sshd[10262]: Accepted publickey for vic from 10.30.172.28 port 58888 ssh2           Sep 22 16:20:42 r5-9-29 sshd[10262]: pam_unix(sshd:session): session opened for user vic by	Description Login session closed. SSHD authentication success.
	Time - September 22nd 2015, 16:40:40.390 September 22nd 2015, 16:22:44.407 September 22nd 2015, 16:22:44.407	3 3 3 3	5502 5715 5501	Details           Sep 22 16:38:41 r5-9-29 sshd[10262]: pam_unix(sshd:session): session closed for user vic           Sep 22 16:20:42 r5-9-29 sshd[10262]: Accepted publickey for vic from 10.30.172.28 port 58888 ssh2           Sep 22 16:20:42 r5-9-29 sshd[10262]: pam_unix(sshd:session): session opened for user vic by (uid=0)	Description Login session closed. SSHD authentication success. Login session opened.

#### Source: https://vichargrave.github.io/assets/images/final-dashboard.png

#### Features:

- It is open source
- Log Based IDS
- Active Response
- Malware and Rootkit Detection

Website: https://www.ossec.net/

**Pricing:** As it is open-source it is free to use.

#### Fail2Ban

Fail2Ban is a lightweight and free Intrusion prevention system that runs on the command line interface and is available on UNIX, Macintosh OS and Linux platforms.

🔻 cyril@	earth:∼	_ 🗆 ×
<u>File</u> <u>E</u> dit	<u>V</u> iew <u>T</u> erminal	Ta <u>b</u> s <u>H</u> elp
02/18/05	23:03:57.936	INFO Fail2Ban v0.3.0-CVS is running
02/18/05	23:03:59.065	INFO Ban 62.94.10.80
02/18/05	23:08:19.221	INFO Restoring iptables
02/18/05	23:08:19.224	INFO Unban 62.94.10.80
02/18/05	23:08:19.238	INFO Exiting
02/18/05	23:12:16.017	INFO Fail2Ban v0.3.0-CVS is running
02/18/05	23:38:43.211	INFO Restoring iptables
02/18/05	23:38:43.213	INFO Exiting
02/18/05	23:45:11.090	INFO Fail2Ban v0.3.0-CVS is running
02/19/05	12:01:32.866	INFO Ban 66.139.75.25
02/19/05	12:11:33.871	INFO Unban 66.139.75.25
02/19/05	12:29:45.734	INFO Ban 66.139.75.25
02/19/05	12:39:46.656	INFO Unban 66.139.75.25
02/19/05	22:12:27.553	INFO Ban 69.10.152.217
02/19/05	22:22:28.475	INFO Unban 69.10.152.217
02/20/05	03:40:57.450	INFO Ban 219.147.179.93
02/20/05	03:50:58.408	INFO Unban 219.147.179.93
02/20/05	06:37:21.951	INFO Ban 211.43.24.222
02/20/05	06:47:22.872	INFO Unban 211.43.24.222
02/20/05	11:35:54.693	INFO Restoring iptables
02/20/05	11:35:54.696	INFO Exiting
02/20/05	12:12:17.195	WARNING Fail2Ban v0.3.0-CVS is running
earth ro	ot #	
		il2ban earth: 0.00 0.03 0.00 20/02 14:44

Source: https://upload.wikimedia.org/wikipedia/commons/7/7b/Fail2ban\_screenshot.jpg

Features:

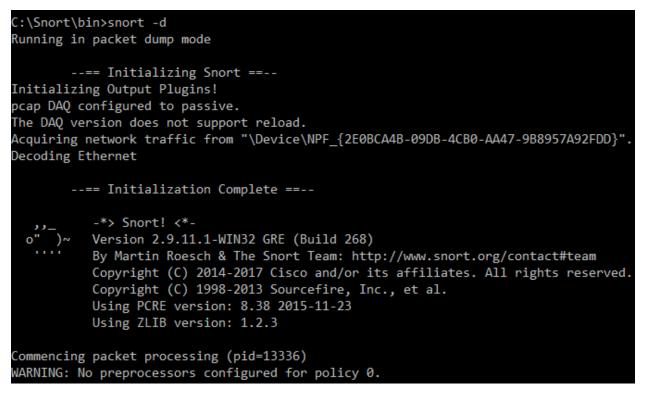
- Log File Analysis
- Open Source
- Automatic blocking of suspicious IP addresses
- Compatible with Unix and Macintosh OS Systems

Website: http://www.fail2ban.org/wiki/index.php/Main\_Page

**Pricing:** It is open-source that is free to use.

#### Snort

Snort is a well-known Network-based Intrusion Detection/Prevention System that has a huge community of users. It is widely accepted as many other available Intrusion detections and Prevention systems are built to be compatible with it.



Source: https://www.itprc.com/wp-content/uploads/2018/06/snort.png

#### Features:

- Open Source
- Cross platform which runs on all operating systems.
- Huge library of prebuilt detection rules.
- Rules can be easily implemented.

#### Website: https://www.snort.org/

**Pricing:** Snort is free to use but the rule subscriptions starts from \$29.99 for personal use to \$399 for business use annually for both of them.

#### Kismet

Kismet is a wireless network detector, packet sniffer and IDS which is different from other wireless network detectors. It is the most widely used open-source wireless monitoring tool.

		🗊 🗋 loca	alhost:2501/#					©	∂ ✿	III\ 🗊 🔹
Kismet									h	. 💠 🔼 96% (
Devices SSIDs	ADSB Live									
All devices	•								Search:	
Name	Туре	Phy	Crypto	🔶 Signal	Channel	Data Packets	Clients	BSSID	QBSS Chan Usage	QBSS Users
6A:EA:1D:D1:32:78	Wi-Fi Bridged	IEEE802.11	n/a	n/a	6	106.83 KB	0	C4:EA:1D:D1:32:79	n/a	n/a
00:E0:4C:68:03:31	Wi-Fi Bridged	IEEE802.11	n/a	n/a	1	1.75 MB	0	02:6A:E3:EA:40:88	n/a	n/a
04:C9:D9:6A:DE:0F	Wi-Fi Bridged	IEEE802.11	n/a	n/a	1	62.06 KB	0	E0:B9:E5:89:3B:B6	n/a	n/a
0 devices										>
ssages Channe	ls 🖉									
		EN Source wix984f	3276d964d successfully	re-opened						
<u>~</u>	55 SOURCEOP									
n 24 2021 21:37		1964d finished confi	iguring kismon0, ready t	o capture						

Source: https://upload.wikimedia.org/wikipedia/commons/f/f2/Kismet\_Web\_UI.png

#### Features:

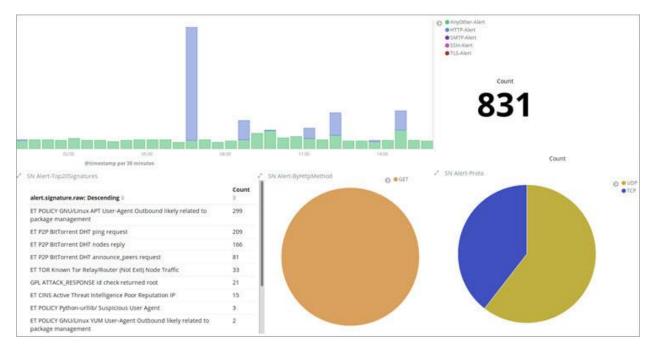
- Open Source Wireless Monitoring Tool
- 802.11 Packet Sniffers
- Client/Server Model Architecture
- Runs on FreeBSD, Linux, NetBSD, OpenBSD and Macintosh OS.

Website: https://www.kismetwireless.net/

**Pricing:** It is open source free software that is distributed under the GNU General Public License.

#### Suricata

Suricata is an open-source network detection engine that is capable of inline intrusion prevention, offline pcap processing, network security monitoring and real-time intrusion detection.



### **Source:** https://www.softwaretestinghelp.com/wp-content/qa/ uploads/ 2019/12/ Suricata.jpg

#### Features:

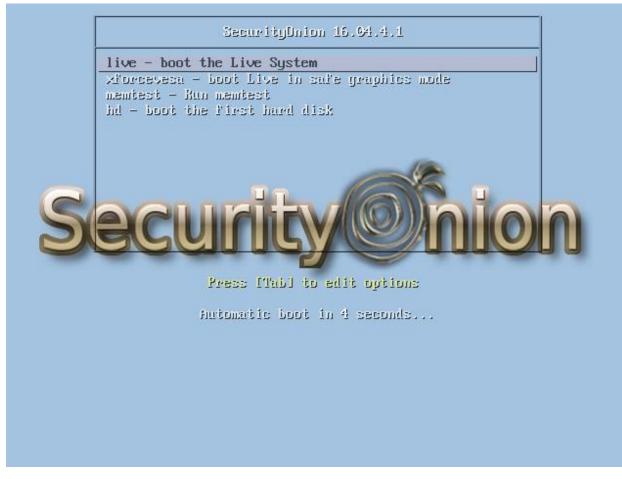
- Open Source
- Lua Scripting
- Automatic detection of protocol
- Integrates easily with the network and can be embedded within numerous opensource and commercial solutions.

#### Website: https://suricata.io/

Pricing: It is freely available to use.

#### **Security Onion**

Security Onion is a free open source Linux-based distribution system that combines with other security tools and intrusion prevention systems within the custom-made Linux distribution. This tool includes such as Zeek, Snort, Suricata and other open source security tools.



Source: https://www.itprc.com/wp-content/uploads/2018/06/security-onion.png

#### Features:

- Network Security Monitoring
- Log Management
- Open Source Linux Distribution
- Integrates with multiple tools.

#### Website: https://securityonionsolutions.com/

**Pricing:** It is open-source IDS that is available free to use.

#### Sagan

Sagan is an open-source free Intrusion Prevention System that mines log files for event data. It can be run on various platforms like Linux, Macintosh OS and UNIX.

< 2012 Ja i01 Sat02 Sun03 N			Mar Fri08 Sat	Apr 09 Sun10	May Mon11 Tue12	Jun Wed13 Thu14 <b>Fri1</b>	Jul         Aug         Sep         Oct           5         Sat16         Sun17         Mon18         Tue19         Wed20         Thu21         Fri22         Sat23	Nov 3 Sun24 Mon25 T	Dec ue26 Wed27	2014 > 4
:00 1:00 2:0		4:00 5:0		7:00	8:00 9:00	10:00 11:00		8:00 19:00 2		22:00 23:0
	limelin	e: 2013-11-1	5 00:00:00	until 201	3-11-15 23:59:	9 (+00:00) Fil	tered by Object: NO Filtered by Sensor: NO	Status: Synchro	nized	
oggle							98.1%			1.9%
vent Grouping:	on	QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
vent Queue Only:	on									
lap:	off	4	4	1		23:16:57	[OPENSSH] No identification string - possible scan	5000070	6	0.008%
vent Summary		18	1	1		11:56:10	[OPENSSH] Invalid or illegal user [oracle]	5001113	6	0.037%
Queued Events:	211	20	1	1		11:55:33	[OPENSSH] Invalid or illegal user [guest]	5001109	6	0.041%
Total Events:	49142									
Fotal Signatures:	15	26	1	1		11:54:31	[OPENSSH] Invalid or illegal user [admin]	5001107	6	0.053%
Total Sources: Total Destinations:	-	19	1	1		11:54:26	[OPENSSH] Invalid or illegal user [webmaster]	5001118	6	0.039%
	-	25	1	1		11:54:16	[OPENSSH] Invalid or illegal user [test]	5001115	6	0.051%
vent Count by Pri		17	1	1		11:54:15	[OPENSSH] Invalid or illegal user [postgres]	5001114	6	0.035%
High:	207 (98.1%)			-		11.5 1.15		5001111	•	
Medium:	-	15	1	1		11:53:36	[OPENSSH] Invalid or illegal user [info]	5001110	6	0.031%
.ow: Other:	4 (1.9%)	12	1	1		11:52:52	[OPENSSH] Invalid or illegal user [web]	5001117	6	0.024%
		15	1	1		11:11:43	[OPENSSH] Invalid or illegal user [user]	5001116	6	0.031%
Admin Access:	ssification	2	1	1		11:06:44	[OPENSSH] Attempt to login using a denied user	5000077	6	0.004%
User Access:	-	2		-		11.00.44	[OPENSSIT] Attempt to login using a denied user	300077	0	0.004%
Attempted Access:	-	6	1	1		10:57:29	[OPENSSH] Invalid or illegal user [nagios]	5001112	6	0.012%
Denial of Service:	-	20	3	1		10:20:02	[OPENSSH] Invalid or illegal user	5000022	6	0.041%
Policy Violation	-	4	2	1		10:20:02	[OPENSSH] Invalid or illegal user [a]	5001106	6	0.008%
Reconnaissance:	-	8	1	1		10:20:02	[OPENSSH] Failed password - Brute force	5001646	6	0.016%

Source: https://securityonline.info/wp-content/uploads/2017/09/sagan.png

#### Features:

- Open Source
- It is lightweight
- Compatible with Snort data
- Integrated with multiple third-party tools.

Website: https://quadrantsec.com/sagan\_log\_analysis\_engine/

Pricing: It is open source so it is free to use.

#### **McAfee Network Security Platform**

McAfee Network Security Platform is not an open-source network intrusion detection system. It comes with very high pricing as compared to others with focused development, support access and other benefits which are not available with other freeware open-source systems.

NSM 10.1.7.29	1								Adm	inistrator 🛔	/My Company	GMT-04.00
McAfee	Dashboard	Analysis	음 Policy	E Devices	🖨 Manager							0
Domain: 7My Comp.	any je									Last 7 day	n	
Attack Severity Su			00	Top Callback Activity			00	Manager Summary				00
0				0				0				
High	10436							Manager Software Version	10.1.7.29			
Medium	3627							Last Reboot	2020-Sep-23 17:	0:25 GMT-0	4:00	
low								Central Manager Synchronization				
Informational								Hostname	W2K12R2-223 (1	0.71.100.223		
Attacks Over Time			60	3ve				Product Registration	Registered			
ALLACKS OVER TIME												
0								Signature Set	😔 10.8.13		10.8.13.1	p
12000			-					Callback Detectors	2749		2749	
0000												
				Top Malware Files			00	1 Administrator	10.248.252.1	0 2	2020-Sep-24 0 14:00	:34:03 GMT-
				0								
				/collectmail.pdf/7331	44140-25-552212							
					idEdge/FileFormatSa	494		System Faults				00
				/collectmail.pdf/a4bf	70bdfa21192c1b33			0				
2020-Sep-17 06:21	2020-Sep-19 08:45	2020-Sep-21 11:09	2020-Sep-23 13	Avtest32.exe/e2cfe1c89		200						
	High Medium	Low Informational		/ATD/NTBA_GAME_te	st_files/multiple_ma			Manager	Up			
fop Targets			00	/SWF/pillow.swf/16b04		198						
0				/xorshellcode.doc/000	637763e81950cf53			AWS-Clust-10.70.1.123	3 Active	0		0
					info.pdf/112d699c1	100		AWS-Clust-10.70.1.199		0		
172.16.232.9			1,092	Artest/v_yodascrypto	r11.exe/316a4c0ab			AWS-Clust-10.70.1.23	Active	0		
10.40.39.22		768		Top Risky URLs			00	mcafee-ips-01 mcafee-ips-02	Active	0 0		0
0.00.00	9 🙂 😁	761						market int 62	1000			

**Source:** <u>https://gdm-catalog-fmapi-prod.imgix.net/ProductScreenshot/163c4b91-7231-</u>4e1c-a211-a44e78953941.png?ixlib=react-9.0.3&ch=Width%2CDPR&auto=format

#### Features:

- Easy to use
- Network Traffic Inspection
- Network Analysis with extended Botnet Intrusion Detection.
- Advanced protection against threats.

Website: <u>https://www.mcafee.com/enterprise/en-us/products/network-security-platform.html</u>

**Pricing:** It is highly expensive that starts from \$10,995.

sst Plagiarism Checker - 100% Free 🗆 🗙 🕂						- 0 ×
← → C				✔ Video To Gif	₿ ✿	* 🕵 E
SALE 20 FLAT 41 DISCOUN	% Deep S	earch 🚺 No Ads 🕞 Reports	읝 User Seats Click here			
		RESULTS				- 1
100% Com	npleted: 100% Checked		0% Plagiarism 100% Unique			
			 → +-			
Sente	nce Wise Result	Document View	Matched Sources			
Unique	Review on Intrusion De	tection and Intrusion Prevention Systems	S			
Unique	IDS is a system that me	onitors traffic for suspicious activities.				
Unique	It issues alerts on deter	cting suspicious system behavior.				
Unique	Any malicious program	or lines of code get reported to the admi				
Unique	Although IDS triggers a	elerts for suspicious activities, it often get	s exposed to false threats.			
Unique	It is the reason why an	IT firm needs to fine-tune IDS when it ins	stalls the software.			
Unique	An intrusion detection s	system assesses network traffic and insp	ects signs of possible cyber-attacks.			0
🚳 🙆 📋 🖸 🚺	wii s		Not		📑 at 🌗	12:48 PM 30-Dec-21

Factor	Author's Rating (1-5)	Publisher Rating (1-5)
<ol> <li>Is this content better than the top 10 results for the given keyword?</li> </ol>	4	
<ol><li>Does this content have a better format, point of view and outline than the top 10 results?</li></ol>	4.5	
3. Does this content have any data points to back up your statements?	4	
4. Does this content cover all the related queries and questions available in the search results?	5	
<ol> <li>Did you avoid superfluous content and made your point straight, easily understandable and useful for the reader?</li> </ol>	5	