Idappcom and Endace

Detect and remediate the most challenging cyber threats across your network.

Idappcom and Endace solutions combine for scalable threat detection, accelerated response to security events and reduced threat exposure.

Idappcom's Distributed Rules Manager (DRM) is a rules-management platform that streamlines and automates rule management across large deployments of Intrusion Detection or Prevention Systems (IDS/IPS). Using rule deployment policies, customers can automatically deploy the appropriate rules to the right locations, reduce false positives and ensure accurate detection of the very latest exploits.

Combining access to multiple SNORT®, and SNORT-format, rule databases with editing, testing and provisioning capability, DRM enables rapid alert assessment and vulnerability remediation to help maintain maximum network and data protection.

EndaceProbe[™] Network Analytics Platforms capture, index and store network traffic with 100% accuracy, regardless of network speeds, loads or traffic types. The EndaceProbe's built-in hosting environment, Application Dock[™], extends security and performance monitoring by allowing Idappcom-managed SNORT instances to be hosted on the open EndaceProbe platform. Hosted SNORT instances can analyze recorded traffic in real-time at full line-rate, or analyze recorded, packet-level Network History for back-in-time investigation.

Streamlining Security Investigations

The Network History recorded by EndaceProbes is integrated with Idappcom's DRM using the Pivot-To Vision™ function of the EndaceProbe's powerful API.

Pivot-To-Vision lets security analysts pivot from DRM threat alerts directly to EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the related, packet-level Network History. Using the IP address and time range of the trigger, Pivot-To-Vision focuses the analyst directly on pre-filtered incident data. EndaceVision lets analysts extract, dissect and review the relevant traffic from the terabytes of Network History recorded by EndaceProbes on the network. It enables analysis to microsecond level with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, allowing rapid insights and accurate conclusions.

Being able to get directly to the related packets lets security analysts quickly and conclusively establish the root cause of issues and respond appropriately, dramatically reducing the time to investigate and resolve

Mappcom

PRODUCTS

- Idappcom Distributed Rules Manager
- Idappcom Managed SNORT IDS
- EndaceProbe with Application Dock

BENEFITS

- Detect threats across your network, anywhere you deploy an EndaceProbe
- Easily manage IDS policy and rulesets from multiple sources across your distributed network
- Respond to and remediate incidents quickly and efficiently with streamlined investigation workflows.
- Rapid, conclusive and actionable investigations with drill down to packet level detail.
- Catch zero day exploits by replaying network history through updated rulesets.
- Reduced threat exposure through greater analyst productivity and faster incident investigation.
- Definitive evidence trail with an accurate record of all relevant packets.
- Increased awareness and remediation of False Positive Alerts

critical incidents.

Scaling IDS Deployment with DRM and Application Dock

Idappcom-managed SNORT deployments can be hosted on the EndaceProbe in Application Dock. Every packet captured and recorded by the EndaceProbe can also be simultaneously streamed to these hosted, Idappcom-managed SNORT instance in real-time.

Security Operations teams can dynamically deploy managed SNORT

© Copyright Endace Technology Limited, 2017. All rights reserved. Information in this data sheet may be subject to change. END_fp_end_idappcom_1.0 anywhere on the network that they have EndaceProbes deployed, allowing them to increase their detection footprint on demand with no additional hardware installs.

EndaceProbes are designed to ensure system resources used for capture and recording are separated from the resources used by hosted applications. This means capture performance is never impacted by hosted applications and vice-versa, guaranteeing 100% accurate recording even when Idappcom-managed SNORT instances are processing heavy traffic loads.

Conclusion

Using Idappcom DRM and integrating Network History into Idappcommanaged SNORT instances delivers comprehensive security detection and deep contextual insight that accelerates the investigation of, and response to, security issues.

And, by deploying Idappcom-managed SNORT instances to EndaceProbes in Application Dock, security teams can extend their reach easily, leveraging existing EndaceProbe hardware deployments to extend security monitoring and network recording capability.

The combined Endace and Idappcom solution provides improved security posture, reduces threat exposure and accelerates incident response with definitive evidence.

Home	File View											
Create New Rule Rules Library	MESSAGE	•	CONTAINS	~ Mahu	sre		•	Filter				
	Signature ID	Revision	Action	Protocol	Source Network	Source Port	Destination Network	Destination Port	Rule Body			
	3082	9	alert	tcp	SEXTERNAL_NET	any	SHOME_NET	5880	mog: MAEWARE-BACK			
Policies	3083	9	alert	tcp	SHOME_NET	\$880	SEXTERINAL_NET	any	msg:'MADWARE-BACK			
	5805 13		alert	top	SHOME_NET	any	SEXTERINAL_NET	SHITP_PORTS	msg:'MADWARE-OTHE			
Sensors	5880	6	alert	tcp	SHOME_NET	any	SEXTERINAL_NET	25	msg:'MAUWARE-OTHE msg:'MAUWARE-OTHE			
	5881	9	alect	tcp	SHOME_NET	any	SEXTERINAL_NET	21				
Systog	5882	7	alert	tcp	SHOME_NET	any	SEXTERNAL_NET	25	mog: MAUWARE-OTHE			
Local IDS	\$907						SEXTERNAL NET	rummonan .	THE MACWARE OTHE			
	5908	8	alert	top	SHOME_NET	any	SEXTERNALINET	Clone Gathle Edit in Rules	a MAEWARE-OTHE			
Web Browser	5909	11	alert	tcp	SHOME_NET	any	SEXTERINALINET		Editor MAEWARE-OTHE			
Web Test Tool	7091	6	alect	tcp	SHOME_NET	5555	SEXTERINAL_NET	Chable	F MADWARE-BACK			
	7096	5	alect	tcp	SEXTERNAL NET	any	SHOME,NET	Copy Copy Celete	C'MAUNARE-BACK			
Base64 Decoder	7097	5	alert	tcp	SEXTERNAL NET	any	SHOME_NET		STMAUWARE-BACK			
	7098	5	alert	tcp	SEXTERNAL_NET	any	SHOME,NET		TMAEWARE-BACK			
Lops	7099	5	alert	top	SEXTERNAL_NET	any	SHOME_NET	Change Action	p:'MADVARE-BAC p:'MADVARE-BAC			
	7104	8	alert	top	SEXTERNAL MET	any	SHOME,NET	Group into a Policy				
Services	7105	6	alect	tcp	top SHOME_NET 30029 SEXTERNAL_NET		Congreup from a Peacy	C'MAUNARE-BACK				
	7108 6		alect	tcp	SHOME_NET	777	SEXTERINAL NET	Support information	TMALWARE-BACK			
	7111	8	alert	tcp	SEXTERNAL_NET	any	SHOME,NET	any	msg:'MADWARE-BACK			
	7112	6	alert	tcp	SHOME_NET	any	SEXTERMAL_NET	any	msg: MAEWARE-BACK			
	7113	8	alert	tcp	SEXTERNAL_NET	any	SHOME_NET	23476	msg:'MADWARE-BACK			
	7114	6	alert	tcp	SHOME_NET	23476	SEXTERNALINET	any	mog: MADWARE-BACK			
	7115	6	alert	tcp	SHOME_NET	any	SEXTERINAL_NET	any	msg:'MADWARE-BACK			
	7114		atest	1.00	THOMAS HET	-	CEVTERNAL NET	ENTER DODTE				

Idappcom DRM manages Rules across multiple SNORT deployments running on EndaceProbes

P Distributed Rules	Manager							-	
Home	File View Options								84
Crasta New Pula	Tine Game V	Sensor IP	Senior Hostname	Message	Cirl - Sid - Rev	Source IP - Port	Destination IP: Part	Metthere	Saus
create ment part	21 November 2017 11:02:17	10.2.2.102	1004-041-00002	TO 499,2013 ArtExt 5.01 (RESOL RAW Server Buffer Overflow Vol.)	1-8003251-2	\$5521801	555511000	DO-469-2015-4	
Rules Library	21 November 2017 11:04:17	10.2.2.101	sec.et	BO 498-3015 ArtEau 5.01 (BESOK RAW Server Buffer Overflow Vol.	1-8008251-2	5552-1301	555511000	TO-469-2019-4	
	21 November 2017 11:04:17	10.2.2.101	second adds_000001	TO 499, 3011 Artifax 5.01 (BENDS RAW Server Buffer Overfilms Vot	1-8008252-2	5552-1241	555511001	10.409.3015-4	
Policies	21 November 2017 11 04-17	10.2.2.102	sead.ids.00002	TO. 409, 2013: ArtEau S.01 (BERDS) BAW Server Buffer Overflow Vol.	1-8003252-2	5557-1241	5.5.5.511001	DO-469-2019-4	
	21 November 2017 11:00-17	10.2.2.102	separate 00002	TIC. 499-3013: ArtEar S.01 (DEROS' RAW Server Buffer Overflow Vol.	1-8003253-2	55571243	5.5.5.511001	00.469.3013-4	
5405015	21 November 2017 11:04:17	10 2 2 101	stort.41-00001	TID APR 2015 Arthur 5 01 (02505) RAW Sever Buffer Overfilmer Ind	1.000111.0.7		555911001	00.400.0011.4	
Systog	21 November 2017 11:04:16	10.2.2.102	snort-ids-00002	TIC-MAR-2008: Acronis True Image Echo Group Server Ren	Rule		\$555	TIQ-M4R-2008	5.5.5
	21 November 2017 11:00:16	10.2.2.101	100000000000000000000000000000000000000	IRO MAR 2008: Access Taxe Image Echo Group Server Res	Idress Lookup		5555	TO.448.2008	
Local IDS	21 November 2017 11 00 16	10.2.2.102	seo#.44.00002	BCAMAR-2008 Access Taxe Image Windows Assed NULL	ihark" Filter	13	5.5.5.9826	TO MIR 2008	5.5.5
	21 November 2017 11:04:16	10.2.2.101	snort-ids-00001	TIQ-MAR-2008: Acronis True Image Windows Agent NULL	ce" Pivot to Vision	13	5.5.5.59876	TIQ-M4R-2008	5.5.
Web Browser	21 November 2017 11.04.16	10.2.2.102	snort-ids-00002	TIQ.APR-2013: ActFax 5.01 "@F506" RAW Server Buffer Ove			5.5.5.5.11000	TIQ-APR-2013: A	5.5.
Web Test Tool	21 November 2017 11:04:16	10.2.2.101	snort-ids-00001	TIQ-APR-2013: ActFax 5.01 "@F506" RAW Server Buffer Overflow Vul-	1.8003250.2	\$5571300	5.5.5.5:11000	TIQ-APR-2013: A	5.5.5
	21 November 2017 10.05:18	10.2.2.102	snort-ids-00002	error Could not load host keys /etc/ssh/ssh. host. dsa. key				error Could not	
Base64 Decoder	21 November 2017 10:03:48	10.2.2.101	short-ids-00001	TIQ-MAR-2008: Acronis True Image Windows Agent NULL Pointer R.,	1:7002101:2	5.5.5.1:1693	5.5.5.99876	TIQ-M4R-2008	\$.5.5
	21 November 2017 10:03:48	10.2.2.102	snort-ids-00002	TIQ-MAR-2008: Acronis True Image Windows Agent NULL Pointer R	1:7002101:2	5.5.5.1:1693	5.5.5.59876	TQ-M4R-2008	\$.5.5
Logs	21 November 2017 10:03:48	10.2.2.101	snort-ids-00001	TIQ-APR-2013: ActFax S.01 "@F506" RAW Server Buffer Overflow Yul	1:8003250:2	5.5.5.7:1300	5.5.5.5:11000	TQ-APR-2013: A	5.5.5
	21 November 2017 10:03:48	10.2.2.102	snort-ids-00002	TIQ-APR-2013: ActFax 5.01 @F506' RAW Server Buffer Overflow Vul	1:8003250-2	\$.5.5.7:1300	5.5.5.5.11000	TQ-APR-2013: A	5.5.
services	21 November 2017 10:03:48	10.2.2.102	snort-ids-00002	TIQ-APR-2013: ActFax 5.01 "@F506" RAW Server Buffer Overflow Vul	1:8003251:2	5.5.5.7:1301	5.5.5.5:11000	TQ-APR-2013: A	5.5.1
	21 November 2017 10:03:48	10.2.2.101	snort-ids-00001	TIQ-APR-2013: ActFax 5.01 @F506' RAW Server Buffer Overflow Vul	1:0003251:2	\$.\$.\$.7:1301	5.5.5.5:11000	TIQ-APR-2013: A	5.5.
	21 November 2017 10:03:48	10.2.2.101	snort-ids-00001	TIQ-APR-2013: ActFax 5.01 @F605' RAW Server Buffer Overflow Vul	1:0003252:2	5.5.5.7:1241	\$.5.5.5:11001	TIQ-APR-2013: A	5.5.5
	21 November 2017 10:03:45	10.2.2.102	snort-ids-00002	TIQ-APR-2013: ActFax 5.01 "@F605" RAW Server Buffer Overflow Vul	1:8003252:2	5.5.5.7:1241	\$.5.5.5:11001	TIQ-APR-2012: A	5.5.5
	21 November 2017 10:03:45	10.2.2.101	snort-ids-00001	TIQ-APR-2013: ActFax 5.01 (@F605' RAW Server Buffer Overflow Vul	1:8003253:2	5.5.5.7:1243	\$.\$.5.5:11001	TIQ-APR-2013: A	5.5.
	21 November 2017 10:03:45	10.2.2.102	snort-ids-00002	TIQ-APR-2013: ActFax 5.01 '@F605' RAW Server Buffer Overflow Vul	1:8003253:2	5.5.5.7:1243	\$.5.5.5:11001	TIQ-APR-2013: A	5.5.5
	21 November 2017 10:03:47	10.2.2.101	snort-ids-00001	TIQ-MAR-2008: Acronis True Image Echo Group Server Remote Deni	1:7002100:2	5.5.5.1	\$3.5.5	TIQ-MAR-2008:	5.5.5
	21 November 2017 10:03:47	10.2.2.102	snort-ids-00002	TIQ-MAR-2008: Acronis True Image Echo Group Server Remote Deni	1:7002100:2	\$.5.5.1	\$.5.5.5	TIQ-MAR-2008:	5.5.5
	21 November 2017 09:58:07	10.2.2.102	snort-ids-00002	TIQ-MAR-2011 (SCADA): 7t Interactive Graphical SCADA System Me	1:7004353:2	5.5.5.1:1535	5.5.5.520222	TIQ-MAR-2011 (5.5.5
	21 November 2017 09:58:07	10.2.2.101	snort-ids-00001	TIQ-MAR-2011 (SCADA): 7t Interactive Graphical SCADA System Me	1:7004353:2	5.5.5.1:1535	5.5.5.5.20222	TIQ-MAR-2011 (5.5.5
	21 November 2017 09:58:06	10.2.2.101	snort-ids-00001	TIQ-APR-2012 (SCADA): 7T Interactive Graphical SCADA System 'ListA	1:7004500:1	5.5.5.7:3682	5.5.5.5:12401	TIQ-APR-2012 (5	5.5.5
	21 November 2017 09:58:06	10.2.2.102	snort-ids-00002	TIQ-APR-2012 (SCADA): 7T Interactive Graphical SCADA System 'ListA	1:7004500:1	5.5.5.7:3682	5.5.5.5.12401	TIQ-APR-2012 (5	5.5.5
	21 November 2017 09:58:06	10.2.2.102	snort-ids-00002	TIQ-MAR-2011 (SCADA): 7t Interactive Graphical SCADA System Buff	1:7004352:2	5.5.5.1:1088	5.5.5.5:12401	TQ-MAR-2011 [5.5.5

From DRM alerts, operators can pivot directly to EndaceVision to analyze related packet history

critical A	lert Investi	gation	,						ъ	Layout +	Tools +	Send	• =
1 Source appqa-	114-02 RotF		,	iter Directionie	ss IP is 192 0 0 0	8		Time 30	sers; 6	hours ago		Cancel	Apply
Traffic Brea	akdown				Undo 🖸 🖸 🔳	Bandwid	th					Undo D	c =
	By Appli	ation		•		Note. Filters a	ere no	t applied to this tool					
Top	10 ordered by Bits F	er Second				1,50084-					Burners (100	and an fa	- delichte
1.50054					2.08								
ž			10	e udo	1.08	1,000 4		******	***	*****	****		
E 1.000M	_		10	0 100	364 MB	500M-							
1 10CM		-	10	 951 	312 MB								
a			8	psec	81 MB	23	48:20	23	1:48:10 T	in date	21:48:4	0	
UN	23-48-30	23-48-45	8	e np	49 MB					ine const			
	Time (UTC)		0	 smtp 	33 MB								
					-	Convers	atio	ns				Undo D	C ≣.
CP Flags					Undo 🖸 🖸 🗮	•		By IP A	dress	•	0		
4/10					Ala 111 001								
			-	 All TOP det SYN 	40.627	IPs						Packets	
1				SYN ACK	39.725	Host A		Host B	Sess	ions Di	ration	Total	A*8
5			0	ACK	110,406	192 168 10	28	192 168 10 123	19	81	\$	69,028	68,724
_		_	8	PSH-ACK	52,320	192.168.10	24	192.168.10.123	20	31	\$	69,576	59,099
04	23:40:30	23:48:45	Θ	FIN-ACK	40,658	192.168.10	16	192.168.10.119	24	31	5	69,576	59,105
	Time (UTC)		8	RST	8,059	+ 192.168.10	19	192.168.10.122	22	31	8	50,170	49,505

EndaceTM, the Endace logo and DAGTM are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA). EndaceVision and EndacePackets let analysts dissect traffic and draw accurate conclusions

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com

page 2