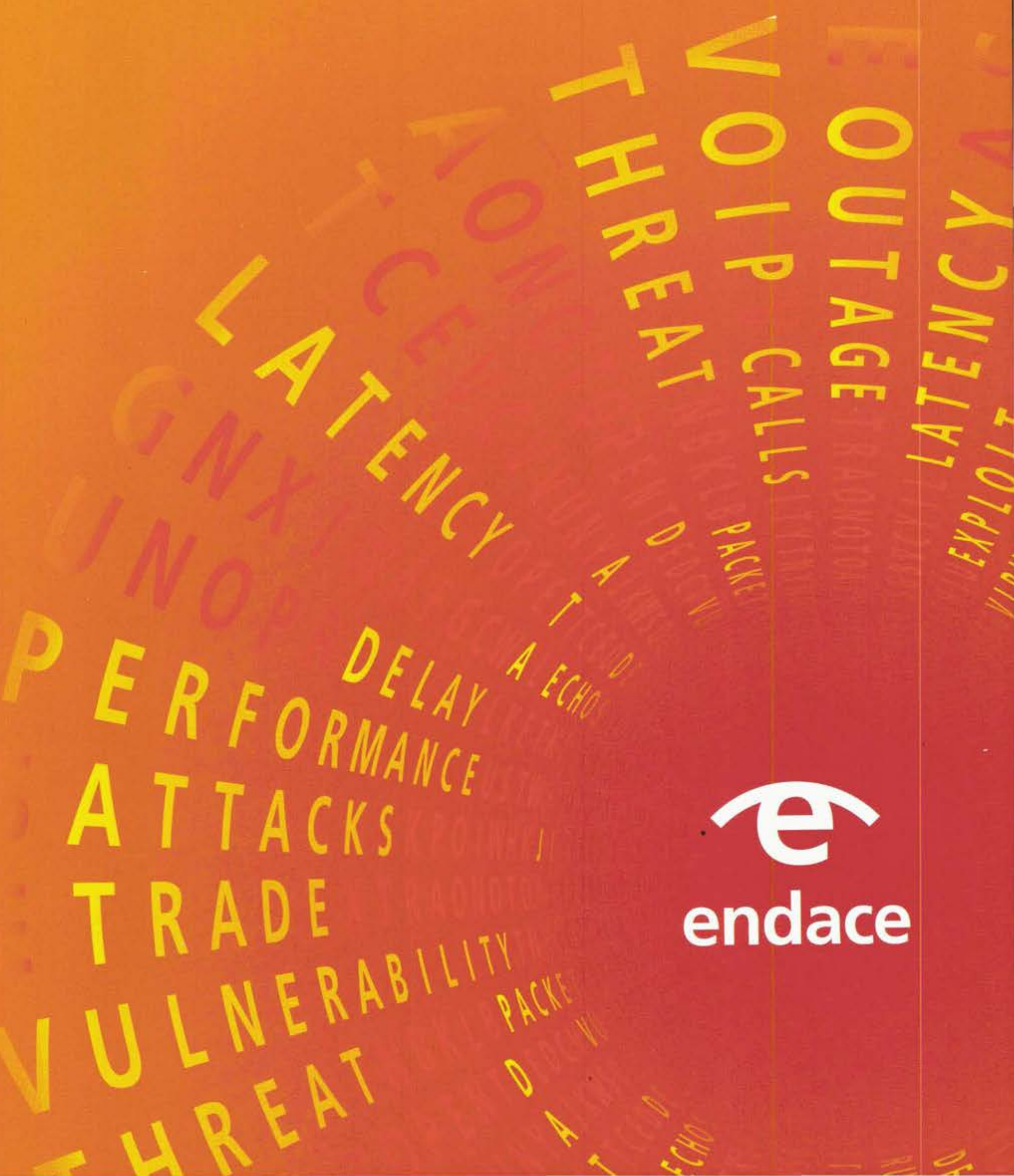
Cyber Security

What every organisation needs to know about Network Monitoring and Recording

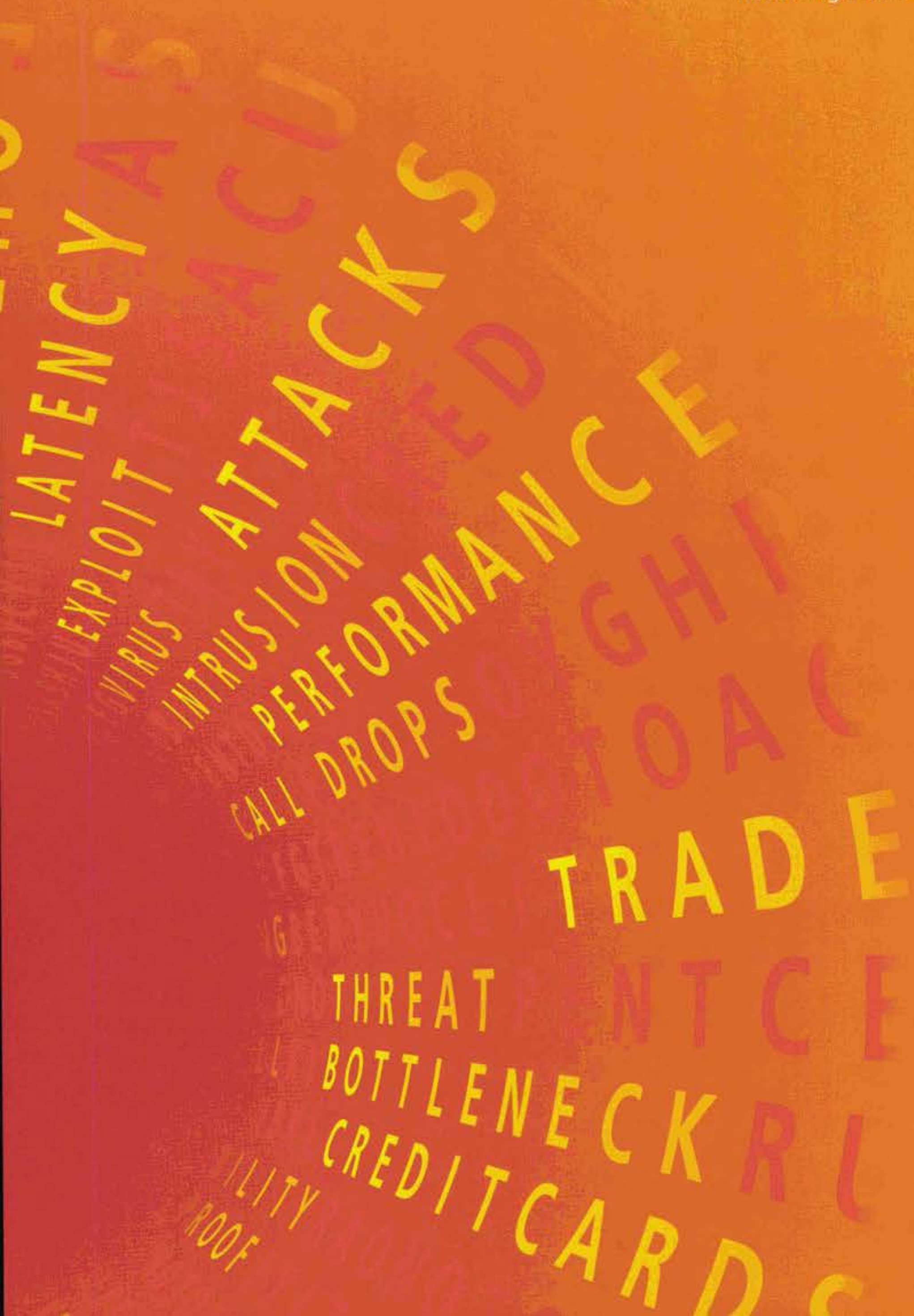


endace

Welcome to Endace

We're a world leader in network monitoring and recording. We've been helping government agencies, banks, telcos, utilities and large enterprises to help protect some of the fastest, most complex and critical networks in the world for more than 10 years. Organisations turn to Endace when the potential consequences of cyber attack are catastrophic.

Whether it's new malware, viruses, trojans or APTs the cyber threat landscape is changing by the day. If your network is critical to your business and you're operating at one, or ten gigabits-per-second, then you should consider deploying an Endace Monitoring and Recording Fabric to monitor and protect it.



Cyber Security Monitoring

In today's world, every organisation is exposed to the risk of cyber attack and data loss. With the network now being critical to almost every organisation, business leaders have an absolute obligation to protect customer information, corporate IP and the integrity of the network – because the consequences of not doing so are extremely serious. The days of tick-box compliance for PCI, HIPAA, SOX or any other government mandated security requirement are gone. Today, it's about reputation, brand and corporate risk which demand a very different approach to network security.

Endace Network Monitoring and Recording Fabrics provide deep network-wide visibility into both internal and external cyber security threats on high-speed and ultra-high-speed networks. They use a distributed 'fabric' of passive systems to analyse network traffic in real-time. Not only does every packet get analysed, but they also get recorded to a local storage buffer to enable retrospective forensic analysis and archiving for evidentiary purposes.

If you have any doubt as to whether accuracy of packet capture matters then consider this:

The Conficker worm is 57KB in size. Based on a standard Ethernet frame (1,518 bytes), Conficker is carried in approximately 37 packets, any one of which could potentially contain the signature that an IDS needs to see in order to trigger an alert.

On a 50% loaded 1Gb/s link, packet loss of 0.00002% could cause a system to miss the critical packet that triggers the alert. So forget '5 nines'; in reality, nothing less than 100% capture is acceptable in the world of signature-based network security.

"If you haven't got every packet, then any analysis that you do is pointless"

Packet Capture's Inconvenient Truth

Network security systems that use software-based techniques to acquire packets from the wire drop some of them. The truth is that software-based NICs were never designed to be used to acquire packets from the wire; they were designed to move data between servers and hosts. Our testing has shown, with alarming consistency, that at line rates over 2Gb/s it's almost impossible to trust systems that aren't built using purpose-built hardware. Endace Systems are designed and built to capture packets, without data loss on high-speed links.

If you're already at 2Gb/s, or you can see 2Gb/s on the horizon, and you are using a software-based system, then you should be treating the output of your network security systems with extreme caution.

Introducing Endace Systems

Our systems come in a range of different sizes and port configurations to enable them to be matched to the needs of particular network segment(s). They scale from 10/100Mb/s to 100Gb/s and are designed from the ground up to enable up to six different applications to leverage the same common source of 100% accurate data.

EndaceSensors

EndaceSensors™ are real-time monitoring systems designed to be deployed in places where no capture-to-disk is required. These 1U systems support either 4x 1Gb/s ports or 2x 10Gb/s ports and can analyse up to 10 Gigabits of network traffic per second with an average rule set (depending on the specific configuration).

EndaceProbes

In addition to monitoring up to 20 Gigabits of traffic per second in real time, EndaceProbes™ support high-speed write-to-disk capability at speeds of up to 10Gb/s. EndaceProbes are available in a range of different configurations with up to 10x 10Gb/s ports or 20x 1Gb/s ports, making them ideal for high-throughput environments where rack space is limited and port density is key.

All Endace Systems are based on a three-layer architecture called the Endace Platform. The Endace Platform leverages commodity hardware which incorporates our own DAG® technology, a proprietary software management layer called OSm which enables central management of all systems and a virtual application layer into which multiple applications or tools can be deployed simultaneously.

Introducing Endace Security Manager

Endace Security Manager (ESM) is our Network Intrusion Detection System. ESM is included with every Endace System as part of the Endace Application Suite, which is designed to address the core monitoring and security needs of every network.

When deployed across a network as part of a Monitoring and Recording Fabric, ESM provides deep, network-wide visibility into the widest possible range of cyber threats. With the knowledge that your IDS is interrogating every single packet on the wire you can, for the first time, rest assured that you're being alerted to everything that really matters on your network.

Key features

- Proven 100% accurate packet capture to 100Gb/s
- SNORT® based deep packet inspection engine
- Integrated forensics and analytics for improved MTTR
- Support for custom and blended rule sets
- Full line rate write-to-disk for post-event forensics
- Rapid and efficient data mining
- Support for multiple VLANs
- System by system rule management capability
- Rapid SIM / SIEM and NMS integration

Endace System Performance Specifications

MODEL	PORT DENSITY	IDS THROUGHPUT*
EndaceProbe Series 7000	8-20 x 1GigE or 4-10 x 10GigE	3.6Gb/s
EP3000	4-8 x 1GigE or 2-4 x 10GigE	3.6Gb/s
EP300	8 x 1Gb Ethernet	1.5Gb/s
EP100	4x 1Gb Ethernet	500Mb/s
EndaceSensor Series 3000	4x 10Gb Ethernet 2x10Gb Ethernet	2.5Gb/s
ES300	8 x 1Gb Ethernet	1.5Gb/s
ES100	4 x 10/100/1Gb Ethernet	500Mb/s

*Average throughput is based upon an average rule set and thus is an estimate only.

ESM Architecture

ESM consists of a distributed set of SNORT-powered systems that are connected to a range of different physical links across the network. The way that the system is architected means that different segments of the network (VLANs) can be monitored with specific rule sets, which is essential as different VLANs within the same organisation can be exposed to quite different cyber threats.

All ESM Systems are connected back to the Endace Management Server which hosts the master ESM database. Using Java-based clients, engineers connect to the ESM database and are presented with an easy-to-use dashboard from which they can interrogate alerts.

SNORT power

ESM is built using the SNORT® industry-standard, open-source IDS engine. SNORT already powers more than 250,000 IDS and IPS sensors around the world and is trusted by government agencies and Fortune 1000 organisations. With a global community of developers contributing to the code base, it is far and away the most flexible and trusted IDS engine in existence.

Your rules

Your network is unique. It has a mix of protocols, users and traffic that are specific to you, so it stands to reason that the rules that you are going to want to deploy are going to be equally unique.

Building an effective cyber monitoring system necessitates creating and maintaining a rule set that is specific to your network. Our intrusion detection system enables you to blend different rule sets from third-party sources, community sources and your own custom-written rules to create a rule profile that really delivers.

Taking control of your rules isn't as daunting as many organisations perceive; like everything, it requires good planning and the right partnerships, which is where we can help with our rule-tuning service. We have a team of professionals on hand to help you get your rules exactly right.

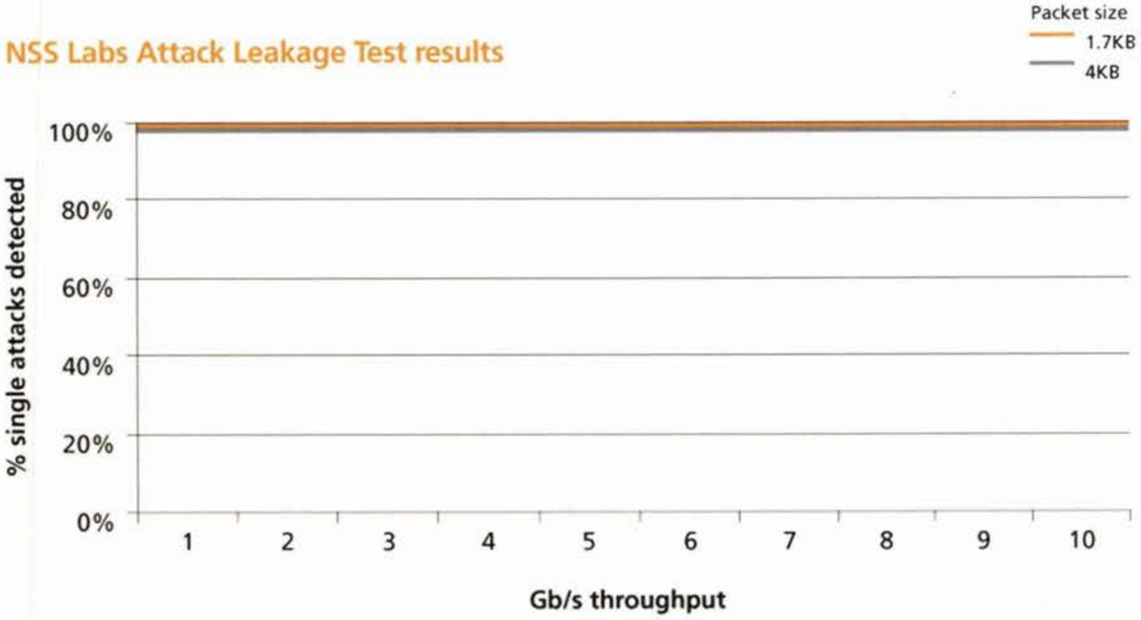
100% Proof

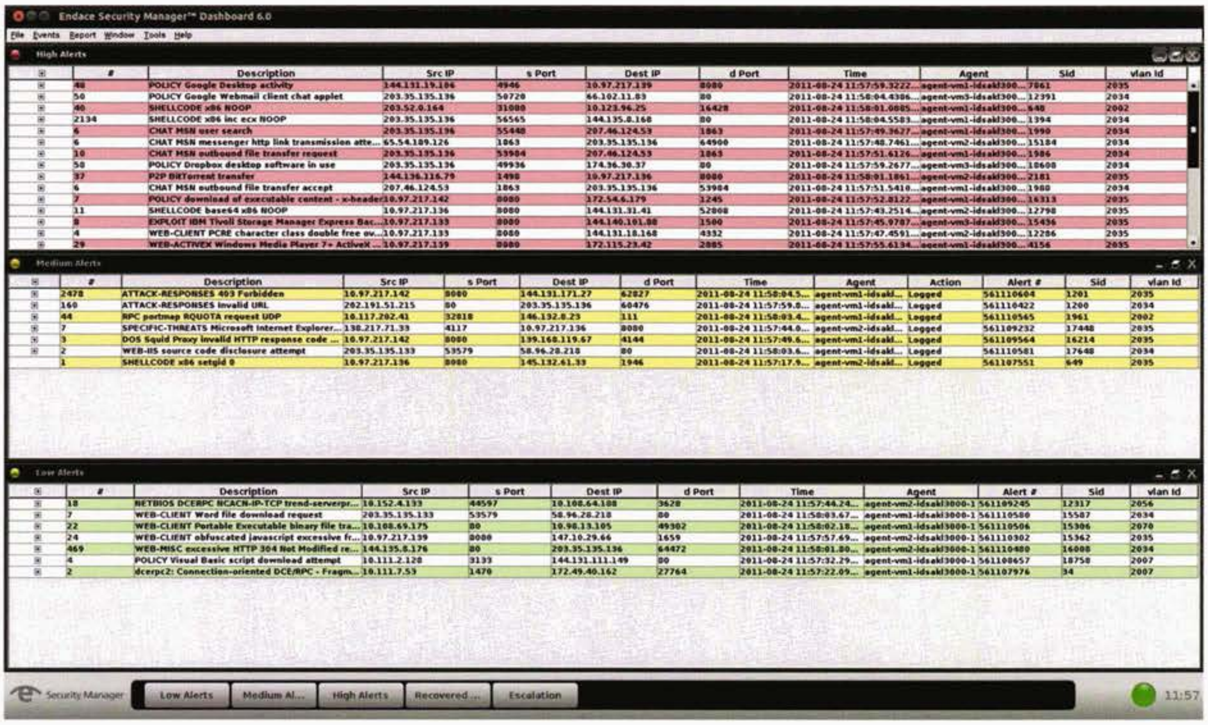
Saying that we capture 100% of packets and proving it are two different things. To make sure that we really do what we say, we gave our system to NSS Labs and asked them to test it for us. Based on their attack leakage detection test, which is the closest thing there is to an industry standard test, we prove that our systems really do capture every packet at 10Gb/s.

NSS Labs

NSS Labs stated that our 10Gb/s system was "one of the few products on the market capable of servicing the high throughput of a true 10-Gigabit environment".

NSS Labs Attack Leakage Test results





High Alerts

	#	Description	Src IP	s Port	Dest IP	d Port	Time	Agent	Sid	vlan Id
⊞	48	POLICY Google Desktop activity	144.131.19.106	4946	10.97.217.139	8080	2011-08-24 11:57:59.3222...	agent-vm1-idsakl300...	7861	2035
⊞	50	POLICY Google Webmail client chat applet	203.35.135.136	50720	66.102.11.83	80	2011-08-24 11:58:04.4306...	agent-vm3-idsakl300...	12391	2034
⊞	40	SHELLCODE x86 NOOP	203.52.0.164	31000	10.123.96.25	16428	2011-08-24 11:58:01.0885...	agent-vm1-idsakl300...	648	2002
⊞	2134	SHELLCODE x86 inc ecx NOOP	203.35.135.136	56565	144.135.8.168	80	2011-08-24 11:58:04.5583...	agent-vm1-idsakl300...	1394	2034
⊞	6	CHAT MSN user search	203.35.135.136	55440	207.46.124.53	1863	2011-08-24 11:57:49.3627...	agent-vm1-idsakl300...	1990	2034
⊞	6	CHAT MSN messenger http link transmission atte...	65.54.189.126	1863	203.35.135.136	64900	2011-08-24 11:57:48.7461...	agent-vm2-idsakl300...	15184	2034
⊞	10	CHAT MSN outbound file transfer request	203.35.135.136	53984	207.46.124.53	1863	2011-08-24 11:57:51.6126...	agent-vm1-idsakl300...	1986	2034
⊞	50	POLICY Dropbox desktop software in use	203.35.135.136	49936	174.36.30.37	80	2011-08-24 11:57:59.2677...	agent-vm3-idsakl300...	18608	2034
⊞	37	P2P BitTorrent transfer	144.136.116.79	1490	10.97.217.136	8080	2011-08-24 11:58:01.1861...	agent-vm2-idsakl300...	2181	2035
⊞	6	CHAT MSN outbound file transfer accept	207.46.124.53	1863	203.35.135.136	53984	2011-08-24 11:57:51.5410...	agent-vm1-idsakl300...	1988	2034
⊞	7	POLICY download of executable content - x-header	10.97.217.142	8080	172.54.6.179	1245	2011-08-24 11:57:52.8122...	agent-vm1-idsakl300...	16313	2035
⊞	11	SHELLCODE base64 x86 NOOP	10.97.217.136	8080	144.131.31.41	52808	2011-08-24 11:57:43.2514...	agent-vm2-idsakl300...	12798	2035
⊞	8	EXPLOIT IBM Tivoli Storage Manager Express Bac...	10.97.217.133	8080	144.140.101.88	1500	2011-08-24 11:57:45.9787...	agent-vm3-idsakl300...	15436	2035
⊞	4	WEB-CLIENT PCRE character class double free ov...	10.97.217.133	8080	144.131.18.168	4332	2011-08-24 11:57:47.4591...	agent-vm2-idsakl300...	12286	2035
⊞	29	WEB-ACTIVEX Windows Media Player 7+ ActiveX ...	10.97.217.139	8080	172.115.23.42	2085	2011-08-24 11:57:55.6134...	agent-vm1-idsakl300...	4156	2035

Medium Alerts

	#	Description	Src IP	s Port	Dest IP	d Port	Time	Agent	Action	Alert #	Sid	vlan Id
⊞	2478	ATTACK-RESPONSES 403 Forbidden	10.97.217.142	8080	144.131.171.27	62827	2011-08-24 11:58:04.5...	agent-vm1-idsakl...	Logged	561110604	1201	2035
⊞	160	ATTACK-RESPONSES invalid URL	202.191.51.215	80	203.35.135.136	60476	2011-08-24 11:57:59.0...	agent-vm1-idsakl...	Logged	561110422	1200	2034
⊞	44	RPC portmap RQUOTA request UDP	10.117.202.41	32818	146.132.8.23	111	2011-08-24 11:58:03.4...	agent-vm1-idsakl...	Logged	561110565	1961	2002
⊞	7	SPECIFIC-THREATS Microsoft Internet Explorer...	138.217.71.33	4117	10.97.217.136	8080	2011-08-24 11:57:44.0...	agent-vm2-idsakl...	Logged	561109232	17448	2035
⊞	3	DOS Squid Proxy invalid HTTP response code ...	10.97.217.142	8080	139.168.119.67	4144	2011-08-24 11:57:49.6...	agent-vm1-idsakl...	Logged	561109564	16214	2035
⊞	2	WEB-IIS source code disclosure attempt	203.35.135.133	53579	58.96.28.218	80	2011-08-24 11:58:03.6...	agent-vm1-idsakl...	Logged	561110581	17648	2034
	1	SHELLCODE x86 setgid 0	10.97.217.136	8080	145.132.61.33	1946	2011-08-24 11:57:17.9...	agent-vm2-idsakl...	Logged	561107551	649	2035

Low Alerts

	#	Description	Src IP	s Port	Dest IP	d Port	Time	Agent	Alert #	Sid	vlan Id
⊞	18	NETBIOS DCERPC NCACN-IP-TCP trend-serverpr...	10.152.4.133	44597	10.108.64.108	3628	2011-08-24 11:57:44.24...	agent-vm2-idsakl3000-1	561109245	12317	2056
⊞	7	WEB-CLIENT Word file download request	203.35.135.133	53579	58.96.28.218	80	2011-08-24 11:58:03.67...	agent-vm1-idsakl3000-1	561110580	15587	2034
⊞	22	WEB-CLIENT Portable Executable binary file tra...	10.108.69.175	80	10.98.13.105	49302	2011-08-24 11:58:02.18...	agent-vm1-idsakl3000-1	561110506	15306	2070
⊞	24	WEB-CLIENT obfuscated javascript excessive fr...	10.97.217.139	8080	147.10.29.66	1659	2011-08-24 11:57:57.69...	agent-vm2-idsakl3000-1	561110302	15362	2035
⊞	469	WEB-MISC excessive HTTP 304 Not Modified re...	144.135.8.176	80	203.35.135.136	64472	2011-08-24 11:58:01.80...	agent-vm2-idsakl3000-1	561110480	16008	2034
⊞	4	POLICY Visual Basic script download attempt	10.111.2.120	3133	144.131.111.149	80	2011-08-24 11:57:32.29...	agent-vm1-idsakl3000-1	561108657	18758	2007
⊞	2	dcerpc2: Connection-oriented DCE/RPC - Fragm...	10.111.7.53	1470	172.49.40.162	27764	2011-08-24 11:57:22.09...	agent-vm1-idsakl3000-1	561107976	34	2007

Endace Security Manager dashboard

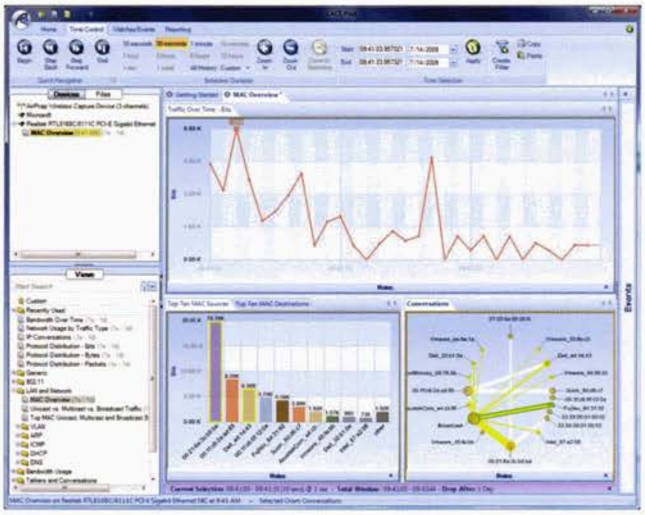
Reducing Mean-Time-To-Resolution

For many organisations, being alerted to security events is one thing; being able to analyse then perform remediation on them when they are coming in fast and furious is quite another. To make the processing of security events more efficient, Endace Security Manager incorporates a unique workflow engine that enables engineers to investigate events efficiently, without compromising accuracy.

The remediation process is based around three simple steps which are all tightly coupled together at the system level to enable rapid workflow through multiple applications on a single host:

- Open the alert in ESM and assess its importance
- View the event in context using Endace Analytics and identify the specific packets of interest
- Extract the raw packets of interest using our data mining tool (Packet Access) and open them in Wireshark or another protocol analyser.

It's quite clear that the volume of events being thrown at security operation centre teams isn't going to start diminishing any time soon, so ensuring that your system is doing everything it can to help accelerate the process of investigating events is a smart move. We're committed to help reducing MTTR with every new release of ESM.



Endace Analytics

SIM/SIEM Integration

Along with SNMP, Syslog and firewall logs, IDS alerts are important contributors to any organisation's security event correlation layer. We work closely with most of the major SIM / SIEM vendors to ensure that our outputs are consistent with their inputs and that integration is rapid, seamless and tested.

eIQ networks

nitrosecurity

netForensics

In addition to providing a critical feed into these systems, Endace Systems also facilitate packet-level interrogation of events generated through the correlation layer. Using the highly accurate timestamps that are attached to every packet as they are captured, users can request packet-level traces in response to events generated by the SIM. As any security operation centre team member worth their stripes will attest to, "until you've seen the packets, you've seen nothing".

Integrated vulnerability scanning

As well as knowing what's traversing your network, it's equally critical to know what systems should and shouldn't be live on your network in order to stop hackers, viruses and malware from exploiting potential weaknesses. Misconfigured networks and unpatched machines are still the most common cause of security breaches and, despite the vigilance of IT staff, these vulnerabilities pose a constant threat.

aura INFORMATION SECURITY

By integrating a market-leading vulnerability scanner into the system architecture, organisations cannot only consolidate hardware in their data centres, but can also leverage the power of the EndaceProbe's write-to-disk capability to capture any traffic going to (or from) systems that are outside of an organisation's trusted white list.

Endace Application Dock

Endace fabrics don't just do IDS; they are in fact an open and flexible hosting platform for any application that uses packet data to generate intelligence.
Each Endace System can host up to six commercial, open-source or custom applications alongside IDS functionality.

Visit **www.endace.com/endace-application-dock** to find out what other applications are certified to run on the platform.

application suite

application dock

WIRESHARK

aura RedEye

NETSCOUT.

The last word on value

The benefits of deploying an Endace Fabric extend well beyond the ability just to see everything. They include:

- Reduction in hardware footprint
- Rapid integration
- Application agility / reduction in time-to-value
- Roadmap to 100Gb/s

Endace Monitoring and Recording Fabrics are unique and are being rapidly adopted by organisations across the world that recognise the need to see everything on their networks.

Endace Systems are the cornerstone for some of the most sophisticated cyber-security deployments on the planet

Endace has been selling the most accurate, open and trusted network monitoring and recording systems to the world's largest telcos, governments, financial institutions and Fortune 1000 enterprises for more than 10 years.

Our systems help our customers to manage risk, reputation and compliance; where the consequences of missing network events have the potential to be catastrophic.

Endace UK
Davidson House
Forbury Square, Reading
Berkshire RG1 3EU
P **+44 118 900 1425**

Endace USA
14425 Penrose Place
Suite 225, Chantilly,
VA 20151
P (toll free) **800 572 0557**

email **enquiries@endace.com**

endace.com

endace