

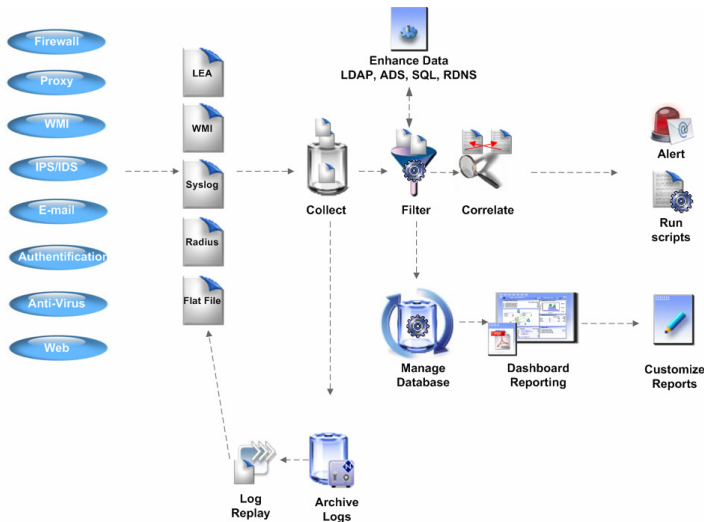


## Net Report Monitoring Center Version 4

### All-in-One Log Exploitation and International Regulatory Compliance Solution

Net Report Monitoring Center is a comprehensive Business Intelligence Solution meeting all your log exploitation issues. Bringing together your heterogeneous enterprise security data (events) into one central point, Net Report analyzes your enterprise network and security infrastructure in real-time, creating integrated alert mechanisms and meaningful dashboards to give you a complete line of sight across your enterprise.

### Real Security Log Management



Net Report Monitoring Center brings you better visibility for your security business decisions:

- Interactive dashboards with meaningful reports.
- Online Alerting & Correlation Console: automatic response to suspicious activity.
- Convert your raw data into real decision-making material.
- Data storage in its unaltered format.
- International regulatory conformity aid (for Sarbanes-Oxley, ISO 17799, Basel II etc...).

### Key Features

- A unique business security data (event) management solution: we take the volume of data your enterprise security devices produce, collect, store, and turn it into meaningful reports and analysis that everyone can use.
- Real-time or scheduled dashboards for each of your security devices in PDF, HTML or Excel format.
- Online access to analysis, results or self-service reporting via the Web Portal.
- Automatic real-time alerts: Net Report Alerting & Correlation Console, SNMP Trap, Pop-Up.
- Data archived in its original format, via standards-based log file compression and signature mechanisms.
- Support for the major log formats and media: Flat File, Syslog, LEA, W3C, CLF, WMI, RADIUS, ODBC.
- Powerful Filter Engine: analysis of up to tens of millions of events per day and per engine.
- Automated database management: archival, aggregation and purge.

### Customer Benefits

- Converts your raw data into actionable business knowledge.
- Centralizes all your security device logs.
- Reduces Business Risk by reacting in real-time to security incidents.
- Enables real-time alerting via the Alerting & Correlation Console.
- Identifies the attack source and type for many devices.
- Reduces your log exploitation costs via automated solutions.
- Meets your need to understand activities by user and device.
- Enables conformity with International Regulations (Sarbanes-Oxley, Basel II, ISO17799 etc...).

### Devices Supported

- **Unified Threat Management:** ARKON Network Security, Fortinet Fortigate, NETASQ.
- **Firewalls:** Check Point™ FireWall-1, Cisco Systems @ ASA & PIX™, Clavister SG Series, Juniper Networks NetScreen, Microsoft ICF & ISA Server, Netfilter ipchains & iptables, SonicWall, Stonesoft StoneGate, Symantec Gateway Security, WatchGuard etc.
- **IDS/IPS:** ISS Proventia G with Site Protector, McAfee IntruShield, Radware Defense Pro, Snort etc.
- **Proxy/Web:** Apache, Blue Coat Security Gateway, F5 WebAccelerator, IBM Lotus Domino, Microsoft Internet Information Server (IIS), Microsoft ISA Server, Netapp Net Cache, Olfeo, Squid etc.
- **RADIUS Servers:** RADIUS, RADIUS Cisco Secure etc.
- **Content Analysis:** Trend Micro IMSS & IWSS, Aladdin e-Safe, McAfee WebShield, MimeSweeper for SMTP etc.
- **Mail Servers:** Microsoft Exchange, PostFix, SendMail etc.
- **Systems:** Microsoft WMI, Unix\* etc.

\* On demand.





### Dynamic Cubes

IPS Cube on Daily Information

Attack Category	Attack ID	Attack Name	Count	Action Group
anomaly	FGT205212777	udp_src_session	1	Blocked
Denial of Service	FGT10187411	Microsoft Works Spreadsheet Memory Corruption	1	Blocked
dns_decoder	FGT18912888	invalid_pointer	10	Blocked
	FGT18912906	invalid_opcode	4	Blocked
	FGT18912909	invalid_param	11	Blocked
icmp	FGT147956877	CyberKit.2.2	4	Blocked
im	FGT108855250	msn	15	Blocked
netbios	FGT102039594	NT_NULL Session	1	Blocked
	FGT102039611	SMB.DCERPC.Registry.OpenHKLM.139	108	Blocked
	FGT102039610	SMB.DCERPC.NetRemoteTOD.445	26	Blocked
	FGT102039618	SMB.DCERPC.SamEnumerateAliasesInDomain.139	1	Blocked
	FGT102039616	SMB.DCERPC.SamEnumerateAliasesInDomain.445	7	Blocked
p2p	FGT109051901	edonkey	48	Blocked
web_misc	FGT103350551	Prozilla.Location.BufferOverflow	1	Blocked
<b>Grand Total</b>			<b>237</b>	<b>38</b>

- Net Report generates real-time cubes – multi-dimensional data views to enable you to interactively examine your results in various dimensions of data.
- Cubes can be easily accessed from the Net Report Web Portal.
- To view Cubes via the Web Portal, you need to use Internet Explorer with Microsoft Office 2003 Web Components, you can easily install this WebVisionCube option via the Net Report Web Portal.

### Alerting & Correlation Console

Status	Alert Received	Due Date	Revised Due Date	Level	Risk	Type	Company	Application	Source	Destination
1	8/15/2006 09:43	8/17/2006 09:43		1	1	NetReport	im_decoder		192.168.0.68	66.102.11.125
2	8/16/2006 09:14	8/16/2006 14:14		2	2	NetReport	Windows Update Agent			
2	8/16/2006 09:13	8/16/2006 14:13		2	2	NetReport	NRFilterEngine		NT AUTHORITY\SYSTEM	
2	8/16/2006 09:12	8/16/2006 14:12		2	2	NetReport	MSSQLServer			
2	8/16/2006 09:12	8/16/2006 14:12		2	2	NetReport	FTPClient			
1	8/15/2006 11:10	8/16/2006 11:10		1	1	NetReport	email		193.252.22.85	192.168.0.201
1	8/14/2006 19:49	8/15/2006 19:49		1	1	NetReport	misc		172.16.0.10	81.52.163.10
1	8/14/2006 18:32	8/15/2006 18:32		1	1	NetReport	email		193.252.23.108	192.168.0.201
1	8/14/2006 15:10	8/15/2006 15:10		1	1	NetReport	web_app		82.139.7.31	172.16.0.10
1	8/14/2006 14:40	8/15/2006 14:40		1	1	NetReport	web_app		92.159.32.178	172.16.0.10
1	8/14/2006 14:25	8/15/2006 14:25		1	1	NetReport	pop3_decoder		192.168.0.201	194.51.100.246
1	8/14/2006 12:32	8/15/2006 12:32		1	1	NetReport	operating_system		84.207.25.124	192.168.0.76

- Real-time HTTP Console for dynamic alert filtering and alert management.
- Real-time Alerts 24/7: Net Report Monitoring Center automates the alert notification process.
- Send alerts via: SMTP, SNMP, Pop-up, the Alerting & Correlation Console.
- Multi-user with advanced user profile management.

### Powerful Reporting & Forensic Analysis

- Net Report proposes pre-configured reports in an accessible dashboard format by default. This format enables a complete line of sight, you can see results across departments and drill down to discover underlying causes and get behind your business performance.
- Dashboards can be created in real-time or scheduled according to your needs. Automatically deliver this time-critical information to decision-makers via e-mail.
- A Tool Kit enables you to create new reports and modify the layout to easily display the key information for your Enterprise Risk Management needs.

### Log Archive Feature

- The Archival Module – Net Report Log Archive – is made up of the Log Storage and Log Vault elements.
- Net Report Log Archive stores logs in unaltered native and enriched CSV (Comma Separated Value) formats and securely archives them in the Log Vault to ensure secure long-term archival.
- Helps satisfy legal log-retention requirements and supplies a powerful, yet simple solution that enables you to meet audit and regulatory requirements that mandate security log and event information be collected and retained for extended periods of time.

### System Requirements

Net Report Monitoring Center, Administration Console and Reporting Engine configuration requirements:

- Windows® 2000 (SP4).
- Windows® 2003 (SP1).
- Internet Explorer 6.0 (Minimum SP1).
- Microsoft SQL Server 2000 (SP4).
- Microsoft SQL Server 2005 (SP1).
- ORACLE 9i and 10g (ORACLE 8.1.7 is only supported in Net Report Versions 4.20 and earlier)
- Microsoft® Internet Information Server.
- Adobe Acrobat Reader (Minimum 6.0.1).

Net Report Monitoring Center includes Net Report Log Analyser and Net Report Log Archive.

Daily General Proxy Statistics

Domain	No. of Visits	Visit Duration (s-hh:mm:ss)	Hits
www.google.fr	23	00:30:28	89
www.netreport.fr	14	00:07:41	157
ac.f.zoubledick.net	6	00:04:55	22
groups.google.fr	6	00:04:55	54
comcast.com	4	00:03:32	17
gA.localvid.com	3	00:11:31	7
edforums.station.sony.com	3	00:45:43	256
global.mcafee.net	3	00:03:07	17
fr.msn.microsoft.com	3	00:04:00	211
pageAC2.googleanalytics.com	3	00:00:16	7

User (IP Address)	Hits	KB	Download Time (s-hh:mm:ss)
192.168.0.81	1 595	14 012	00:17:54
192.168.0.87	1 432	6 501	00:00:03
192.168.0.56	1 099	8 447	00:08:13
192.168.0.83	279	1 321	00:01:36
192.168.0.82	263	1 123	00:04:08

User (IP Address)	Session Duration (s-hh:mm:ss)	Sessions	Average Duration (s-hh:mm:ss)
192.168.0.81	02:35:31	5	00:25:58
192.168.0.56	01:19:31	6	00:11:45
192.168.0.87	00:41:39	9	00:04:38
192.168.0.82	00:36:13	3	00:12:04
192.168.0.83	00:28:08	7	00:04:51

