SureLog

ANET

2014

1. SURELOG: ADVANCED SECURITY MANAGEMENT 3

2. ADVANTAGES 3

Why Fast EPS Performance Matters 3

3. LOG MANAGEMENT 5

Comprehensive Log Data Collection and Log Management 5

Cross-platform Log Collection 6

Windows Event Logs: Agent-less or Agent-based 6

Syslog 6

Flat File Logs 6

Universal Database Log Collection and Log Management 7

Scalable Log Centralization 7

Log Archiving and Retrieval 7

What platforms and devices does it support? 8

4. COMPLIANCE MANAGEMENT 11

5. SIEM 12

1. SURELOG: ADVANCED SECURITY MANAGEMENT

SureLog delivers enterprise security management capabilities including SIEM capabilities, Log Management and Compliance Management

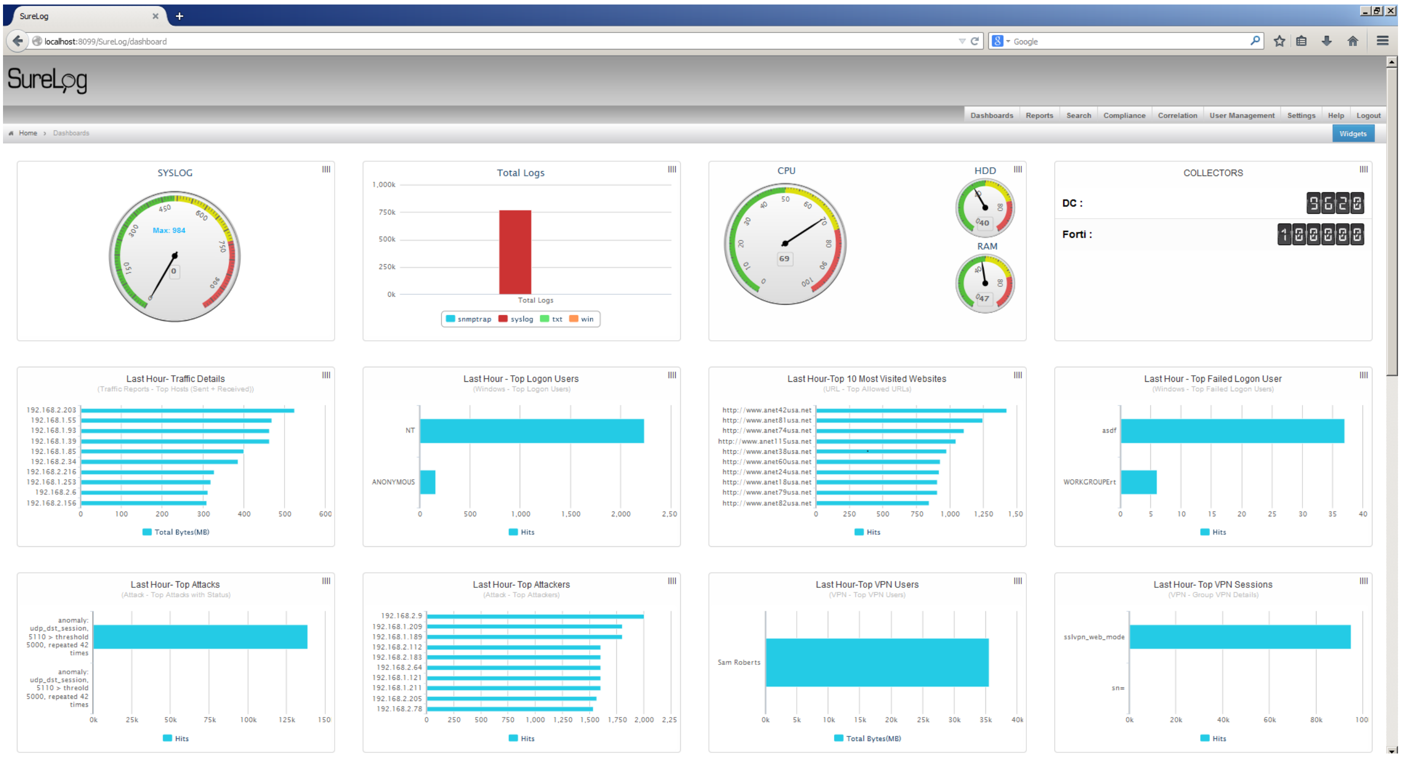
Security Information and Event Management

Log Management

Security Reporting

Event Correlation & Analysis

Fault Management



2. ADVANTAGES

SureLog combines performance and strong correlation engine features to reach a top security management framework.

Why Fast EPS Performance Matters

The sooner threats and attacks to network security can be identified, the more effectively they can be contained. With the fastest events per second performance available in SureLog provides the tools and data necessary to properly monitor security incidents in real-time. With our comprehensive incident reporting tools, you'll have instant answers to the most important questions: who was involved, which systems were affected and how the attack happened.

Supported EPS and minimum requirements:

Peak EPS	500	1000	2500	5000	10000	15000	25000	50000
Sustained EPS	250	500	1250	2500	5000	7500	12500	25000
OS	Windows 64	Windows 64	Windows 64	Windows 64	Windows 64	Windows 64	Windows 64	Windows 64
Web User	5							
CPU	Intel Xeon E5620 @ 2.40GHz	Intel Xeon E5620 @ 2.40GHz	Intel Xeon E3-1240 @ 3.30GHz	Intel Xeon E3-1240 @ 3.30GHz	Intel Xeon E3-1240 @ 3.30GHz	Intel Xeon E3-1276 v3 @ 3.60GHz	2 X Intel Xeon E3-1276 v3 @ 3.60GHz	2X Intel Xeon E5-2680 v2 @ 2.80GHz
RAM	8	12	16	36	48	72	128	256
Storage	250 GB or higher on 15K RPM Drives	250 GB or higher on 15K RPM Drives	500 GB or higher on 15K RPM Drives	1 TB or higher on 15K RPM Drives	1 TB or higher on 15K RPM Drives	1 TB or higher on 15K RPM Drives	1 TB or higher on SSD Disk	1 TB or higher on SSD Disk

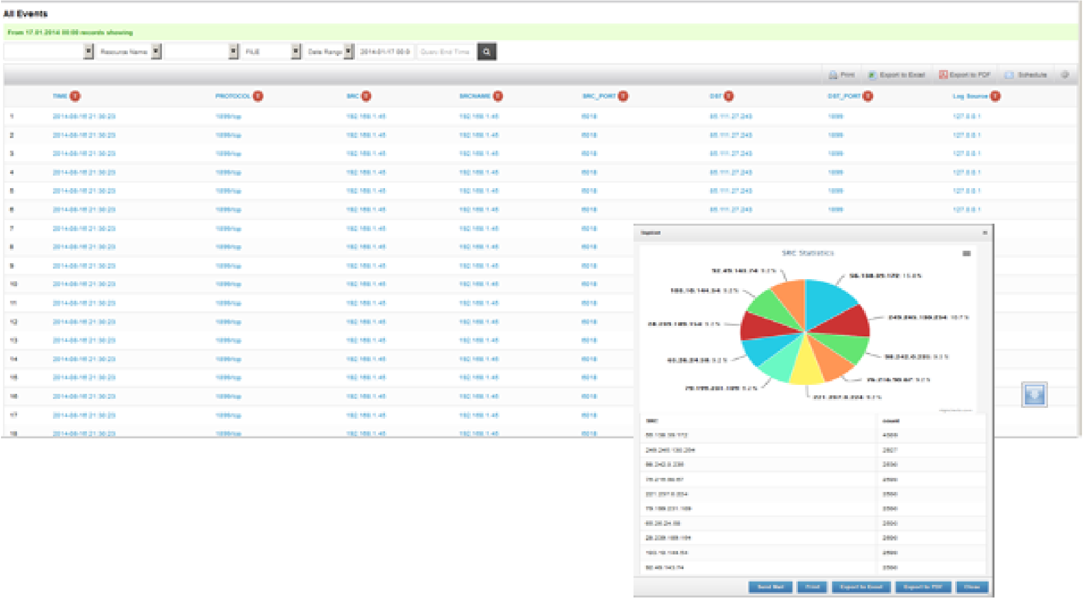
Correlation Engine

- Fast. Supports 50 000 EPS with thousands of rules.
- Trace multiple logs with different types within define time frame. Sample rule: Detects An Unusual Condition Where A Source Has Authentication Failures At A Host But That Is Not Followed By A Successful Authentication At The Same Host **Within 2 Hours**
- Correlate different logs (Example: Windows User Creation Event and Telnet Event) according to related fields. Sample rule:Look for a **new account being created** followed by immediate authentication activity from that same account would detect the backdoor account creation followed by **the account being used** to telnet back into the system
- Trace both a log being created with desired parameters or not. Sample rule: Detects An Unusual Condition Where A Source Has Authentication Failures At A Host But That **Is Not Followed** By A Successful Authentication At The Same Host Within 2 Hours
- Audit privileged user activity such as new account creation for greater operational transparency
- Correlate privileged user behavior with specific network activity. Sample rule:Look for a new account being created followed by immediate authentication activity from that same account would detect the backdoor account creation followed by the account being used to telnet back into the system
- Correlation rule editor is simple to use
- Multiple filtering options
- Compression-based correlation. Monitors multiple occurrences of the same event, removes redundancies and reports them as a single event.
- Threshold-based correlation. Has a threshold to trigger a report when a specified number of similar events occur.
- Filter-based correlation. Inspects each event to determine if it matches a pattern defined by a regular expression. If a match is found, an action may be triggered as specified in the rule.
- Sequence-based correlation. Helps to establish causality of events. Events can be correlated based on specific sequential relationships. For example, synchronizing multiple events such as event A being followed by event B to trigger an action.
- Time-based correlation is useful for correlating events that have specific time-based relationships. Some problems can be determined only through such temporal correlation. For example, time based correlation can be used to implement cleanup rules given a specific interval

3. LOG MANAGEMENT

Suresec unique log management feature being able to collect log data from across an enterprise regardless of their source, present the logs in a uniform and consistent manner and manage the state, location and efficient access to those logs is an essential element to any comprehensive Log Management and Log Analysis solution. The Suresec solution was designed to address core log management needs including:

- The ability to collect any type of log data regardless of source
- The ability to collect log data with or without installing an agent on the log source device, system or application.
- The ability to "normalize" any type of log data for more effective reporting and analysis
- The ability to "scale-down" for small deployments and "scale-up" for extremely large environments
- An open architecture allowing direct and secure access to log data via third-party analysis and reporting tools
- A role based security model providing user accountability and access control
- Automated archiving for secure long term retention
- Wizard-based retrieval of any archived logs in seconds



Comprehensive Log Data Collection and Log Management

Being able to collect log data from across an enterprise regardless of their source, present the logs in a uniform and consistent manner and manage the state, location and efficient access to those logs is an essential element to any comprehensive Log Management and Log Analysis solution. The Suresec solution was designed to address core **log management** needs including:

- The ability to collect any type of log data regardless of source
- The ability to collect log data with or without installing an agent on the log source device, system or application.
- The ability to "normalize" any type of log data for more effective reporting and analysis
- The ability to "scale-down" for small deployments and "scale-up" for extremely large environments
- An open architecture allowing direct and secure access to log data via third-party analysis and reporting tools
- A role based security model providing user accountability and access control
- Automated archiving for secure long term retention
- Wizard-based retrieval of any archived logs in seconds

Cross-platform Log Collection

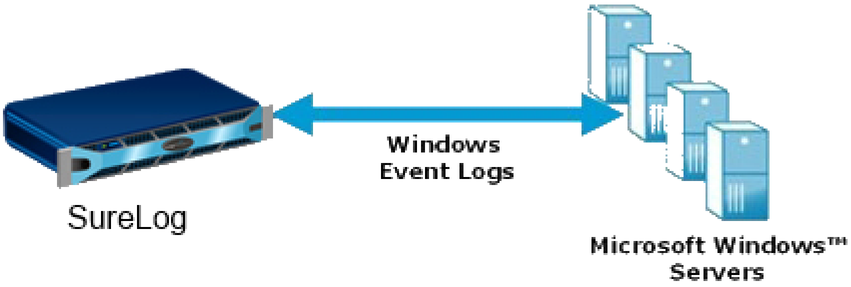
Today's IT operations require many technologies; routers, firewalls, switches, file servers, and applications to name a few. Suresec has been designed to collect from them all through intelligent use of agent-less and agent-based techniques.

Windows Event Logs: Agent-less or Agent-based

Suresec can collect all types of Windows Event Logs with or without the use of an agent. Many Windows-based applications write their logs to the Application Event Log or a custom Event Log.

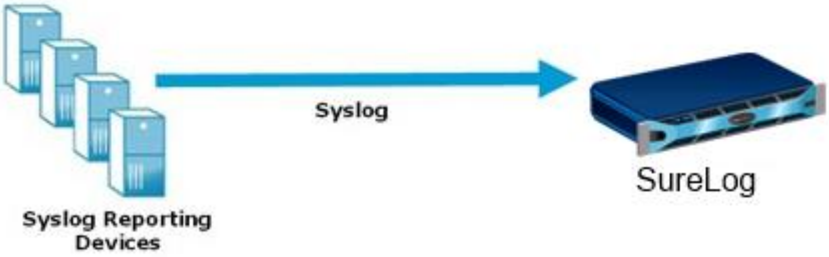
Examples of supported log sources that can be collected by Suresec in real time include:

- Windows System Event Log
- Windows Security Event Log
- Windows Application Event Log
- Microsoft Exchange Server application logs
- Microsoft SQL Server application logs
- Windows based ERP and CRM systems application logs



Syslog

Many log sources, including most network devices (e.g. routers, switches, firewalls) transmit logs via Syslog. Suresec includes an integrated Syslog server for receiving and processing these messages. Simply point any syslog generating device to Suresec and it will automatically begin collecting and processing those logs.

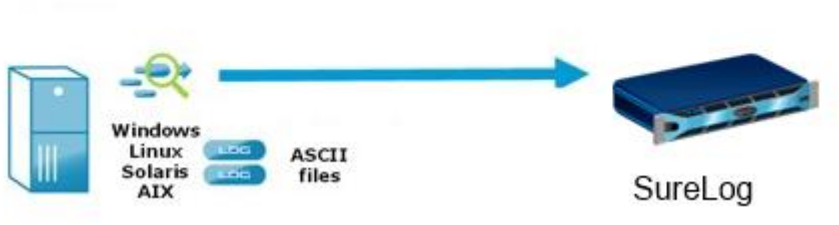


Flat File Logs

Suresec can collect logs written to any ASCII-based text file. Whether it is a commercial system or homegrown application, Suresec can collect and manage them.

Examples of supported log sources using this method include:

- Web servers logs (e.g. Apache, IIS)
- Linux system logs
- Windows ISA server logs
- DNS and DHCP server logs
- Host based intrusion detection/prevention systems
- Homegrown application logs
- Exchange message tracking logs



Universal Database Log Collection and Log Management

Since so much sensitive information resides in databases, it is important to monitor and track access and activity surrounding important databases. The actual and reputational cost of a theft of customer records can be very large. Suresec can help. Suresec collects, analyzes, alerts, and reports on logs from Oracle, Microsoft SQL Server. It also captures data from custom audit logs and applications that run on the database. This capability enables customer to use Suresec for real-time database monitoring to guard against insider and outsider threats.

Scalable Log Centralization

Suresec is architected to scale easily and incrementally as your needs grow. Whether you need to collect 10 million or more than 1 billion logs per day, Suresec can handle it. With Suresec you simply deploy the capacity you need when you need it, preserving your initial investment along the way. Deployments can start with a single, turnkey appliance and grow easily by adding incremental log manager appliances as needs expand. With Suresec's "building blocks" distributed architecture, you can access and analyze logs throughout your deployment with ease.

Log Archiving and Retrieval

Many businesses have compliance requirements to preserve historic log data and be able to provide it in its original form for legal or investigative purposes. Collecting, maintaining and recovering historic log data can be expensive and difficult. Imagine trying to recover logs from a specific server two years ago. Were the logs archived or saved anywhere.   If so, where have the logs been stored?   What format are they in? Can the correct archived log files be identified among the tens of thousands (or millions) of other archive files…in a reasonable period of time? With Suresec, the answers to these questions are easy.

What platforms and devices does it support?

Platforms: Windows and Linux

Devices:

NetFlow Log Support

Cisco	Cisco ASA NetFlow Log

Firewall Log Support

Company Name	Device/Version (versions up to)
3Com	3Com X-family Version 3.0.0.2090 or later. But earlier versions will work to a lesser extent.
Anchiva	Secure Gateway Series 200, 500, 800, 1000, 2000
Applied Identity	Identiforce
ARKOON Network Security	ARKOON 2.20
Astaro	Astaro Security Linux v7.0, v8.0
Aventail	Extranet Center v3.0
AWStats	Most versions
Barracuda	VF250 Version 5.4.1
BlueCoat	SG Series, Proxy Server
CheckPoint	Log import from most versions, VSX Firewalls, LEA support for R54 and above
Cimcor	CimTrak Web Security Edition
Cisco Systems	Cisco Pix Secure Firewall v 6.x, 7.x, Cisco ASA, Cisco IOS 3005, 1900, 2911, 3925, Cisco FWSM, Cisco VPN Concentrator, Cisco CSC-SSM Module 6.3.x, Cisco SSL WebVPN or SVC VPN, Cisco IronPort Proxy, Cisco Botnet module
Clavister	Most versions
CyberGuard	CyberGuard Firewall v4.1, 4.2, 4.3, 5.1
Cyberoam	Cyberoam Firewall Version: 9.5.4
D-Link	Most DFL versions

DP Firewalls	DP Firewall 1000-GE
Electronic Consultants	IPTables Firewall
Fortinet	FortiGate family, Webfilter, DLP, IPS modules, and IPSec, SSL VPN - v300A, v310B, FortiOS 5.x VPN
FreeBSD	Most versions
Funkwerk UTM	Funkwerk Enterprise Communications
Global Technologies	Gnatbox (GB-1000) 3.3.0+
IPCop	IPCop Firewall Version 1.4.17 / 1.4.18
Ingate	Ingate firewall: 1200, 1400, 1800/1880
Inktomi	Traffic Server, C—Class and E—Class
Juniper Networks	• **Juniper SRX series** SRX100, SRX210, SRX220, SRX240, SRX650, SRX1400, SRX3400, SRX3600, SRX5600, SRX5800 • **NetScreen series** NetScreen most versions of Web Filter & Spam Modules • **IDP, SSL VPN series** 4500 & 6500, New Format Logs • **ISG series** 2000 • **6360, 8350 series**
Kerio	Winroute
Lenovo Security Technologies	LeadSec
Lucent	Security Management Server V. 6.0.471
McAfee (formerly Secure Computing)	SnapGear, SG580, Sidewinder (uses **SEF** Sidewinder Export Format), Firewall Enterprise - Sidewinder (S4016)

Microsoft	Microsoft ISA (Firewall, Web Proxy, Packet Filter, Server 2006 VPN) Server 2000 and 2004, W3C log format Threat Management Gateway (TMG)
NetApp	NetCache
NetASQ	F10, F100 v3.x v8
NetFilter	Linux Iptables
Netopia	S9500 Security Appliance v1.6
Network-1	CyberwallPLUS-WS and CyberwallPLUS-SV
Opzoon	Firewall ISOS v5
Palo Alto	Palo Alto Firewalls PA 5000 series, PANOS 4.1.0
Recourse Technologies	ManHunt v1.2, 1.21
Ruijie	Firewall
Securepoint	Securepoint UTM Firewalls
Snort	Most versions
SonicWALL	SOHO3, SOHO TZW, TELE3 SP/TELE3 Spi, PRO 230, 2040, 3060, 4060, 5060, TZ 100/ TZ 100w, TZ 170, TZ 170 Wireless, TZ 170 SP Wireless, TZ 200/ TZ 200w, TZ 210/ TZ 210w, NSA 240, NSA 2400, NSA 2400MX, NSA 3500, NSA 4500, NSA 5000, NSA E5500, NSA E6500, NSA E7500, NSA E8500, NSA E8510, Management, Application control & SSL-VPN logs
Squid Project	Squid Internet Object Cache v1.1, 2.x
St. Bernard Software	iPrism 3.2
Stonesoft	Firewall version 5.5
Sun Microsystems	SunScreen Firewall v3.1
Untangle	
Vyatta System	Vyatta Firewall -IPv4 Firewall, IPv6 Firewall, Zone-Based Firewall
WatchGuard	All Firebox Models v 5.x, 6,x, 7.x, 8.x, 10.x, 11, Firebox X series, x550e, x10e, x1000, x750e
Zywall	Most versions

Supported Applications

SureLog is compatible with the following applications:

- MS IIS W3C Web Server Logs
- MS IIS W3C FTP Server Logs
- DHCP Windows Server Logs
- DHCP Linux Server Logs
- MS SQL Server Logs
- Oracle Audit Logs
- Print Server Logs
- Apache Web Server Logs
- Terminal Server Logs
- Websense
- VMware
- MS Exchange Mail Server
- Merak Mail Server
- McAfee Mail Gateway
- Zimbra Mail Server
- MDaemon Messaging Server
- Trendmicro Web Filter
- MetaTrader
- Postfix Mail Server
- IronPort Email Security Appliances
- Fortinate DHCP Server Logs
- Juniper DHCP Server Logs

Supported Operating Systems

SureLog is compatible with the following operating systems:

- Microsoft Windows
- Linux/Unix

Supported Network Devices

SureLog is compatible with the following network devices:

- Cisco
- HP
- Juniper
- Any SNMP-Enabled Device

4. COMPLIANCE MANAGEMENT

The regulatory compliance reports are mandated by industry bodies/ government authorities to assure minimum security to the IT users in various industries. Non-compliance to the regulatory acts attracts penal action. To ensure credible security and address the mandatory requirement compliance reports of IT networks are required. SureLog generates the major compliance reports required for the IT industry.

The major pre-built reports available in SureLog are **PCI-DSS, HIPAA, ISO 27001:2013, FISMA, SOX, and GLBA**. This compliance management software keeps the future IT compliance regulations in mind and offers custom compliance reports generation feature. ISO-27001 and NIST-1075 are some of the regulatory compliance acts for which the reports can be generated. Even the existing compliance can be modified to suit the individual internal needs of the company.

5. SIEM

SureLog identifies suspicious patterns that would otherwise go unnoticed. Multi-dimensional correlation delivers unprecedented security visibility by tying together diverse security activities across the network. SureLog is designed to efficiently process the high volume of data that comes from security and network devices, core applications, and databases. Only SureLog provides this powerful, all-in-one correlation capability for addressing historical, real-time, and potential threats.

- SureLog help identify network threats in real time by capture and analysis of logs from thousands of devices in multiple branches.
- SureLog enable quick forensics as they can store and retrieve all log data from any device for any period.
- SureLog provide a GUI based dashboard with a uniform format of reporting of logs and events from multiple devices.
- SureLog can correlate events from logs generated by multiple network devices and report only if there were real network breaches of high priority, hence reducing the number false positives and saving a lot of time for the administrators.
- SureLog enable administrators to study the root causes of errors and security breaches by looking in to the log information and reports. Users can identify what exactly caused the errors (like configuration changes, etc) and which systems are vulnerable.
- SureLog come with ready made reports and report formats for various security compliance regulations like PCI, HIPAA, ISO27001, etc so that the security administrators can focus on more important network security enhancement activities.
- SureLog can give reports like top ‘n’ users of specific applications and bandwidth consumption levels for each device on the network, etc.