Federal and Large Enterprise Solutions - FAQs

Correlog has special capability working with Federal (and other) large enterprises. Our technology operates either independently of, or alongside, other SIEM technology to improve threat management and incident response capabilities. This functionality includes the ability to interoperate with virtually any previously installed similar products or other solutions executing on Windows or UNIX-based systems, including Apache Servers, McAfee ePO, as well as any other application or device (e.g., printers or scanners) that produces a streaming log file.

For example, Correlog provides the immediate flexibility to complement technologies that may have been previously deployed in either commercial or U.S. Government environments, such as ArcSight, McAfee ePO, or HP Openview. Moreover, Correlog offers a wide range of deployment options, including multi-tiered and/or highly centralized or decentralized environments, or any combination thereof.

Correlog offers data security managers a rapid and scalable solution to accommodate virtually any iteration and combination of environment architectures or existing SIEM solutions or applications. In sum, Correlog's COTS software offers an existing and immediate approach to address the risk of inadequate or cumbersome threat detection and management, thereby avoiding costly, untested, or unnecessary delays associated with designing to-be-developed solutions.

What is the message capacity of CorreLog?

> CorreLog operates in a stand-alone or distributed environment. Each copy of CorreLog can receive messages from 9999 data sources, with a total message rate of 2500 messages per second / per copy of CorreLog. The maximum amount of data that can be collected per day, per CorreLog server, is approximately 20 Gbytes. The maximum of data that is correlated is approximately 2 Gbytes. (Uncorrelated data can still be searched and reported on.) CorreLog stores collected data for a maximum

of 5000 days.

In a distributed environment, CorreLog can act as an agent and feed messages to a higher-level copy of CorreLog (or some other SIEM collector.) In this case, CorreLog is scalable by X10000. In practice, a two-tier system can handle in excess of 1 million devices, and message rates exceeding 1 million events per second across an enterprise.

What specific firewalls, routers, mainframes, UNIX operating systems can be managed?

CorreLog is a standards-based system that collects log data using a combination of syslog, and SNMP, as well as various optional adapters and agents to gather log data.

CorreLog operates with all versions of Windows X86 based systems (including Windows 2003, 2008, Windows 7, Vista, and XP), and all devices that support syslog and SNMP, including Cisco, Juniper, all UNIX and Linux platforms, Sonic Wall, Checkpoint, and many other devices.

CorreLog does not require an agent to manage UNIX platforms, and uses the native syslog and SNMP capability of these programs. However, CorreLog also includes specialized agents, log file monitors, and file integrity monitors that execute on Linux, Solaris, AIX, and HPUX systems. (These agents can be used to extend the range of monitoring to include arbitrary streaming log files and application programs.)

CorreLog can receive messages from Windows event logs (via either WMI or the CorreLog windows agent). CorreLog can also receive data from application programs executing on Windows or UNIX based systems, including Apache servers, IIS servers, McAfee ePO, and any other application that produces a streaming log file.

Finally, CorreLog supports an MVS Z/OS Mainframe Agent that monitors SMF and RACF messages on mainframe LPARS.

What other environments are available for management? (Example, printers?)

CorreLog has several adapters that can poll data from many different devices in addition to receiving syslog and SNMP traps. This includes an SNMP monitor that can extend the range of CorreLog to poll network printers, routers, switches, wireless devices, relational databases, DHCP servers, and other SNMP capable equipment.

CorreLog has a POP3 adapter that permits messages mailed from any

system to be treated as standard messages, permitting CorreLog to interoperate with any e-mail sending program (such as a trouble-ticketing system.)

CorreLog includes a "File Transfer Queue" that allows any file copied to a particular folder to be read by CorreLog, useful for managing systems that may generate log files, but which have no other management capability other than FTP or HTTP. Information on CorreLog adapters can be found here:

http://www.correlog.com/solutions-and-services/index.html

What is the numerical limitation to quantity of correlated messages from firewalls, routers, and mainframes?

Each copy of CorreLog can collect, search, archive, and report on up to 20 Gbytes worth of data daily. Detailed correlation can be applied on up to 2 Gbytes worth of data each day. (Detailed correlation passing each message through up to 2000 different correlation rules.)

The maximum number of events per second is typically 2500 messages per second per copy of CorreLog. In a two-tier management strategy, the user can scale upwards to a maximum of 10,000 CorreLog implementations, each managing 10,000 devices and 2500 messages per second.

What is the architecture for deployment?

CorreLog can be configured to operate as a distributed system, where each copy of the program collects data from a group of devices (up to 10,000 devices per copy.) CorreLog stores the data locally, or on a remote disk. CorreLog can correlate the data, detect anomalies or exceptions, and forward this information to a higher copy of CorreLog, with possible failover capability. Using this two-tier architecture, CorreLog can manage millions of devices and millions of messages per second.

CorreLog has specific elements to support its role as a distributed SIEM management agent as follows (1) CorreLog runs on a wide selection of Windows operating systems, and can co-exist with other server applications on a node (2) CorreLog is easily installed, does not require the target system to be rebooted, and can be installed using MSI files (3) CorreLog includes optional encrypted TCP tunneling processes to securely and reliably send data over long distances, including secure transmission across a public network (4) CorreLog includes an SNMP agent that permits a network manager to obtain status on many different installations using a standards-based protocol (5) CorreLog includes a

distributed search capability, which can launch simultaneous searches on multiple copies of CorreLog (6) CorreLog is entirely web-based and relies on no console for all configuration activities (7) CorreLog can be remotely distributed and configured from a centralized location using secure SNMP or HTTPS.

What are the deployment limitations? (Can CorreLog execute in virtualized environments?)

CorreLog is not an appliance, and is a software-only solution. The program does not require a database, but can make use of an ODBC compliant database if available. CorreLog does not require Java or .NET to fully execute, and requires no third-party software.

The CorreLog server software executes on Windows 2003, 2008, XP, Vista, and Windows 7 systems. Depending upon the message throughput, CorreLog can usually co-exist with other applications. CorreLog runs in a Virtual Machine with no adaptation required.

General information on CorreLog site requirements, along with Frequently Asked Questions regarding CorreLog deployment, can be found here:

http://www.correlog.com/support-public/CO-Install-Reqs.pdf

How Many Devices Can CorreLog Support?

CorreLog can support 1 million nodes (or more) in a distributed system. This would require a minimum of 100 different CorreLog servers, each handling a specific device type, network region, or other arbitrary division. (See response 5 above for details on how CorreLog operates as a distributed SIEM agent.) The theoretical maximum number of devices that can be managed in a two-tier system is 100 billion devices (i.e. 10,000 X 10,000 devices.)

Can the device operate with DHCP leases, expiring at hourly intervals?

CorreLog can track devices by IP address, device name, or keyword. CorreLog includes an "address override" facility that tags devices based upon IP address, message content and keyword, or time-of-day. This permits CorreLog to track devices based upon some unique identifier (other than the DHCP assigned IP address, which may change periodically.)

Can the product support log files that are overwritten at periodic hourly or daily intervals?

CorreLog is a real-time system. In most cases, CorreLog immediately receives event information as it occurs, eliminating the need to keep log files on the native system.

Can software cover devices such as printers, scanners, storage devices, each with separate log files?

CorreLog correlates data by device type, device location, user name, time of day, and other arbitrary criteria. CorreLog aggregates messages, and then assigns messages to one or more "catalogs" of information that correspond to the requirements of the user. Therefore, CorreLog can create a catalog of information specific to a single printer, all printers, all printers of a specific type, etc.

How does the product comply with FIPS 140?

CorreLog is designed to be FIPS 140-2 compatible. (CorreLog is not FIPS certified, but is ready for compliance testing.) This compatibility includes the ability to create and update AES-256 bit keys (used to encrypt message transmissions), as well as the ability to maintain these keys (such as to perform encryption self-tests.)

Information on CorreLog and FIPS compliance is available under our homepage “Resources” link as well as:

http://www.correlog.com/support-public/CO-SECURE.pdf

Provide an overview of clients where the product has been installed

CorreLog is currently deployed at a variety of Federal, state, and local governments, as well as various commercial enterprises. Commercial enterprises include both domestic and foreign countries. CorreLog serves as a general-purpose security solution as well as a solution for regulatory compliance (such as PCI-DSS, HIPAA, SOX, and other security specifications.)

Explain total operating costs from pilot through fielding, including operations, maintenance, training, and support.

CorreLog is intended to be a highly cost-effective solution that maximizes return on investment. This is a major objective of both the product and the company. Achievement of high ROI for our customers and partners is explicitly incorporated in the company's mission statement, available at the corporate website:

http://www.correlog.com/media-kit/mission.html

What version of McAfee's ePO is supported?

CorreLog supports McAfee ePO Versions 4.0 and 4.5. CorreLog is a certified McAfee Solutions Integration Alliance (SIA) partner.

Can CorreLog run in an environment where some EPO is not supported?

CorreLog receives events from one or more copies of ePO, and can send correlated results to one or more copies of ePO. Therefore, the program can operate in an "N X N" type fashion, accepting data from multiple copies of ePO and relaying correlated results to multiple copies of EPO.

How does the product store / backup data?

CorreLog stores archive data for a maximum of 5000 days within a user specified folder. (The precise time interval is configurable by the CorreLog administrator.)

Log message data is compressed using Gzip, and stored in daily time stamped log files. Each log file has a message digest in clear text, and a second message digest encrypted using a one-way encryption algorithm to prevent tampering with the message digest or file. The Gzip compression provides approximately 80% compression rates of typical log data.

Additional Notes

CorreLog also provides a variety of standards-based agents and adapters that interoperate with other log file management systems. These adapters include Windows and UNIX agents for log management, Mainframe z/OS and MVS agents for RACF and SMF monitoring, Interfaces to McAfee ePO, AND FIPS compatible encryption, File Integrity Monitor (FIM) software for Windows and UNIX platforms, as well as other highly specialized interface software for custom requirements.

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, Syslog, Syslog-NG, SNMP, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution.

CorreLog also provides a variety of standards-based agents and adapters that interoperate with other log file management systems. These adapters include Windows and UNIX agents for log management, Mainframe z/OS and MVS agents for RACF and SMF monitoring, Interfaces to McAfee ePO, FIPS compatible encryption, File Integrity Monitor (FIM) software for Windows and UNIX platforms, as well as other highly specialized interface software for custom requirements.

We consider our technology approach to be the most cost-effective solution currently available for all types of enterprises. Our history backs up that claim. We encourage all users who are frustrated by the high-cost of ineffective software and unresponsiveness of vendors to contact us, so we can begin a discussion. Contact us right now. Further information and evaluation downloads are available at our corporate website.

CorreLog markets its solutions directly and through partners.

CorreLog, Inc.
http://www.correlog.com