The fuel that runs a security information and event management (SIEM) is Syslog messages. Historically, Syslog messages were sent using Universal Datagram Protocol (UDP) as described in RFC 3164 (Figure 1). Unfortunately, UDP provides neither reliable delivery nor encryption and authentication.

To that end Syslog protocol has been “enhanced” by various software vendors without the benefit of an industry standard to ensure reliable delivery, encryption, and authentication. These vendors are randomly using various methods. These enhancements however, have created a Syslog “Tower of Babel” in which many Syslog collectors are unable to receive messages sent across complex IT environments. SyslogDefender bridges that gap by accepting Syslog messages using any of the common Syslog protocols including IPv6, TCP/IP, and TLS, and forwards them to one or more Syslog collectors using protocols that every Syslog collector can accept. (Figure 2).

With no industry standard, large enterprises running on complex infrastructures and application architectures are at risk because 1) there is no proven method for the most reliable connection, and 2) the gateway is not secured through encryption and authentication. CorreLog SyslogDefender ensures a reliable connection because each Syslog stream, regardless of the protocol, is “wrapped” within an encrypted and authenticated pipeline whose reliability is traceable. In this method, you have the luxury of knowing your highly-sensitive SIEM log data is secure and all of it is ported over to your SIEM system with 100% reliability (Figure 3, page 2).

In Figure 3, a number of Syslog senders are installed at a remote location. One instance of SyslogDefender in the remote location is used to “bundle” all of the remote Syslog messages into a single, reliable, encrypted connection. Even though some or all of the Syslog senders are only capable of unreliable, unencrypted UDP Syslog, all messages flow over the public Internet using a reliable protocol and state-of-the art TLS encryption and authentication.
authentication. A second instance of SyslogDefender, located in the datacenter, receives and decrypts the messages and passes them to the CorreLog Correlation Server (or other SIEM), which is installed on the same machine or LAN segment.

SyslogDefender collects Syslog messages from any source (IPv4, IPv6, UDP, TCP/IP, and TLS) and combines them into a single encrypted, reliable tunnel and delivers them to CorreLog or other Syslog collector established in a remote location. The main customer benefits are:

- Reliable delivery,
- Encryption and authentication – SyslogDefender can use both public and client SSL certificates
- Single “hole” through the firewall, and
- Support of any protocol (as shown below).

Compliance Considerations
For enterprises, data security through a verifiable and reliable connection is critical for adherence to corporate and industry compliance standards such as PCI DSS, HIPAA, Sarbanes-Oxley, FISMA, NERC and many others. CorreLog SyslogDefender helps ensure your data management meets these rigorous standards, much to the satisfaction of your compliance auditors.

For more information on CorreLog SyslogDefender please visit www.correlog.com/products.html

About CorreLog, Inc.
CorreLog, Inc. is the leading independent software vendor (ISV) for IT security log management and event correlation. CorreLog’s flagship product, the CorreLog Enterprise Server, combines log management, Syslog, Syslog-NG, SNMP, auto-learning functions, neural network modeling, proprietary semantic correlation, automated help-desk ticketing and reporting functions into a unique multi-platform security solution. CorreLog Enterprise Server operates across Windows, UNIX, Linux and mainframe platforms, shipping with an out-of-box PCI DSS compliant CorreLog agent for IBM z/OS, the world’s most popular mainframe operating system. Visit www.correlog.com for more information.