FUTUREX
WHITEPAPER

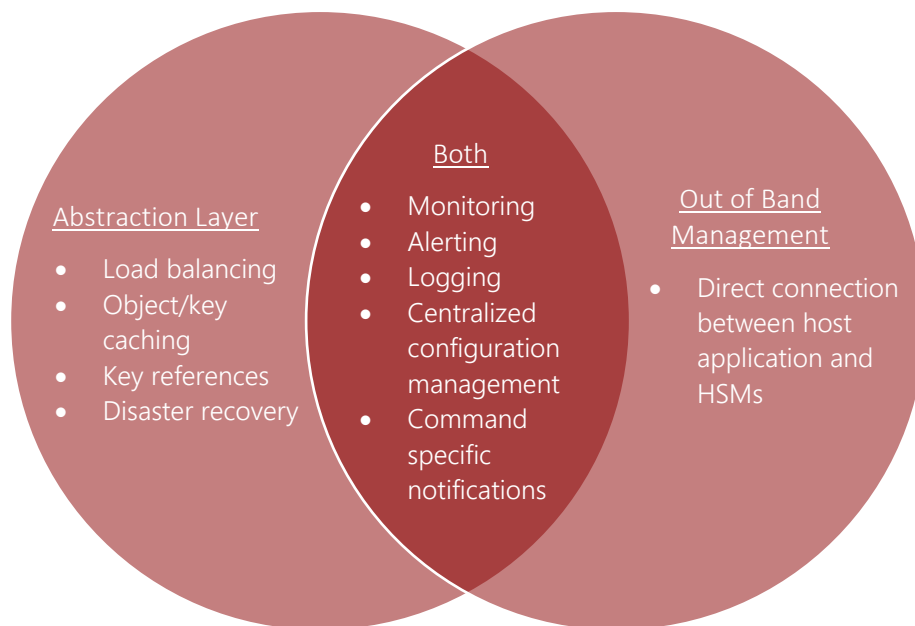*Guardian Series 3 Service Models*

GUARDIAN.1/10/20.14:12

GUARDIAN SERIES 3 OVERVIEW

Systems administrators are familiar with the enterprise cryptographic infrastructure insights that are needed to maintain a cryptographic infrastructure. Futurex's Guardian Series 3 is an enterprise-class centralized configuration, monitoring, alerting, and load balancing solution designed to manage client Futurex devices, such as the Excrypt Plus, Vectera Series, ESM1000, and Key Management Enterprise Server (KMES) Series 3. The Guardian Series 3 forms the cornerstone of an enterprise cryptographic infrastructure in addition to being used to save organizations the resources used to visit and maintain geographically dispersed data centers.

SERVICE MODELS OVERVIEW

The Guardian Series 3 is typically used as an abstraction layer, in which it serves as the intermediary between host application and Futurex devices, but for varying reasons, not all organizations are able to use this method. Organizations would instead opt for the out of band management model, where the host application connects directly with the Futurex device, which is then managed separately by the Guardian Series 3. While abstraction layer is the preferred method, Futurex clients are able to take advantage of a range of functionalities in both models. This whitepaper outlines the functions associated with both the abstraction and out of band management service models.

Abstraction Layer
- Load balancing
- Object/key caching
- Key references
- Disaster recovery

Both
- Monitoring
- Alerting
- Logging
- Centralized configuration management
- Command specific notifications

Out of Band Management
- Direct connection between host application and HSMs

Venn Diagram: Advantages of Abstraction Layer vs. Out of Band Management

# ABSTRACTION LAYER SERVICE MODEL
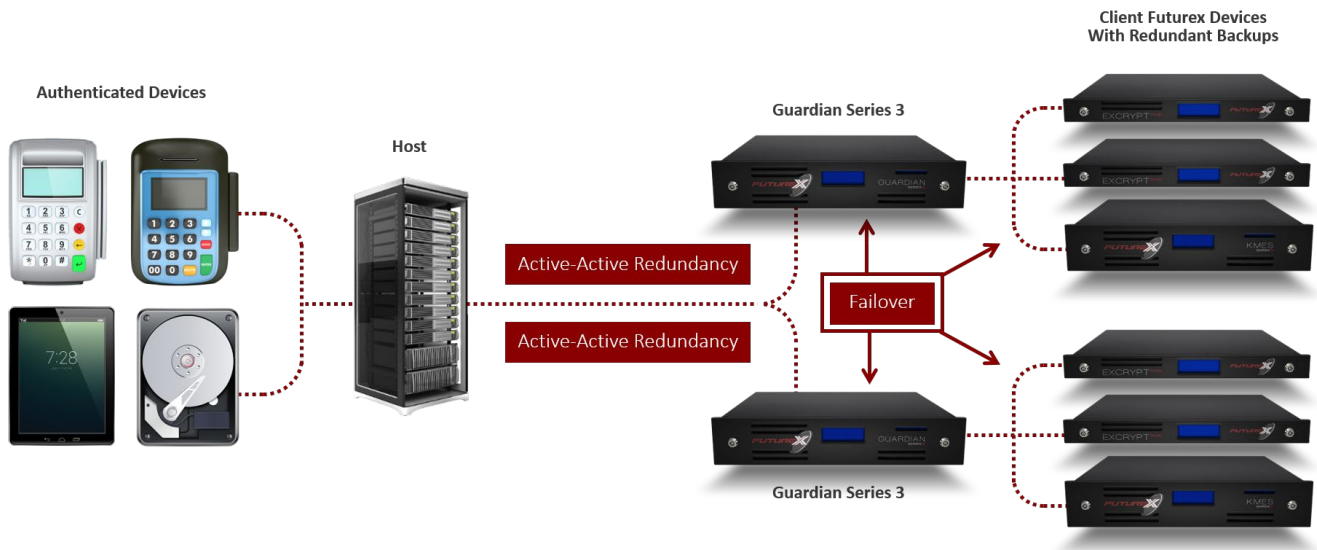
ABSTRACTION LAYER BENEFITS

- Maintain full system redundancy by detecting which devices are available and redistributing loads with zero downtime
- Object and key caching for rapid access to repeatedly-used cryptographic material
- Key referencing, to enable direct integration between key management servers and hardware security modules
- Load balancing of transactions between client Futurex devices

The figure above illustrates transaction processing with two redundant Guardian Series 3's. The Guardian Series 3 ensures that when one client device is taken out of service, the other automatically absorbs the transaction loads. In this example, many devices are able to be managed as one group or as multiple groups rather than individually. This highly efficient model will save organizations the time and resources required to manage each device independently.

The primary difference between this service model and the out of band management service model is that this model allows for load balancing, disaster recovery, object/key caching, and key referencing. Load balancing occurs automatically, according to parameters set during initial setup.

OUT OF BAND MANAGEMENT SERVICE MODEL
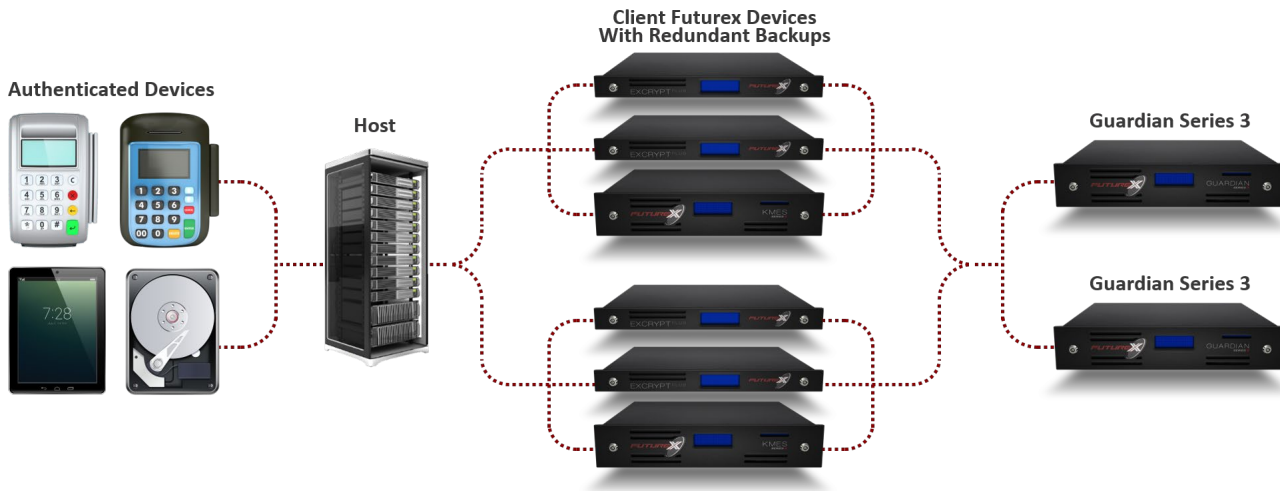
OUT OF BAND MANAGEMENT CHARACTERISTICS

- Direct connection between host application and HSMs
- Host-managed failover and disaster recovery

The out of band management service model allows for most functionality of the Guardian Series 3, but it lacks load balancing, object/key caching, and key referencing. Load balancing may instead be performed within the host software; otherwise, it should be conducted with external network devices or third-party software. Without key referencing, the host application will have to either maintain a standalone key reference database, or communicate directly with the key management server(s) prior to sending API calls containing keys to the HSM.

BENEFITS OF BOTH SERVICE MODELS

The benefits of the Guardian Series 3, regardless of the service model selected, include: monitoring, alerting, logging, centralized configuration management, and command specific notifications. The Guardian Series 3's monitoring ability allows system administrators to automatically receive notifications by e-mail, text, or SNMP for a wide variety of events occurring either on monitored client devices or on the Guardian Series 3 itself. The log capabilities include recording and exporting a full range of log files, exporting audit logs to satisfy regulatory audit requirements, and maintaining a record of command-specific error messages. The Guardian Series 3's centralized client device management allows users to provide a console for modifying and updating client device information and firmware on a massive scale. Although these benefits apply to both service models, the abstraction layer is still preferred when considering the features that the out of band management model excludes.

CONCLUSION

The minor differences between service models lie in that the out of band management service model excludes some functionality, including: load balancing, disaster recovery, object/key caching, and key referencing. While the abstraction layer service model is recommended, out of band management offers a similar functionality and is set apart by offering a direct connection between host application and HSMs. Regardless of the selected service model, organizations can receive significant benefit from the convenience and efficiency offered by the Guardian Series 3.

FUTUREX ENGINEERING CAMPUS

OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112

864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163