Whitepaper

Futurex's Base Architecture Model (BAM)

The data security industry is undergoing rapid changes. Outdated encryption technology can be the downfall of an infrastructure, no matter how secure it may have once been. Each day, criminals develop new ways of bypassing security measures and stealing sensitive and confidential data. Systems administrators charged with protecting their organization's information must be able to rely on their security infrastructure to protect their sensitive data.

Futurex's Hardened Enterprise Security Platform protects the data of some of the largest Tier-1 organizations in the world. One of the keys to the platform's continued success is the common code found in all Futurex devices known as the Base Architecture Model. Through this model, Futurex is able to add new features across all products; expedite coding, development, and quality assurance testing; and develop new products faster, providing our customers with quicker access to the technology they need to successfully defend their infrastructures.

The Hardened Enterprise Security Platform

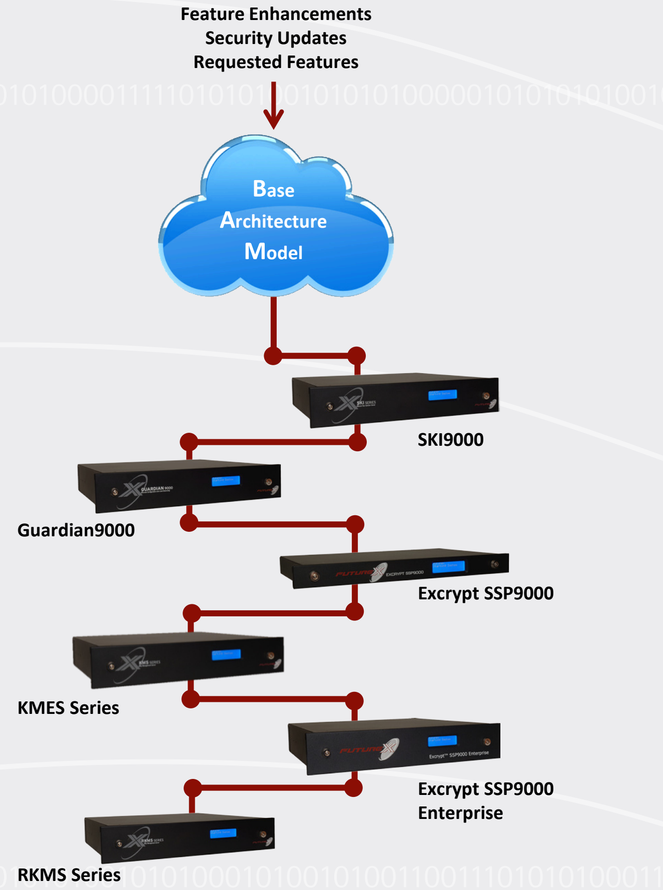
Systems administrators are tasked with the important responsibility of keeping their organization's sensitive data secure from compromise and theft. The technology that network administrators select to defend their infrastructures must be secure, scalable, and versatile, and organizations must be able to place absolute confidence in the technology they employ. As criminals develop new means of stealing sensitive information, data encryption technology must stay ahead of the curve.

Futurex's Hardened Enterprise Security Platform is a collection of advanced data security solutions that operate together to produce a result far beyond the sum of its parts. The platform combines numerous hardware-based encryption devices including hardware security modules (HSMs), key management servers, remote management and configuration devices, and certificate authority servers together to protect every aspect of an organization's infrastructure.

The Hardened Enterprise Security Platform remains the most versatile, scalable, and secure platform employed by many Tier-1 customers in various industries across the globe in part because of the common code and functionality base it utilizes. This common code base, known as the Base Architecture Model, allows Futurex to provide customers with expedited access to the first rate technology needed to secure their infrastructures.

Base Architecture Model

1. Code changes are applied to the Base Architecture Model.
2. BAM replicates changes across all future releases of the Hardened Enterprise Security Platform.



Base Architecture Model in the Hardened Enterprise Security Platform

The Base Architecture Model is the common code and functionality base found in all Futurex cryptographic devices. “Common code and functionality base” refers to the portion of the code that all of the products share or have in common. Through this model, Futurex is able to maintain a faster turnaround time for improvements, emerging developments, and new products, giving Futurex customers expedited access to first-class technology.

Feature Enhancement

As the data security industry advances and changes, so, too, does the Hardened Enterprise Security Platform. New features, updates, and functionality improvements are continuously added in order to further develop the functionality and usability of the individual devices.

The Base Architecture Model allows these new features to be seamlessly replicated in all future releases of the device, as well as in all other technology in the product line. This accelerated feature development ensures optimal quality in all devices that work tirelessly to combat new threats as well increase ease-of-use for systems administrators.

For example, to further increase device security and authentication procedures, Futurex devices are capable of utilize principles of dual-factor authentication. When logging into a Futurex device, users can be required to enter a username and password combination and present a smart card with matching credentials. Using this system, if a thief acquires an employee’s smart card, the thief will not be able to log into the device without the correct username and password. Likewise, if an employee’s username and password becomes compromised, access will not be granted without the corresponding smart card.

This feature was initially instituted in Futurex’s RKMS Series (Remote Key Management Server). Through the Base Architecture Model, this new feature was seamlessly replicated in all future releases of the other device in the Hardened Enterprise Security Platform without having to manually update each device separately. These new features will also be included in all new technology that Futurex develops in the future. This allows customers to have expedited access to the most secure technology on the market.

Quality Assurance Testing and Development

Cryptographic infrastructures that do not utilize a common code base can often face many challenges when it comes to updating their technology. It may take longer to update the entire system if a security flaw is found. Routine updates may be delayed because they are time consuming, and adding new devices requires a great deal more integration work. Quality assurance testing and development takes more time because desired updates take longer to implement when performing updates on each device individually, rather than being able to update each device in the entire platform at once.

The Base Architecture Model significantly reduces the amount of time required to develop, test, and code existing products. Each product is similar in design because of the common code and functionality base, so modifications or usability updates that are made to one product can be easily replicated across the entire Hardened Enterprise Security Platform. Emerging compliance updates in various industries can be made to existing products and easily distributed to each device through the model.

Futurex specializes in custom development projects, where customers require unique features and abilities from their technology that may not currently exist. Through the Base Architecture Model, the time required to perform quality assurance testing is significantly reduced. Existing features have already been tested and perfected, meaning focus can be placed on the quality assurance testing of the newly designed features. Additionally, these new features, developed through custom projects, will be available immediately to all other customers who may have need of the same features and functionality.

Similarly, when Futurex adds new devices to its product lineup, the time-to-market for new products is also reduced because the device is designed and developed using the common code base, rather than beginning from scratch. Thorough quality assurance testing is performed on all Futurex products before they are released into the market, and the new products will automatically include all previously developed features, security measures, and functions, so the engineering team can instead focus on developing new technology to meet the ever-changing and evolving needs of customers.

Base Architecture Model in the Hardened Enterprise Security Platform

Graphical User Interface

One of the most important requirements of any device is usability. Encryption devices are vital to any data security infrastructure, so the device must be easy to use and should not require lengthy or complex employee training. These factors will contribute to a more overall productive environment.

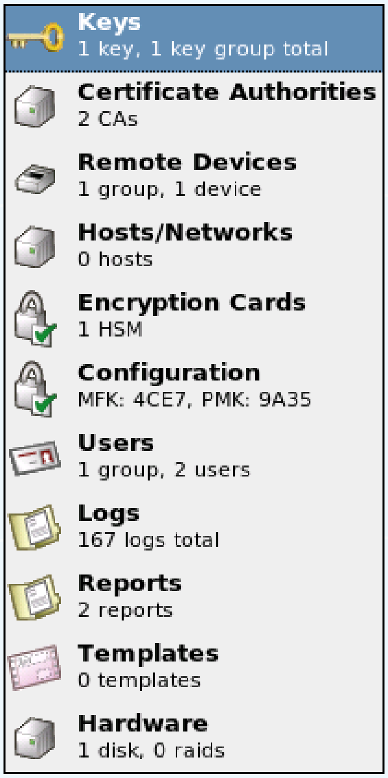
All Futurex devices have a similar graphical user interface. Toolbars, options, and features common to all products are located in the same place on each device. This design significantly reduces the amount of time dedicated to training employees in the use of devices, and increases the ease with which employees can use multiple devices.

Each device in the Hardened Enterprise Security Platform has a toolbar on the left hand side of the screen that contains all of the options available on that device. Tabs such as Configuration, Users, Logs, Reports, and Templates are common to all devices. These common tabs all serve the same function and offer the same additional options when clicked on.

The remaining tabs in each toolbar are unique to each device and will vary from product to product. This organization style contributes to a more overall productive work environment because systems administrators do not have to waste unnecessary time searching for the desired option.

Hardened Enterprise Security Platform Toolbars

- The Graphical User Interface (GUI) of all Futurex devices are similar in design to maintain consistency.
- Many options in the toolbars, such as Configuration, Users, Logs, Reports, and Templates, are found within every Futurex device, making the devices easier to use and reducing training time and costs.



Keys
1 key, 1 key group total

Certificate Authorities
2 CAs

Remote Devices
1 group, 1 device

Hosts/Networks
0 hosts

Encryption Cards
1 HSM

Configuration
MFK: 4CE7, PMK: 9A35

Users
1 group, 2 users

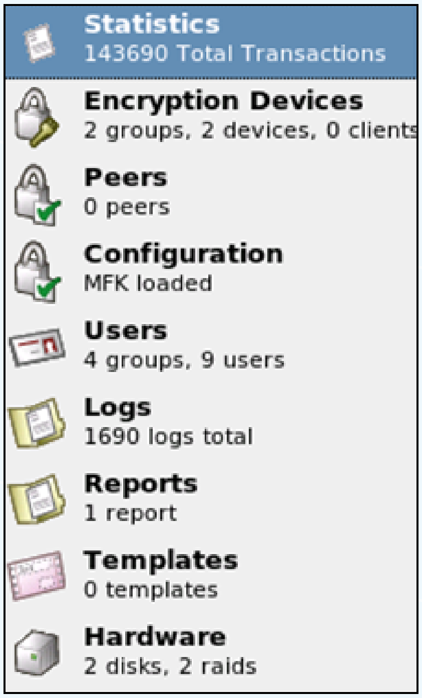
Logs
167 logs total

Reports
2 reports

Templates
0 templates

Hardware
1 disk, 0 raids

RKMS Toolbar



Statistics
143690 Total Transactions

Encryption Devices
2 groups, 2 devices, 0 clients

Peers
0 peers

Configuration
MFK loaded

Users
4 groups, 9 users

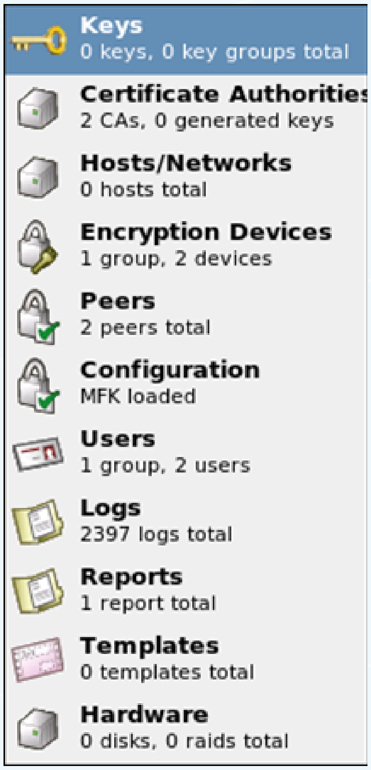
Logs
1690 logs total

Reports
1 report

Templates
0 templates

Hardware
2 disks, 2 raids

Guardian9000 Toolbar



Keys
0 keys, 0 key groups total

Certificate Authorities
2 CAs, 0 generated keys

Hosts/Networks
0 hosts total

Encryption Devices
1 group, 2 devices

Peers
2 peers total

Configuration
MFK loaded

Users
1 group, 2 users

Logs
2397 logs total

Reports
1 report total

Templates
0 templates total

Hardware
0 disks, 0 raids total

Certificate Authority Server Toolbar

Base Architecture Model in the Hardened Enterprise Security Platform

Custom Development Initiatives

Futurex specializes in custom development projects, frequently designing new features to meet the unique needs of customers all over the world. Futurex's Solutions Architects will meet with the customer to evaluate the customer's infrastructure in order to design a new solution that satisfies their requirements. Once the solution has been built and tested, the Solutions Architect will go on-site with the customer to implement the solution, train the staff on its use, and provide any additional assistance needed along the way.

However, once these features have been developed and incorporated into the Hardened Enterprise Security Platform, they can be made available in future releases of the device, granting other potential customers the ability to take advantage of these additional features as well.

The Base Architecture Model allows features or developments to be easily distributed across the entire Security Platform, eliminating the need to manually incorporate changes into each device. If another customer decides that they want or need access to a specific feature, providing them with this access can be as simple as flipping a switch or checking off a box within the device.

Customer Experience

The data security industry is constantly evolving. The sensitive information that companies are responsible for must be protected, and in order to do so, organizations require proven and trusted data encryption hardware.

The combination of an easy-to-use graphical user interface, expedited quality assurance testing and coding, and accelerated feature development guarantees that Futurex customers will always have access to the most secure, scalable, and versatile technology available.

The Hardened Enterprise Security platform is used across the globe by Tier 1 organizations in every industry, and the Base Architecture Model will help to ensure the platform's continued success in the years to come.

About Futurex

For over 30 years, Futurex has been a globally recognized name in providing secure, scalable, and versatile data encryption solutions.

More than 15,000 customers worldwide have trusted Futurex's Enterprise Security Platform to provide innovative, first-to-market solutions for the secure encryption, storage, and transmission of sensitive data.

Futurex maintains an unyielding commitment to offering advanced, standards-compliant hardware security modules, key management servers, and general-purpose data encryption technology alongside world class customer service.