MokaFive Suite Security

In Depth :: **3.0**

mokafive™

Table of Contents

MokaFive
475 Broadway Street, 2nd Floor
Redwood City, CA 94063
http://www.mokafive.com

Documentation version: 2.002

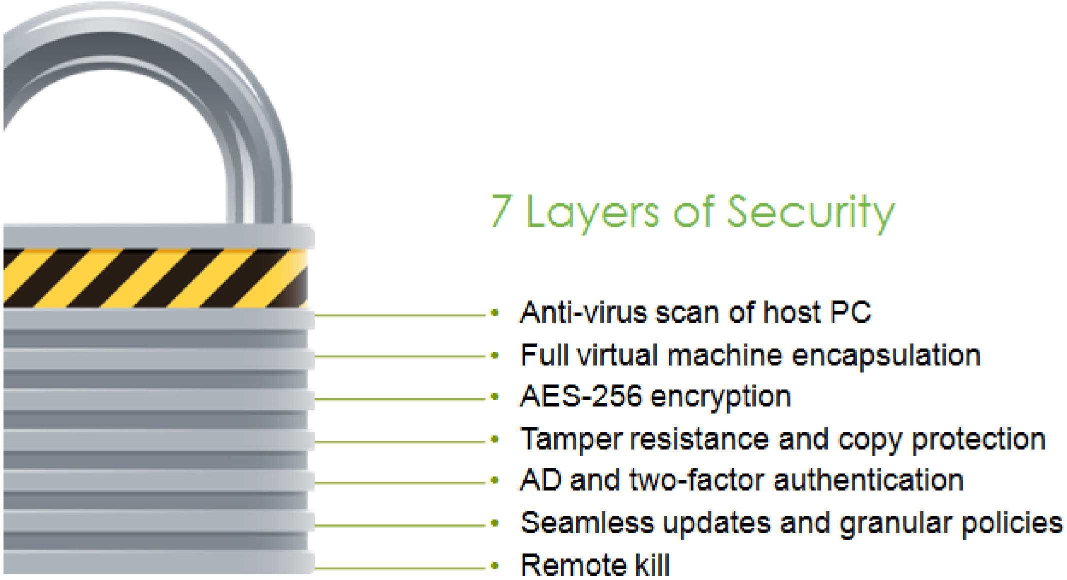
Introduction

MokaFive Suite provides industry-leading security for protecting corporate data and network resources, even when the LivePC images, MokaFive's proprietary virtual machine format, are used on personal or unprotected machines.

This document describes the method and approach of security in MokaFive.

Seven Layers of Security

MokaFive Suite has seven layers of security, each of which increases the overall protection of the corporate environment.


7 Layers of Security
Anti-virus scan of host PC
Full virtual machine encapsulation
AES-256 encryption
Tamper resistance and copy protection
AD and two-factor authentication
Seamless updates and granular policies
Remote kill

All communications over SSL

As a baseline protection, all communications with MokaFive server components (Management Console, Image Store, and Application Gateway) can be configured to communicate over SSL. This in combination with SSL certificate verification prevents man-in-the-middle attacks as well as providing data privacy of all data in transit over the network.

1. Malware scan of host PC

Personal or unprotected machines carry the risk of malware on that machine which can spy on key strokes or screen displayed information. Before a virtual desktop is allowed to run, or a user is asked to provide credentials to authenticate, MokaFive protects against this threat with a built-in malware scanner.

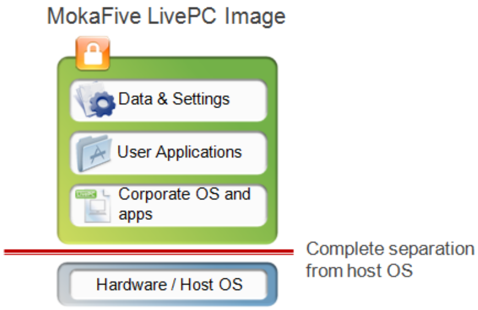
MokaFive has partnered with security industry leader AVG to provide a malware scanner that can detect malware, and automatically shut down the Mokafive Player (the client application which runs LivePC images), before the user can type passwords or view sensitive information. The built-in scan is designed for performance, and is typically completed in seconds, so it has minimal impact on user experience.

The malware scan can run in three modes: run only before authentication events, run during LivePC sessions, or run all the time. Many aspects of the scanning behavior can be controlled through MokaFive policies.

2. Full virtual machine encapsulation

The LivePC image, provides multiple levels of security above and beyond basic Windows and virtual machine security.

MokaFive's LivePC image fully encapsulates the entire corporate desktop, including the OS.



The LivePC image is completely isolated from, and independent of, the underlying host machine. Although the virtual machine "borrows" what it physically needs from the host (CPU, RAM, keyboard, mouse, monitor, etc.), the operating system, applications and data are kept separate. Viruses and malware on the host are not able to infect the virtual machine, and the virtual environment does not leave a trace of data on the device once shut down.

The LivePC image behaves like a physical computer, and as such, the base LivePC image is capable of running standard Windows-based security applications (e.g. firewalls, anti-virus, etc.). On top of the base image, the LivePC is protected further by the hypervisor on which the LivePC image runs.

Over and above the fundamental isolation and encapsulation of the LivePC image, LivePC images provide the following additional protections:

Seamless Updates and Rollback

If a critical vulnerability appears in the wild, and you need to quickly update your corporate image with a patch, MokaFive provides a seamless update process to all users of your image.

Updates are inherently bit-accurate with the golden image, so there is no risk of patch installation failure. Also, if there's an issue with the update, you can also easily roll it back to the last known good version.

Self-Removal of Malware

Should a user introduce an infection on their machine, they can remove the malware themselves through MokaFive's rejuvenation feature. Rejuvenation will return a user's image to the pristine IT-certified state, while maintaining all of the user's data.

Keylogger Protection

Beyond MokaFive's malware scanner, MokaFive still provides protection against keyloggers. LivePC images on Windows hosts include a low-level host keyboard driver that can bypass most software keyloggers. When the LivePC window is activated, all keystrokes are captured by the low-level host keyboard driver and forwarded directly into the guest operating system.

Kiosk-mode Protection

MokaFive offers an enforced full-screen mode on Windows hosts, also known as "kiosk" mode. When run in this mode, LivePC images take up the entire full screen of the host machine and the user is not able to access the host OS environment until the image is shut down.

While in this mode, the LivePC image provides additional security protection. The image is placed on a separate "kiosk" desktop that is independent from the normal desktop. The normal desktop continues to run in the background, but it is not visible. Screen-capture utilities on the host that are not aware of the separate desktop will not be able to capture images from the LivePC. Instead, they will capture the normal desktop. Likewise, malware that captures screen images will not capture images from within the LivePC unless it is aware of the separate desktop.

Kiosk mode also prevents the user from being able to switch back and forth between the host environment and the LivePC. The user will not be able to click back to the host desktop until the LivePC shuts down or is suspended.

Encrypted Swap

When a host computer runs a large set of applications including a virtual desktop, it may move data in memory to swap space to accommodate the memory demand. Data in swap space can be inspected and poses a potential security risk. Most modern operating systems safeguard against this with an option of encrypting the swap space. With MokaFive, administrators can set a policy which enforces the use of encrypted swap.

When this policy is enabled, anytime the host computer starts, Player checks if swap is encrypted. If not, it will warn the user, and offer to enable encrypted swap on the host machine for the user. If the user doesn't enable encrypted swap, Player will refuse to start.

Clipboard Protection

When copy and paste from LivePC image to host (or vice versa) is disabled, the guest operating system in the LivePC uses a completely separate clipboard from the host. Thus, when clipboard sharing is disabled there is no data leakage between the host and guest operating systems through the clipboard. Users cannot copy from the host and paste into the LivePC, or vice versa.

Track Files Copied from Guest to Host

When this policy is enabled, for Windows hosts, MokaFive keeps a log of all files that are copied from the guest to host via drag-and-drop or copy and paste. (Note that drag-and-drop and copy and paste can be completely disallowed through a separate policy.)

The log includes a timestamp, the name and path of the file, and to where it was copied. This allows administrators to audit data leaving the LivePC without restricting access.

3. AES-256 Encryption

If encryption is enabled for a user, MokaFive will encrypt all LivePC images using AES (128-bit or 256-bit) encryption. Encryption uses a different random initialization vector (IV) for each block, and all blocks are encrypted in CBC mode with a SHA256 or SHA512 HMAC. In addition, metadata blocks have additional tamper protection. Unique identifiers are hashed into the keys so blocks cannot be moved between disks or within a disk, and blocks are not susceptible to replacement attacks.

This security exceeds the requirements in IEEE P1619.1 Standard for Authenticated Encryption with Length Expansion for Storage Devices. It is more secure than TrueCrypt and similar full disk encryption technologies. Thus, even if an attacker obtains the files for a LivePC, they will not be able to decrypt the data without breaking the AES encryption.

4. Tamper Resistance and Copy Protection

A MokaFive LivePC images consist of a set of files on the host machine. A malicious attacker may attempt to edit the image itself or metadata associated with the image. Or, the attacker may attempt to copy the image to a different machine for unauthorized access. MokaFive protects against both of these risks through tamper resistance and copy protection.

Tamper Resistance

MokaFive signs files related to LivePC images and Player itself, and checks those signatures on each start. If these files are altered in an unexpected way, images and Player will no longer be usable.

Copy Protection

At device registration time and LivePC subscription time, MokaFive records the unique model and serial number of the underlying device. When copy protection is enabled, the device model and serial number must match; otherwise all usage of the LivePC is blocked.

5. AD and Two-Factor Authentication

Before using the MokaFive Player and images, the user must login to authenticate. There are a range of options for authentication which help increase security.

Active Directory authentication

Player authentication can be configured to require valid Active Directory (AD) credentials. If a user's account has been disabled, deleted or locked, Player and images which require those credentials will be inaccessible to the user.

Two-factor Authentication

- **RSA SecurID.** Player can be setup to require two-factor authentication through integration with RSA SecurID (a popular two-factor authentication solution). Using this option, organizations can require a RSA SecurID passcode in addition to directory services login. The RSA integration is designed to augment standard authentication for users that are accessing their Players while outside your corporate network. The MokaFive Application Gateway integrates with RSA Authentication Manager, and, if enabled, will validate each user authentication with RSA before allowing those users to connect with the MokaFive Management Server.

- **PKI.** LivePC images can be further protected through PKI. A client certificate can be assigned to each LivePC subscription through MokaFive's automated AD domain join process. Through this process, as part of the image's domain join, MokaFive receives a unique client certificate from AD. When a user starts their image, the client certificate is automatically injected into the image, so the image's Windows OS has the client certificate for authentication.

Limit on Maximum Failed Login Attempts before Client is Locked

If the number of invalid attempts to login to MokaFive Player exceeds an administrator-configurable threshold, the Player will shut down. This protects against brute-force attacks against the user's password.

6. Granular Security Policies

MokaFive offers over 60 policies that allow you to tailor the security protections for your users. You can have a set policies apply across your entire organization or target different policies for different groups of users.

The following are an example of the most commonly used security policies.

Lease Time

The administrator may set a lease time that requires the Player to check back in with the Management Server for continued use. If the user is working offline and exceeds this threshold, access will be revoked until the Player checks back in with the server. This insures that the Player and LivePC use current policies and that the user is still approved to use the LivePC.

Offline Auto-Kill Time

Through MokaFive policies, administrators can also set Player to self-delete all data if that Player has not checked in with it's management server in a prescribed period of time. This provides assurance that corporate images cannot be stored indefinitely without contacting the server periodically.

Disabling LivePC Peripherals (Floppy, USB, CD Drives)

To prevent data leakage, and to protect the guest from viruses, the administrator may choose to disable access to floppy disks, USB and CD/ DVD drives.

7. Revoke and Kill from Management Console

In the event that the user's device is lost or stolen, the administrator may remotely revoke or kill the subscription (or the device) from the Management Console.

Revoke

A revoke command allows you to remove access to any user's subscription. Revoked subscriptions are inaccessible by users, but they continue to exist on the user's devices. Revoked subscriptions can be un-revoked with no impact to user data or user-installed applications.

Kill

A kill command allows you to permanently delete the LivePC image from the user's device. When a subscription is killed, all user data and user-installed applications associated with that LivePC image are permanently deleted.

Conclusion

MokaFive encapsulates the entire virtual desktop to keep corporate virtual desktops safe on unmanaged personal computers. MokaFive has engineered seven layers of security, including AES 256 encryption and a built-in malware scanner, to enable secure remote access to corporate networks from personal or unprotected machines.