Security
DATASHEET

Centralized Control – Distributed Trust

Only Moka5 delivers:

Built-in AVG® anti-virus scanning constantly monitors for key loggers and screen scrapers. It also scans the host computer at startup.

Virtual desktop encapsulation keeps corporate data separate from personal files on BYO devices.

AES 256 encryption of the virtual disk ensures compliance with government regulations and prevents data leaks.

Tamper resistance and copy protection keeps the virtual desktop from being moved or edited.

AD and two-factor RSA SecurID authentication allows access only to authorized users.

Granular security policies give IT full control.

Remote revoke or kill allows you to wipe the encrypted data container from lost or stolen devices.

Trying to limit which devices an end-user can use actually undermines corporate security. Too often, those sneaky folks will find stealth workarounds that include accessing corporate information from their unsecure iPhones or Android phones with no security, using cloud-based files sharing with little or no security, or simply downloading information onto their personal laptops. Fortunately, there's a solution that enables end-users to use the devices they prefer when and where they want, while giving IT the level of security and control it needs.

Moka5 is the first enterprise mobility solution that puts the focus where it needs to be: on managing and securing the data and applications you need to be productive, not a commodity device. The M5 platform creates a highly-elastic enterprise perimeter where data and applications follow the end-user and are delivered as simply-managed, highly-secure workspaces for popular end-user devices from notebooks to tablets to smartphones. The M5 containerized workspace effectively isolates corporate assets from personal ones, as well as from the underlying host. This unique architecture ensures host-level malware, vulnerabilities and configuration errors of unsecure, unmanaged devices won't affect critical data and applications.

With over 30 control policy options, M5 enables IT to configure data security the way that best meets their unique requirements. Using a single console, IT can configure access and security policies for all devices that touch critical enterprise data, from laptops to tablets to smartphones. Corporate data is encrypted for maximum security, leaving all transmissions secure and free of sensitive information.

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

Secure data storage, anywhere, any time, on any device

M5 is architected to provide secure data storage from anywhere, at any time, on any device. Because M5 encrypts data at the device level, enterprises can choose to use public cloud storage or their own datacenter. Either way, because only encrypted information is transmitted, all communication remains secure.

To meet enterprise compliance policies, move from cloud-based shared files with minimal security to M5 platform, which meets full SSL and https compliance standards while providing the flexibility needed for a distributed mobile workforce.