VMUNITY

Securing Freedom

**PRODUCT DATA SHEET**

# VMunity Platform – Exceeding the Most Stringent Compliance Requirements for Secure Computing

## The VMunity Secure Computing Platform

**VMunity** is a patented platform that uses nano-virtualization, a class-of-service (COS) matrix, and real-time continuous monitoring to immunize computing environments against cyber-borne threats and unauthorized access. VMunity fully meets the “paradigm-changing” research objectives for system segmentation and virtualization identified in the National Institute of Standards and Technology Interagency Report on computer security (NISTIR 7628, § 8.6.10.) VMunity is vastly superior to inherently-flawed anti-virus applications, which work only against “listed” or heuristically-identified malware, generally fail against malware residing below the operating system (OS), and don’t provide protection once Antivirus checkpoints are breached. By contrast, VMunity:

- Protects against all malicious code, even code not identified previously or heuristically
- Protects against all foreign language code
- Protects all authorized applications, including custom applications
- Works with all computer hardware
- Compatible with all OS, including legacy OS such as Windows 98
- Operates below the OS (BIOS/system bus/kernel) to provide a trusted computing base
- Allows granular COS assignments for all permitted files, apps and processes
- Protects against infected versions of authorized applications (whitelist)
- Lightweight: No negative impact on computer speed or other performance measures
- Easy, rapid deployment across enterprise’s computers
- Compatible with legacy anti-virus and firewall systems the user may choose to continue
- Automated real-time monitoring, reporting and response features, viewable from a cloud-server console or smartphone

**VMunity** works in laptop, desktop, server, and cloud configurations. Once installed, VMunity guards enterprise computers regardless of their location or the source or type of threats.

[continued]

VMUNITY

Securing Freedom

## How it Works

**VMunity** is a patented, component-based, polymorphic software applications platform that completely controls access to computing resources, so that malicious code cannot persist or propagate. VMunity's hypervisor, which loads before the OS, serves up surrogate (virtual), disposable and isolated computing nano-virtualized environments, which are created and discarded every time a process is executed. Thus, unauthorized access to user resources are denied.

VMunity's architecture manages virtual computing environments in a controlled manner. Virtual environments are managed, validated and tracked by the VMunity controller. User data is isolated from the virtual environments, OS and applications and accessed through a digital airlock based on a rules engine with validated OS and applications. Resources are tightly managed or eliminated: Folders are not shared, configuration files are not shared, backdoors are not allowed, network connections are isolated and communications are handled with mandatory access controls such as sHype. DOS attacks are controlled through maximum thresholds on virtual environments.

**The platform components are:**

- Core Controller
- Cloud-Based Administration (Enterprise version)
- Automated Audit and Learning (AI) module
- Automated Cloud-Based Remediation Module
- Triplex Authentication Module
- COS Matrix
- Advanced COS Matrix (Enterprise version)
- Counter Measures Module
- Monitor, Report, Respond Module

## Regulation and Compliance

**VMunity** is appropriate for any industry sector, including the sixteen areas of critical infrastructure identified by the President of the United States and the Department of Homeland Security. The combination of nano-virtualization, a COS matrix and real-time reporting make VMunity an ideal solution for industries which must protect against both malicious code and unauthorized access (internal or external). Accordingly, VMunity has unique advantages as a solution to compliance and regulatory requirements—the healthcare and securities industries being just two examples.

VMUNITY

Securing Freedom

**PRODUCT DATA SHEET**

# Advanced COS Matrix

## Comprehensive and Secure Control of Desktop and Server Applications

### Class of Service (COS) Control Over Applications and Programs

The Advanced COS Matrix extends the basic class-of-service (COS) function of the VMunity secure computing platform to provide highly granular control over all commercial and custom applications and programs. Advanced COS Matrix also provides full access control to virtually all path names and command functions.

### How it Works

The Advanced COS Matrix provides an expanded table of COS functions for every application and program that is part of the VMunity trusted computing base Master Profile. From this table, enterprise managers can automatically or manually create a COS and apply it to programs and applications including custom programs and bespoke applications. The COS Matrix fully integrates with the VMunity Platform (Basic) to provide secure computing of endpoint computing activity and identifies any attempt to run unauthorized applications, programs and scripts as well as attempts to perform functions that exceed the COS.

VMUNITY

Securing Freedom

**PRODUCT DATA SHEET**

# Mobile Commander

## Powerful Real-Time Monitoring, Reporting and Response Tools for the Enterprise

### Monitor, Report, Respond

Mobile Commander puts the power of real-time monitoring, reporting and response tools for secure computing in the hands of enterprise managers. Mobile Commander leverages the VMunity Cloud Console to deliver real-time data visualization of global enterprise cyber events and delivers this real-time data to a handheld smartphone application. Mobile Commander monitors computing activity and identifies any attempt to run unauthorized applications, programs and scripts.

### How it Works

Mobile Commander prioritizes and summarizes global activity related to cyber events to deliver at-a-glance data visualization of the state of information security across the enterprise in real-time. Mobile Commander is fully integrated into the VMunity secure computing platform that ensures secure computing and preempts both known and unknown cyber threats.

**PRODUCT DATA SHEET**

# VMunity iKit

## The VMunity Developer Environment for Securing Industrial Controls Applications for Critical Infrastructure

### VMunity-Inside Next Generation Cybersecurity Technology

iKit is designed to allow providers of critical infrastructure and industrial controls applications to add, quickly and easily, next-generation, true-secure VMunity technology to applications used in mission-critical, dedicated computing environments. (See VMunity Product Data Sheet.) iKit exceeds the capabilities of all security solutions on the market today and defeats both known and unknown threats.

### Regulation and Compliance

iKit is designed to make software applications that control critical infrastructure immune to cyber-borne threats. iKit allows developers and industrial control and IT professionals to incorporate Vir2us "VMunity- Inside" technology into their applications to achieve the benefits of system segmentation and virtualization described as "paradigm-changing" in the National Institute of Standards and Technology Interagency Report on computer security (NISTIR 7628, § 8.6.10.) This allows for the creation of secure computing processes that are inherently immune to cyber threats. Legacy security solutions do not address unknown threats adequately and provide virtually no security once breached.

iKit is appropriate for any industry sector, including the sixteen areas of critical infrastructure identified by the President of the United States and the Department of Homeland Security. VMunity's combination of nano-virtualization and a COS matrix make iKit an ideal solution for industries which must protect against both malicious code and unauthorized access (internal or external).

### Deployment from the Cloud

Once you have used iKit to create the "VMunity-Inside" module for your application and computing environment, you have the option to deploy the module enterprise-wide through your own network or through Vir2us' cloud deployment system. Please contact us if you would like support in creating your applications module or for large deployments.

VMUNITY

Securing Freedom

**PRODUCT DATA SHEET**

# **Genesis** Automated Remediation

## Cloud-Based Remediation for Assurance of Pristine Uncompromised Computing Environments

### Remediation for the Enterprise

Genesis’ patented, cloud-based remediation solutions enable IT professionals to remediate, restore and repair compromised computing systems in minutes from a secure cloud-based server on a fully automated basis. For systems that will not boot or lack network access, the Genesis iPac3 portable (handheld) unit performs the same functions (See iPac3 Product Data Sheet.)

### Remediation functions

Genesis is patented, breakthrough technology for computer servicing and remediation. Genesis automates thousands of processes (that can take skilled technicians hours) in just minutes, and provides true restoration and repair of computer systems without the need for extensive technical knowledge. Genesis delivers immediate ROI in most service environments. Only Genesis delivers:

- Comprehensive computer restoration and repair in minutes
- First, second and third level data recovery
- 100% solution to previously embedded malware, viruses, etc.
- 100% solution to operating system and application file corruption
- 100% solution to hard drive problems
- 100% solution to registry problems
- 100% solution to BIOS corruption (Enterprise version)

### Additional invaluable functions

Genesis’ patented computer services platform includes these additional automated services:

- Comprehensive computer-to-computer migration
- Instant hard drive migration
- Comprehensive system analysis reports, including hardware and hard drive diagnostics
- Application keys report, listing all application names, SN’s and product keys
- E-cycling: A new, quick, top-class technique for erasing hard drives (non-recoverable status)
- Backup tools

VMUNITY
Securing Freedom

**PRODUCT DATA SHEET**

# **iPac3** Handheld Remediation Unit

## Portable High-Speed Remediation, Restoration, and Repair of Compromised Computing Environments

### Remediation for the Enterprise

iPac3 is a portable (handheld) unit that performs the same functions as Genesis, for systems that will not boot or lack network access. (See Genesis Product Data Sheet.) iPac3 and Genesis' patented, cloud-based remediation solutions enable IT professionals to remediate, restore and repair compromised computing systems in minutes from a secure cloud-based server on a fully automated basis.

### Remediation functions

iPac3 and Genesis are patented, breakthrough-technology for computer servicing and remediation. Genesis automates thousands of processes (that can take skilled technicians hours) in just minutes, and provides true restoration and repair of computer systems without the need for extensive technical knowledge. Genesis delivers immediate ROI in most service environments. Only iPac3 and Genesis deliver:

- Comprehensive computer restoration and repair in minutes
- First, second and third level data recovery
- 100% solution to previously embedded malware, viruses, etc.
- 100% solution to operating system and application file corruption
- 100% solution to hard drive problems
- 100% solution to registry problems
- 100% solution to BIOS corruption (Enterprise version)

IPAC3
RESTORATION · REPAIR · REMEDIATION

### Additional invaluable functions

iPac3 and Genesis include these additional automated services:

- Comprehensive computer-to-computer migration
- Instant hard drive migration
- Comprehensive system analysis reports, including hardware and hard drive diagnostics
- Application keys report, listing all application names, SN's and product keys
- E-cycling: A new, quick, technique for erasing hard drives (to non-recoverable status)
- Backup tools