



Product Component

DEFINITION

<i>Name</i>	Computer Associates InoculateIT (workstation)
<i>Description</i>	Provides virus detection and removal solution for workstations.
<i>Rationale</i>	<ul style="list-style-type: none"> Meets State of Missouri Virus Detection and Elimination criteria for workstations as defined within the MAEA; Currently operating successfully within State infrastructure; and Listed as a niche player by the Gartner group and the Butler group, and certified by the ICSA.
<i>Benefits</i>	Provides comprehensive protection for enterprise workstations capturing both known and new viruses before they infect multiple users.

ASSOCIATED ARCHITECTURE LEVELS

<i>List the Domain Name</i>	Security
<i>List the Discipline Name</i>	Technical Controls
<i>List the name of the associated Technology Area</i>	Virus Detection & Elimination

KEYWORDS

<i>List all Keywords</i>	Virus, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management
--------------------------	---

VENDOR INFORMATION

<i>Vendor Name</i>	Computer Associates	<i>Website</i>	www.ca.com
<i>Contact Information</i>	Michael.Ramatowski@ca.com		

POTENTIAL COMPLIANCE ORGANIZATIONS/GOVERNMENT BODIES

Standard Organizations

<i>Name</i>	ICSA Labs	<i>Website</i>	www.icsalabs.com
<i>Contact Information</i>	ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com)		

Government Bodies

<i>Name</i>	NIST	<i>Website</i>	nvl.nist.gov
<i>Contact Information</i>			

COMPONENT REVIEW

<i>List Desirable aspects</i>	<ul style="list-style-type: none"> • Low cost of ownership • Flexible scanning options • Content scanning • Expedient updates • Ties to enterprise management and centralized policy management tools • Protection from the newest threats • Enterprise reporting • Broad platform support {Windows NT/2000/XP, Linux, NetWare} • Complete desktop lock-down • Heuristics (i.e., pattern matching) • Incremental updating • E-mail protection • Internet protection
<i>List Undesirable aspects</i>	<ul style="list-style-type: none"> • System performance impacts (e.g., scan at logon) • Potential software conflicts

ASSOCIATED COMPLIANCE COMPONENTS

Product

<i>List the Product-specific Compliance Component Names</i>	
---	--

Configuration Links

<i>List the Configuration-specific Compliance Component Names</i>	
---	--

COMPONENT CLASSIFICATION

<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i> <input type="checkbox"/> <i>Current</i> <input checked="" type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>
-----------------------------------	---

Component Sub-Classification

Sub-Classification	Date	Additional Sub-Classification Information
<input type="checkbox"/> <i>Technology Watch</i>		
<input checked="" type="checkbox"/> <i>Variance</i>	TBD	Pending results of Business Case review for agencies requesting continued use of product.
<input type="checkbox"/> <i>Conditional Use</i>		

Rationale for Component Classification

Document the Rationale for Component Classification

Though CA InoculateIT meets most of the basic criteria established for selection of workstation virus protection, it has been marked as Twilight for the following reasons:

- It has not generated sufficient demand across the State to be considered an acceptable enterprise-wide solution.
- As it is not widely used across the State, the purchase of CA InoculateIT for workstations does not keep with the Enterprise Principles related to cost reduction through consolidated purchasing power.
- The continued use of CA InoculateIT also impacts many of the interoperability principles of enterprise architecture including:
 - Convergence towards a common architecture
 - Elimination of “islands” of technology
 - Elimination of overlapping technologies and solutions
 - Avoiding the proliferation of technologies and solutions.
- According to Gartner Research, CA InoculateIT is a niche player in the anti-virus market, not a market leader or visionary.
- Use of CA InoculateIT for workstations requires a variance business case.

Migration Strategy

Document the Migration Strategy

Organizations using CA InoculateIT for workstations shall begin investigation of the budget, training, and any conversion issues associated with moving to one of the workstation anti-virus products labeled as “current” within the MAEA.

These organizations shall look for opportunities (such as workstation image or O/S upgrades) to migrate to one of the MAEA approved products.

Impact Position Statement

Document the Position Statement on Impact

Only those agencies and/or organizations within the State of Missouri actively using CA InoculateIT will be impacted.

- This change shall have minimal impact the physical technical environment.
- Such a migration will have a visible impact to end-users as CA InoculateIT is replaced on workstations.
- The largest impact will be the conversion efforts necessary to replace CA Inoculate IT on the agencies workstations with acceptable MAEA approved workstation anti-virus software.

AGENCIES

List the Agencies Currently Utilizing this Product

Office of the State Courts Administrator

CURRENT STATUS

Provide the Current Status

In Development

Under Review

Approved

Rejected

AUDIT TRAIL

<i>Creation Date</i>	02/06/2003	<i>Date Accepted / Rejected</i>	02/27/2003
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	
<i>Reason for Update</i>			