



Product Component

DEFINITION

<i>Name</i>	Computer Associates InoculateIT (management tool)
<i>Description</i>	Scalable tool for managing and enforcing virus protection and policies.
<i>Rationale</i>	Gives you the power to ensure virus protection, central control, and visibility.
<i>Benefits</i>	<ul style="list-style-type: none"> • Comprehensive policy management. • Detailed graphical reporting. • Software deployment enabling administrators to ensure virus protection.

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"> • Comes as part of the InoculateIT package. • Lower Cost of Ownership than not having a product. • Multi-Tiered Active Virus Defense. • Enterprise-wide Visibility. • Enterprise-scalable Policy Management.
<i>List Undesirable aspects</i>	<ul style="list-style-type: none"> • Less market share than other vendors – increasing risk of vendor longevity issues.

ASSOCIATED COMPLIANCE COMPONENTS

Product

List the Product-specific Compliance Component Names

--	--

Configuration Links

List the Configuration-specific Compliance Component Names

--	--

COMPONENT CLASSIFICATION

Provide the Classification

Emerging
 Current
 Twilight
 Sunset

Component Sub-Classification

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

Rationale for Component Classification

Document the Rationale for Component Classification

Though the centralized-management features of CA InoculateIT meet most of the basic criteria established for selection of anti-virus management tools, 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 anti-virus management 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.
- CA's focus with regards to anti-virus management is to move the InoculateIT product into its *eTrust* security management umbrella to more closely tie the product to the *CA Unicenter* event management product line. Such a move will require additional investment to capitalize on the added functionality.

Use of CA InoculateIT management tool requires a variance business case.

Migration Strategy

Document the Migration Strategy

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

These organizations shall look for opportunities 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 for anti-virus management will be impacted.

- This change shall have minimal impact to the physical technical environment.
- Such a migration shall not have a visible impact to end-users.
- The largest impact will be the conversion efforts necessary to replace CA InoculateIT on the organizations servers with acceptable MAEA approved anti-virus management 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

Creation Date

02/06/2003

Date Accepted / Rejected

02/27/2003

Reason for Rejection

Last Date Reviewed

Last Date Updated

Reason for Update