

Introduction to Cisco Security Agent Correlation

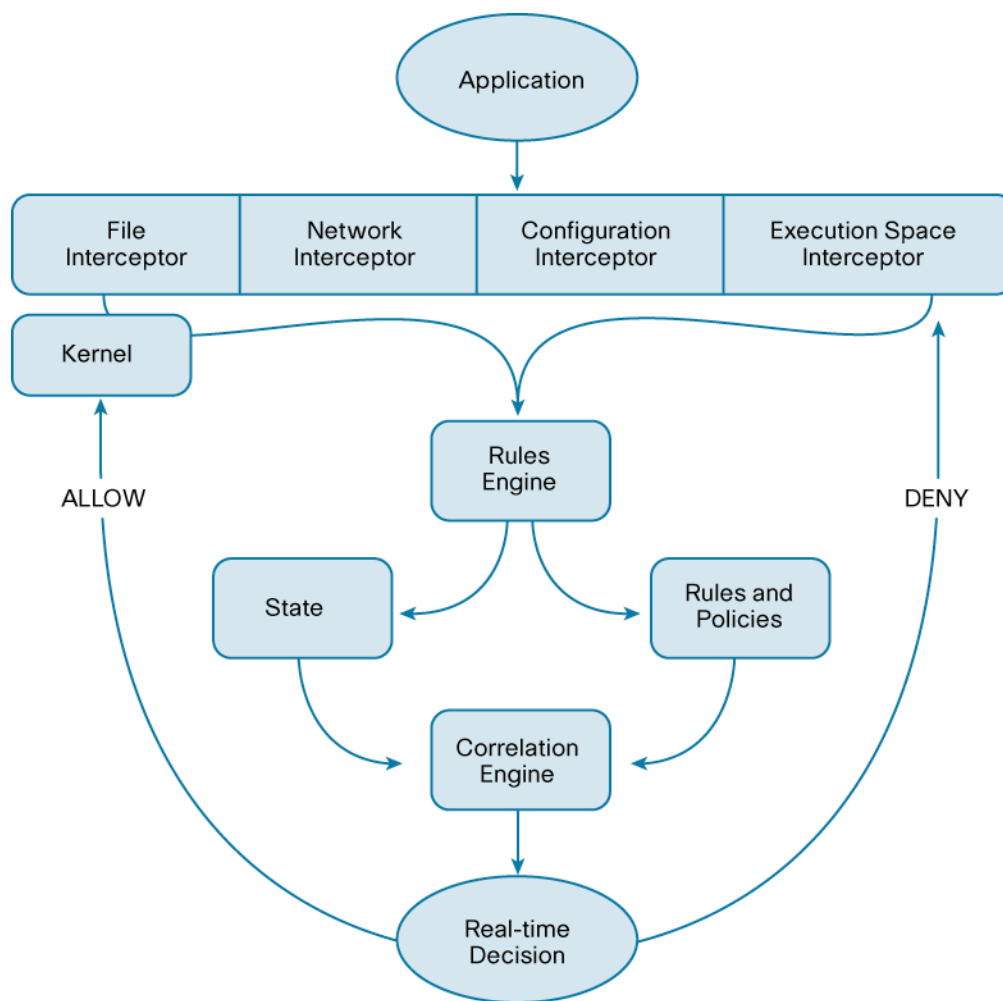
Cisco® Security Agent security software provides threat protection for server and desktop computing systems. Cisco Security Agent goes beyond conventional endpoint security solutions, providing an industry-leading defense against targeted attacks, spyware, rootkits, and day-zero attacks. Proactive protection is offered against unknown, never-seen-before threats, brand new exploits, and variants trying to take advantage of recently announced vulnerabilities. Cisco Security Agent provides “zero update” system integrity protection for critical servers that cannot be taken out of service to apply operating system or application-specific vulnerability patches. It helps reduce emergency patching of systems to respond to vulnerability announcements, minimizing patch-related downtime and IT manhour expenses. Organizations can now patch on their own schedule, not in crisis mode.

Robust policy compliance controls offer protection for sensitive data files and critical servers. Access to key files, applications, and servers can be monitored or controls enforced to stop inadvertent or malicious data loss. Removable media usage controls reduce risk and ensure workplace compliance. Granular controls may be put in place as needed to manage policy compliance for users, applications, systems, locations, and network addresses.

Agent Correlation

Cisco® Security Agent, installed on servers and desktops in the network, intercepts system calls between applications and the operating system, correlates them, compares the correlated system calls against a set of behavioral rules, and then makes an “allow” or “deny” decision based on the results of its comparison.

Figure 1. Graphical Representation of Cisco Security Agent Correlation

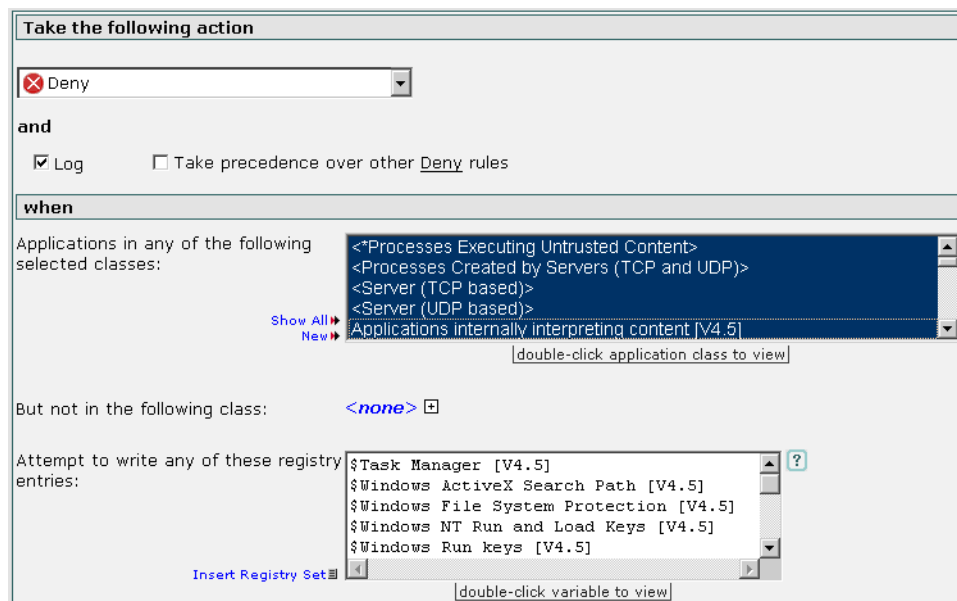


What Is Correlation?

Correlation is the act of establishing a relationship between events, things, or in the case of Cisco Security Agent, system calls. Cisco Security Agent correlation can also be described as the ability to keep system calls and application activities in “state.” For example, if an application on an endpoint writes a file to disk, Cisco Security Agent can “remember” that action and change how it protects the system in response.

Practically speaking, the agent uses correlation to tie some of its rules to application behavior, rather than application name. An example of this is the Windows Common Security Module. One of the rules in this module prevents vulnerable applications from modifying registry keys typically targeted by viruses. Rather than applying the rule to specifically named processes—such as `iexplore.exe`, `svchost.exe`, and `outlook.exe`—the rule is applied to any process exhibiting one of a set of behaviors. In this case, if any process on the system receives an unsolicited TCP or UDP network connection, Cisco Security Agent remembers it, treats the process as a “server” application, and dynamically applies the rule.

Figure 2. Vulnerable Processes Are Not Permitted to Write Dangerous Registry Keys

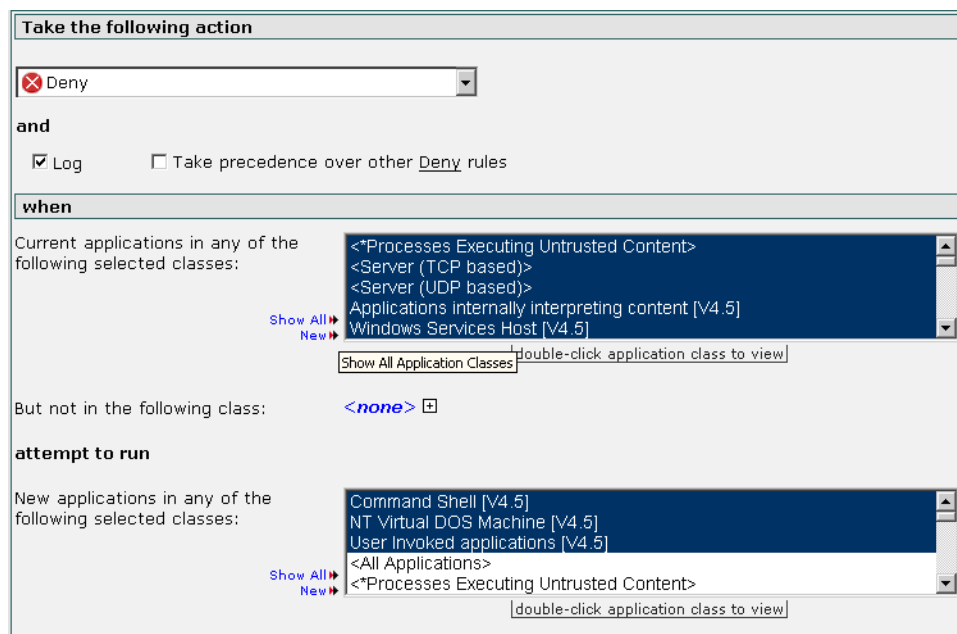


How Is Correlation Used?

First, correlation is used to make Cisco Security Agent more effective. One of the challenges associated with endpoint security is trying to determine which application or service could be the target for the next big attack. Cisco Security Agent doesn't force users to guess what might be a target—it allows administrators to dynamically assign rules based on application category.

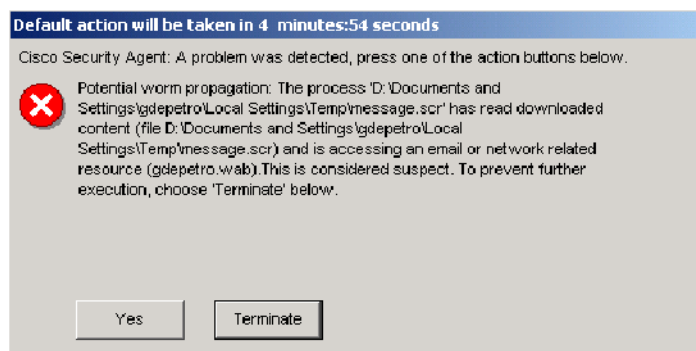
Attacks commonly manipulate endpoints by issuing commands using a command shell, so vulnerable applications should not be able to invoke command shells. The idea sounds simple, but knowing which specific processes might be vulnerable and cataloguing them is not. Correlation allows Cisco Security Agent to prevent vulnerable application categories such as “servers,” “processes created by servers,” or “processes executing untrusted content” from invoking command shells. The categories are automatically populated by Cisco Security Agent, based on previously observed actions.

Figure 3. Vulnerable Processes Are Not Permitted to Invoke Command Shells



Correlation can also be described as built-in defense-in-depth. When the MyDoom worm arrived via an e-mail message, for example, it installed itself by modifying system binaries, and then infected other systems by forwarding itself to everyone in the address book of the infected system. In systems running Cisco Security Agent, agent rules stopped the arrival and installation activities. Correlation tracked the worm at each stage of its lifecycle, remembered what it did, and took action, adding a third layer to Cisco Security Agent's defense.

Figure 4. Query Generated by the Network Worm Propagation Rule



Correlation also enhances interoperability. Although it might seem easier or safer to prevent command shells from running at all, they are constantly used for legitimate purposes—blocking them entirely would likely disrupt applications, generate helpdesk calls, and inhibit productivity.

Cisco Security Agent correlation automatically creates and dynamically maintains a “white list” of applications that are less vulnerable and should be able to invoke command shells. There are some exceptions, but for the most part any application can invoke a command shell until it becomes vulnerable. Correlation can remove applications from the list as well, so when a process is no longer vulnerable, it is allowed to run commands again.

Finally, correlation is used to increase the accuracy of Cisco Security Agent rules and policies. Cisco Security Agent can correlate numerous activities to improve its ability to make the correct decision about what is dangerous. The network worm propagation rule is a perfect example of this:

1. Any running process that acts as a client or server for a network service receives the Network Application “tag.”
2. Files written by Network Applications are considered to be Downloaded Content.
3. Files written by applications that have read Downloaded Content are also tagged.
4. Applications that access Downloaded Content are placed in a less-trusted class.
5. When an application in a less-trusted class tries to access certain objects, such as mail COM objects, mail.dll files, files used by mailers, an IRC client, or the TCP SMTP port, the network worm propagation rule is activated.

Correlation makes network worm propagation detection extremely accurate—four out of the five criteria must be met before the rule is activated. By itself, any one of the previously listed activities would not be cause for concern, but when they are put in context, it is clear that something abnormal is going on. Without correlation, Cisco Security Agent would likely have to flag each activity as potentially dangerous, generating numerous false positives.

Global Correlation

Events are correlated locally on the agent, as well as globally on the CSA Management Center, resulting in an extraordinary increase in accuracy when compared to signature-based host IDS/IPS systems. Global correlation correlates events received from the many server and desktop agents deployed. By looking at events across the enterprise, attacks that might have been missed will be detected. Attackers who send only a few (sometimes only one) packet to each host in the enterprise have traditionally been able to map the entire network while evading detection. These “distributed scans” would be detected by the CSA Management Center due to global correlation.

Benefits of Cisco Security Agent Correlation

- Cisco Security Agent is safer than other products—Cisco Security Agent can automatically determine which applications are more vulnerable to attack based on previously observed behavior. There is no need to predict which applications might be vulnerable, catalogue them, maintain a list, or download updated lists from product vendors.
- Cisco Security Agent is easier to deploy and manage—It allows less-vulnerable applications to operate with fewer restrictions. It also generates fewer false positives by putting potentially dangerous activities in context before taking action.
- Cisco Security Agent is tougher—Not only does Cisco Security Agent have default rules to stop malicious behavior at every phase in an attack’s lifecycle, but it can also track an attack’s activities and implement a final layer of defense based on a group of behaviors.

Resources for Cisco Customers

For Cisco Security Agent product information, visit: <http://www.cisco.com/go/securityagent>

**Americas Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSF, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0701R)