Threat Severity Assessment
The Symantec Security Response Threat Severity Assessment evaluates computer threats (viruses, worms, Trojan horses, and macros) and classifies them into clearly defined categories of risk for computer users. There are three major threat components that are analyzed to determine the severity rating:

- The extent to which a malicious program is in-the-wild
- The damage that a malicious program causes if encountered
- The rate at which a malicious program spreads

Based on an evaluation of its subcomponents, each category is rated as High, Medium, or Low risk. The overall severity measure, which is drawn from various combinations of risks, falls into one of five categories, with Category 5 (CAT 5) being the most severe and Category 1 (CAT 1) the least severe.

Threat Metrics
Following is a description of each threat component and their subcomponents.

**In-the-Wild**
The Wild component measures the extent to which a virus is already spreading among computer users. Information in this metric includes:
- Number of independent sites infected
- Number of computers infected
- Geographic distribution of infection
- Ability of current technology to combat threat
- Virus complexity

Classification guidelines for the Wild component include:
- High – 1,000 machines or 10 infected sites or five countries
- Medium – 50 to 999 machines or two infected sites or countries
- Low – Anything else

**Damage Caused**
The Damage component measures the amount of damage that a given infection can inflict. Information in this metric includes:
- Triggered events
- Clogged e-mail servers
- Deleted/modified files
- Release of confidential information
- Performance degradation
- Buggy routines that cause unintended loss of productivity
- Compromised security settings
- Ease of fixing damage

Classification guidelines for the Damage component include:
- High – File destruction/modification, very high server traffic, large-scale non-repairable damage, large security breaches, destructive triggers
- Medium – Non-critical settings altered, buggy routines, easily repairable damage, non-destructive triggers
- Low – No intentionally destructive behavior
Rate of Distribution
The Distribution component measures how quickly a program spreads itself. Information in this metric includes:

- Large-scale e-mail attack (worm)
- Executable code attack (virus)
- Spreads only through download or copy (Trojan horse)
- Network drive infection capability
- Difficult to remove/repair

Classification guidelines for the Distribution component include:

- High – Worms, network-aware executables, uncontainable threats (due to high virus complexity or low antivirus ability to combat)
- Medium – Most viruses
- Low – Most Trojan horses

Overall Risk Assessment Measure
The Overall Risk Assessment Measure unifies the three components above into a measure of risk to computer users. There are five severity threat categories, as described below.

Category 5 (Very Severe)
Highly dangerous threat type, very difficult to contain. All machines should download the latest virus definitions immediately and execute a scan. E-mail servers may need to come down. All three threat metrics—Wild, Damage, and Distribution—must be High.

Category 4 (Severe)
Dangerous threat type, difficult to contain. The latest virus definitions should be downloaded immediately and deployed. The Wild metric must be High and either the Damage or the Distribution metric must also be High.

Category 3 (Moderate)
Threat type characterized either as highly Wild (but reasonably harmless and containable) or potentially dangerous (and uncontainable) if released into the wild. The Wild metric must be High or both the Damage and Distribution metrics must be High.

Category 2 (Low)
Threat type characterized either as low or moderate Wild threat (but reasonably harmless and containable) or non-Wild threat characterized by an unusual Damage or spread routine or perhaps by some feature of the virus that makes headlines. Either the Wild metric must be Low or Moderate, or the Damage or the Distribution metric must be High.

Category 1 (Very Low)
Poses little threat to users. Rarely even makes headlines. No reports in the wild. Either the Wild metric must be Low and either the Damage or Distribution metric must be Low.
Event Severity Assessment

Security events are logical groupings of multiple attacks; the term “event” is used only by Symantec. A security event may include a group of similar but non-threatening individual attacks experienced by companies during the course of a day—for example, all non-threatening HTTP scans experienced during a single day are grouped into an event. A security event may also include multiple attacks against a single company by a single attacker during a specific period of time.

Every event validated by Symantec security analysts is assigned to one of four severity classifications: informational, warning, critical, and emergency. The primary purpose of this rating system is to prioritize client response to malicious activity based on the relative level of danger that the event presents to their environment.

A determination of severity is based on characteristics of an attack, defensive controls of the client, value of the assets at risk, and the relative success of the attack.

These four severity levels are further grouped into two classifications: severe and non-severe events. Severe events include activity classified as either “emergency” or “critical,” while non-severe events include activity classified as either “informational” or “warning.” For example, a severe event requires immediate countermeasures from an organization, while a non-severe event is mainly informative.

Event Severity Classifications

Following is a description of each event security classification.

- **Informational** – These are events consisting of scans for malicious services and intrusion detection system events that do not have a significant impact on the client’s network. Example: Scans for vulnerable services where all connection attempts are dropped by the firewall.

- **Warning** – These are events consisting of malicious attacks that were unsuccessful in bypassing the firewall and did not compromise the intended target systems. Example: Scans and horizontal sweeps where some connections were allowed but a compromise has not occurred.

- **Critical** – These events are malicious in nature and require action on the part of Symantec or the client to fix a weakness or actual exploit of the client network or devices. By definition, if a critical event is not addressed with countermeasures, it may result in a successful compromise of a system. Examples: 1) Continuous attacks by a single IP address against the client network or a significant vulnerability on the client’s network that was identified by either an attacker or the Symantec Security Response’s Security Operations Center (SOC). For example, a Web exploit is observed and appears to be successful, but there is no observed follow-up activity to take advantage of the vulnerability. 2) Unknown suspicious traffic that warrants an investigation by the client to track or eliminate the traffic flow.

- **Emergency** – These events indicate that a security breach has occurred on the client’s protected network. An emergency event requires the client to initiate some form of recovery procedure. Example: Successful exploit of a vulnerable Web server.
Severity Assessment

Threats, Events, Vulnerabilities, Risks

Vulnerability Severity Assessment

Vulnerability severity is a measure of the degree to which the vulnerability gives an attacker accessibility to the targeted system. It also measures the potential impact that successful exploitation of the vulnerability may have on the confidentiality, integrity, or availability of the information stored on or transmitted across the affected system. Symantec analysts calculate a severity score on a scale of 1 to 10 for each new vulnerability discovery.

The severity score is based on the following factors:

- **Impact** – The relative impact on the affected systems if the vulnerability is exploited. For example, if the vulnerability enables the attacker to gain full root access to the system, the vulnerability is classified as “high impact.” Vulnerabilities with a higher impact rating contribute to a higher severity score.
- **Remote exploitability** – Indicates whether the vulnerability can be exploited remotely. Vulnerabilities are classified as remotely exploitable when it is possible to exploit the vulnerability using at least one method from a position external to the system, typically via some type of communication protocol such as TCP/IP, IPX, or dialup. Vulnerabilities that are remotely exploitable contribute to a higher severity score.
- **Authentication requirements** – Indicates whether the vulnerability can be exploited only after providing some sort of credentials to the vulnerable system, or whether it is possible to exploit it without supplying any authentication credentials. Vulnerabilities that require no authentication on the part of the attacker contribute to a higher severity score.
- **Availability of the affected system** – Rates how accessible the system is to attackers in terms of exploitability. Some vulnerabilities are always exploitable once the attacker has accessed the system. Other vulnerabilities may be dependent on timing, the interaction of other objects or subjects, or otherwise only circumstantially exploitable. Increased availability of the affected system to attackers will increase the calculated severity.

After gathering information on these four attributes, analysts use a pre-established algorithm to generate a severity score that ranges from 1 to 10 and are categorized as high, moderate, or low severity based on the scores.

Vulnerability Severity Levels

Vulnerabilities are categorized as one of three of the following severity levels:

- **Low severity (0-3)** – Vulnerabilities that constitute a minor threat. Attackers cannot exploit these vulnerabilities across a network and successful exploitation does not result in a complete compromise of the information stored on or transmitted across the system. Low-severity vulnerabilities include non-critical losses of confidentiality (for example, system configuration exposure) or non-critical losses of integrity (for example, local file corruption).
- **Moderate severity (4-7)** – Vulnerabilities that result in a partial compromise of the affected system. An attacker may gain elevated privileges but does not gain complete control of the targeted system. Moderately severe vulnerabilities include those for which the impact on systems is high but accessibility to attackers is limited. This includes vulnerabilities that require the attacker to have local access to the system or to be authenticated before the system can be exploited.
- **High severity (8-10)** – Vulnerabilities that result in a compromise of the entire system if exploited. In almost all cases, successful exploitation can result in a complete loss of confidentiality, integrity, and availability of data stored on or transmitted across the system. High severity vulnerabilities will allow attackers access across a network (that is, remotely) without authentication.
Remotely Exploitable Vulnerabilities, Adjusted Severity
Because the majority of vulnerabilities are remotely exploitable, and remote exploitability raises severity, the overall severity composition of vulnerabilities is skewed towards having a higher severity. This metric attempts to compensate for this. The metric is computed using the severity rating formula with the remote exploitability criteria (as a weighted factor in the formula) removed. This metric only includes remotely exploitable vulnerabilities.

Ease of Exploitation
The ease of exploitation metric indicates how easily vulnerabilities can be exploited. The vulnerability analyst assigns the ease rating after thoroughly researching the need for and availability of exploits for the vulnerability.

All vulnerabilities are classified into one of the following three possible categories:

- Exploit Available – Sophisticated exploit code to enable the exploitation of the vulnerability is publicly available to all would-be attackers.
- No Exploit Required – Would-be attackers can exploit the vulnerability without having to use any form of sophisticated exploit code. In other words, the attacker does not need to create or use complex scripts or tools to exploit the vulnerability.
- No Exploit Available – Would-be attackers must use exploit code to make use of the vulnerability; however, no such exploit code is publicly available.

Security Risk Assessment and Classification
While security risks such as spyware and adware can be seen as an extension of the malware problem, the existing classification system for threats such as worms and viruses—which are always undesirable and should be automatically removed from a computer—does not fit this new category of potentially unwanted applications.

Given the important differences between malware threats and security risk programs, Symantec designed a risk classification system for rating adware and related applications that guides users to make informed decisions about what to keep and what to remove from their computers. Using a risk calculator, this system scores the overall impact of applications in four different categories, providing a final designation of the application as a “high,” “medium,” or “low” risk alongside a recommendation on how to proceed. This overall risk score and rating is used by Symantec’s LiveUpdate to ensure customers have up-to-date protection against spyware and other security risk programs.

The four categories used within the risk classification system include:

- Performance impact; this might include system instability, sluggish Internet connections, unusual browser behavior, increased pop-ups
- Privacy impact; this might include capturing and releasing confidential information, tracking and releasing surfing habits, or the absence of clear privacy policy
- Ease of removal; this might include avoiding uninstall, offering a non-functional or incomplete uninstall, or lacking an uninstall feature
- Stealth; this might include silent installs with little or no indication to the user, no user interface, concealment of application processes, or the lack of a legitimate EULA

There are times when a software vendor may feel that its product has been unfairly or inaccurately categorized by Symantec as a security risk program. When this occurs, Symantec offers an online form for vendors to submit an inquiry to Symantec for further examination and resolution. In addition, Symantec offers a Web-based form for reporting false positive detections of spyware and adware.