

# Symantec Threat Monitor, powered by Symantec DeepSight™

Screensaver: Get a view into the threat landscape right on your desktop

---

This document is intended to answer technical and general questions about the Symantec Threat Monitor screensaver.

---

## 1. What does this screensaver show?

The screen saver gives a high-level overview of the Internet threat landscape. It shows the number of attacks being reported from around the world, based on global data feeds from Symantec DeepSight™ Threat Management System and other sources in the Symantec™ Global Intelligence Network. It also provides some high level statistics about the most common attacks detected.

---

## 2. Can I share this screen saver with others?

Yes.

---

## 3. Can I use the screensaver to respond to security incidents?

No. This screen saver is for entertainment or informational purposes only. It is not meant to replace a comprehensive early warning or threat management system.

---

## 4. What is the Symantec DeepSight Threat Management System?

The DeepSight Threat Management System tracks security events on a global basis, providing early warning of active attacks. With personalized notification triggers and expert analysis, the system enables enterprises to prioritize IT resources in order to better protect critical information assets against a potential attack.

---

## 5. Why does the time/date display change in the upper-right corner?

The current time and date displayed in the upper-right hand corner of the screensaver will change according to which region is currently being zoomed in on by the screensaver.

---

## 6. What does “data last updated” in the upper-left hand corner mean?

The date and time indicate how old the data are. Threat information is time-delayed by approximately 8-12 hours. If your computer is connected to the Internet (“system online”) you will always receive the latest updates.

---

## 7. Is the screen saver displaying threat updates in real-time?

Threat information for the screensaver is time-delayed by approximately 8-12 hours. If your computer is connected to the Internet (“system online”), you will always receive the latest updates.

---

## 8. What is meant by an “attack”?

An attack is any detected activity that is malicious in nature such as attempts to exploit vulnerabilities in software, or malicious code infection attempts.

---

## 9. What does “number of events” mean?

The total count of attacks matching the description or region in the time period indicated.

---

## 10. What does “Top Countries Attacking” mean?

This shows the countries from which the most attacks are originating.

### 11. What does “Top Firewall/IDS events” mean?

This shows the most commonly detected attacks by firewall and Intrusion Detection Systems (IDS).

---

### 12. What is a Security Operations Center?

The Symantec Security Operations Centers are a key part of the Symantec™ Managed Security Services infrastructure. Partnering with Symantec skilled and experienced analysts and engineers, Symantec Managed Security Services has market-leading security analysts, proven best practices for delivering a consistent, global service and sophisticated technology to keep your infrastructure available and secure. Managed Security Services provides a mature approach to business continuity and disaster recovery with a global redundant infrastructure that provides failover across four Security Operations Centers worldwide.

- Receive over 2 billion security alerts daily
  - Over 40,000 devices under management
  - 100% GIAC Certification for Analysts
  - Security Technology and Response team of more than 500 experts
  - Security Operations Centers are SAS70 Type II and ISO 27001 compliant
- 

### 13. What is ThreatCon? What do the different levels (1-4) mean?

The Symantec ThreatCon rating is a measurement of the global threat exposure, delivered as part of Symantec DeepSight Threat Management System. Level 1 is the lowest threat level, and Level 4 is the highest. A detailed description of each threat level follows below.

#### **ThreatCon Level 1**

**Low: Basic network posture** - This condition applies when there is no discernible network incident activity and no malicious code activity with a moderate or severe risk rating. Under these conditions, only a routine security posture, designed to defeat normal network threats, is warranted. Automated systems and alerting mechanisms should be used.

#### **ThreatCon Level 2**

**Medium: Increased alertness** - This condition applies when knowledge or the expectation of attack activity is present, without specific events occurring or when malicious code reaches a moderate risk rating. Under this condition, a careful examination of vulnerable and exposed systems is appropriate, security applications should be updated with new signatures and/or rules as soon as they become available and careful monitoring of logs is recommended. Changes to the security infrastructure are not required.

#### **ThreatCon Level 3**

**High: Known threat** - This condition applies when an isolated threat to the computing infrastructure is currently underway or when malicious code reaches a severe risk rating. Under this condition, increased monitoring is necessary, security applications should be updated with new signatures and/or rules as soon as they become available and redeployment and reconfiguration of security systems is recommended. People should be able to maintain this posture for a few weeks at a time, as threats come and go.

#### **ThreatCon Level 4**

**Extreme: Full alert** - This condition applies when extreme global network incident activity is in progress. Implementation of measures in this Threat Condition for more than a short period probably will create hardship and affect the normal operations of network infrastructure.

#### 14. Under “Threat Rating”, what do the following terms mean?

**Severity:** This rates the severity of malicious code or vulnerability on a scale of 0 (low) to 10 (high). The rating of a malicious code's severity depends on what security properties and system objects an organization finds more important. Severity is based on the malicious code's effect on the following: availability (malicious code), confidentiality, and/or integrity. Severity of a vulnerability is based on the weighted values of impact, availability, authentication, and remote fields.

**Impact:** This field rates the impact of malicious code or vulnerability on a scale of 0 (low) to 10 (high). For malicious code, impact means the compounded affect of the impact of each action performed by the malicious code. It is calculated by ordering the individual payload impact ratings from highest to lowest, setting the overall impact to the highest rating, then incrementally adding to the overall rating the scaled difference between each lesser impact rating and the last. For a vulnerability, the numerical value is determined by a formula based on the value of the security properties lost, the privilege obtained, and the objects affected.

**Urgency:** This rates the urgency of the vulnerability on a scale of 0 (low) to 10 (high). It implies the priority that should be placed on fixing or mitigating the vulnerability. It is based on the weighted values of severity, ease, and credibility.

**Risk:** The risk rating is an overall assessment of hazards posed by an instance of a malicious code or a security risk. The degree of risk is calculated from the values of *Infection Potential*, *Prevalence*, *Impact*, and *Target Distribution*. The rating ranges from a low of 1 to a high of 5.

---

#### 15. What are the “crawlers” along the bottom of the screensaver?

The two crawlers along the bottom provide additional information about Symantec's security leadership. These crawlers highlight awards Symantec has received for its consumer and enterprise security products and also highlight key research findings from Symantec Global Intelligence Network and Symantec Internet Security Threat Report.

---

#### 16. What are the minimum hardware requirements to run the screensaver?

**Windows®:**

Intel Pentium II 450Mhz, AMD Athlon 600Mhz or faster processor (or equivalent); 128MB of RAM or greater.

**Mac®:**

PowerPC G3 500Mhz or faster processor; Intel Core Duo 1.33Ghz of faster processor; 128MB or RAM or greater.

---

#### 17. What operating systems are supported?

Windows® 98, Me, XP, Vista®, Vista 64 and Windows 7

Mac OSX® 10.2 – 10.5.

*An update of the screensaver for OSX 10.6 "Snow Leopard" will be available soon.*

---

#### 18. What resolutions does this screen saver support?

640x480; 800x600; 1024x768; 1200x1024; 1600x1200

---

#### 19. Do I need any other programs to run the screensaver?

The screensaver requires Adobe Flash Player 9 or greater, which is included with the screensaver.

## 20. Has this screensaver been tested for security vulnerabilities?

Yes. Symantec has conducted a thorough security evaluation for the screensaver.

---

## 21. Do I need to be connected to the Internet to run the screensaver?

An Internet connection is required to download the latest threat information from Symantec DeepSight, however, the screensaver will run even if no connection is available. The screensaver must connect at least once to the Internet to cache the data feed.

---

## 22. How do I install the screensaver?

### For Windows users:

Download the installer to a convenient place (such as your desktop) and double-click “Symantec Threat Monitor”. Follow the on-screen instructions to complete the installation.

### For Mac users:

Download the ZIP file to a convenient place (such as your desktop). Double-click the ZIP file to extract the installer. Once extracted, double-click “Symantec Threat Monitor” and follow the on-screen instructions to complete the installation.

---

## 23. How do I uninstall the screensaver?

### For Windows users:

Go to, Start > Control Panel > Add Remove Programs, and look for “Symantec Threat Monitor” in the program list. Click “Remove” and follow the on-screen instructions.

### For Mac users:

On your menu bar click the Apple® Logo > System Preferences > Desktop & Screen Saver. Select “Symantec Threat Monitor” from the Screen Savers list. Click the “Options” button. In the dialog that drops down, click the Delete button and follow the on-screen instructions.

---

## 24. I am not able to change my screen saver. What can I do?

### For Windows users:

Go to, Start > Control Panel > Display. Select the “Screen Saver” tab in the Display Properties window that popped up. Under the drop-down list, select “Symantec Threat Monitor”.

### For Mac users:

On your menu bar click the Apple Logo > System Preferences > Desktop & Screen Saver. Select “Symantec Threat Monitor” from the Screen Saver list.

---

## 25. I got an error message when I was trying to install the screensaver. What should I do?

If you experience problems with the installation, you can try any of the following solutions:

- Download the installer again. Your download may have become corrupted.
- Reboot your computer and try the re-installing the screensaver.
- Make sure you have all the latest security updates applied to your operating system.
- Make sure your computer user account has permission to install new applications.

**26. The screensaver runs very slowly and the animations do not move very smoothly. What should I do?**

- Please verify that your computer meets the minimum requirements (see earlier question about requirements)
  - Check to see that you have the latest video card drivers installed.
  - Make sure you do not have any processes running in the background that could be consuming large amounts of system resources.
- 

**27. I am running the screensaver on dual monitors and the screensaver runs very slowly and the animations do not move very smoothly. What should I do?**

- Please verify that your computer meets the minimum requirements (see earlier question about requirements)
  - Check to see that you have the latest video card drivers installed.
  - Make sure you do not have any processes running in the background that could be consuming large amounts of system resources.
- 

**28. The screensaver crashed unexpectedly. What should I do?**

If you are experiencing crashes, try re-installing the screensaver by downloading the latest version from the screensaver website at <http://go.symantec.com/screensaver>.

---

**29. I received a Macromedia Flash Player Settings pop-up on my screen. What should I do?**

The pop-up is likely asking for permission to increase or decrease the local storage space being granted to Flash. The screensaver requires a few kilobytes to store temporary information on your hard disk so that it may operate even if you are not connected to the Internet. You may grant the screensaver more storage space by sliding the slider bar up several notches or by simply clicking on “grant”.

---

**30. I received an Adobe® security pop-up on my screen. What should I do?**

The pop-up is likely asking permission for the screensaver to access the Symantec DeepSight servers to get an updated data feed. Click “Settings” to enable this.

---

**31. Does the screensaver store any information on my hard drive?**

The screensaver will temporarily store a text copy of the threat information it obtained from the server. It does this so that it can operate even if you do not have an active Internet connection. All such information is stored in a flash “cookie” in the specially designated directory provided by the Flash player.

---

**32. Where can I get support for the screensaver?**

We are not providing live technical support for this screensaver. However, you can get additional information at <http://go.symantec.com/screensaver>.

---

**33. When will there be an updated version?**

Symantec will periodically release newer versions of the screensaver. The screensaver will notify you when a new update is available.

**34. How can I use this on a kiosk screen (non-screen saver mode)?**

Please contact [screensaver\\_feedback@symantec.com](mailto:screensaver_feedback@symantec.com) to obtain a kiosk version of the screensaver.

---

**35. How can I submit bugs or errors?**

Submit any bugs or errors to the Security Forum on Symantec Connect at <http://www.symantec.com/connect>

---

**36. How can I make suggestions for improvements?**

Please send an email to [screensaver\\_feedback@symantec.com](mailto:screensaver_feedback@symantec.com) or make a suggestion to the Security Forum at <http://www.symantec.com/connect>

---

*Download the screensaver*

<http://go.symantec.com/screensaver>

*To submit questions or feedback*

Contact us at: [screensaver\\_feedback@symantec.com](mailto:screensaver_feedback@symantec.com)

*About Symantec*

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.