

# SOPHOS

## SOPHOS ANTI-VIRUS



**Sophos Anti-Virus** съвместява в себе си всички функции по откриването и отстраняването на компютърни вируси от сървъри, работни станции и преносими компютри. Мобилните устройства се предпазват от заразяване по време на синхронизация. Sophos предоставя три вида сканиране за вируси - при достъп, при поискване и с разсрочено изпълнение. Чрез вградената уникална технология за интелигентен подбор, системата избирателно сканира само определени файлове в които се предполага наличието на вируси, като по този начин значително се намалява процесорното време изразходено за сканиране за вируси и се освобождават ресурси за други приложения. Sophos Anti-Virus притежава мощни инструменти за централизирана инсталация, конфигуриране, обновяване и справки.

### Начин на работа

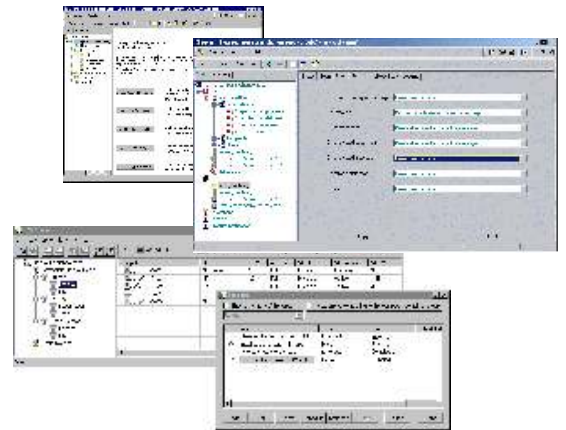
За сканиране за вируси Sophos Anti-Virus използва вградения Sophos Virus Detection Engine.

Патентованата от Sophos технология InterCheck чувствително оптимизира сканирането при достъп. Използват се комбинации от сканиране и контролни суми с цел намаляване на броя на проверките за всеки отделен файл, като в същото време нивото на сигурност не намалява.

Инсталацията, конфигурацията и обновяването се контролират централизирано. Набор от инструменти за управление позволява на администраторите да наблюдават и контролират мрежата, като по този начин отпада необходимостта от каквато и да била намеса на крайни потребители.

Sophos Anti-Virus се инсталира в централна инсталационна директория от която сървърите и работните станции автоматично изтеглят последните версии и обновяват своя софтуер.

Enterprise Manager се грижи за поддръжката на централната инсталационна директория, като автоматично на предварително зададени интервали изтегля през Интернет последните версии от базата данни на Sophos. След него идват наред SAVAdmin, който управлява обновяването по цялата мрежа и на Remote Update осъществяващ обновяването на отдалечените компютри.



**MailMonitor** следи целия трафик през SMTP, NOTES и Exchange 2000, включително прикачените файлове архивирани със ZIP или други подобни програми. Намирането и отстраняването на вируси се осъществява от високоскоростния Sophos virus engine, който се грижи за незабележимото за потребителите обновяване с последните вирусни дефиниции. Развита система за известяване уведомява администратора, получателя и изпращача на дадено съобщение в случай на откриване на вирус в него.

### Начин на работа

Sophos virus engine се инсталира едновременно с инсталацията на MailMonitor.

Веднъж инсталиран MailMonitor прихваща и сканира целия входящ и изходящ трафик на електронната поща. Работи в три режима:

**Директен:** сканирането на пощенските кутии и бази данни са стартира при поискване.

**По програма:** сканирането се осъществява в предварително зададени дни и време.

**В реално време:** прихваща и сканира всеки e-mail и прикачен файл по време на изпращане или получаване.

Чистите от вируси писма се насочват към пощенския сървър, а инфектираните прикачени файлове се почистват, изтриват или поставят под карантина.

Специален модул за намаляване на опасността от заразяване (само за SMTP) позволява на администраторите да блокират:

- Файлове според тяхното разширение или име;
- Windows или DOS изпълними файлове, дори и тяхното разширение да е сменено с друго с цел да не бъдат разпознати;
- Всички съобщения със специфичен текст в темата;
- Всички масови писма с повече от един получател.

# SAVAdmin

**SAVAdmin** е визуален инструмент за управление, който прави инсталацията, поддръжката и работата на Sophos Anti-Virus с множество свързани мулти-сървърни мрежи лесна, бърза и удобна. Чрез него Sophos Anti-Virus може да бъде разпространен из огромна система само от една централна машина и само с една единствена операция, изключваща каквато и да била по нататъшна намеса на оператор.

SAVAdmin намалява опасността от вирусни атаки срещу фирмената компютърна мрежа, като дава справки за всички машини, които не са защитени или ползват остарели вирусни дефиниции. Всяка една машина идентифицирана като недобре защитена, може незабавно и автоматично да бъде обновена с последната версия на антивирусния софтуер.

## Начин на работа

SAVAdmin дава възможност за графично избиране на отдалечени сървъри, работни станции и преносими компютри, които разполагат с инсталиран софтуер на Sophos.

Централните инсталационни директории на мрежовите машини съдържат дистрибутивни копия на Sophos Anti-Virus за Windows. Веднъж създадена, централната инсталационна директория започва да служи като източник от който всички останали компютри започват да извличат последните версии на софтуера. Разполагайки със SAVAdmin администратора на системата може да обновява тази директория дистанционно.

След като е създадена и в следствие обновена, централната инсталационна директория може да бъде използвана от всички компютри за автоматично обновяване без да е необходима намеса на потребител или на администратор, чрез SAVAdmin. В същото време SAVAdmin може да "надзирава" процеса по обновяването в реално време.

На практика, мрежа от над 1000 машини може да бъде обновена само от един администраторски компютър за по малко от пет минути.

SAVAdmin може да бъде използван самостоятелно или в комплект с Enterprise Manager, който автоматично изтегля най-новите вирусни дефиниции от централната база данни на Sophos.

## sav interface

**SAV interface** позволява на софтуерните доставчици да интегрират вирусната защита на Sophos в тяхното оборудване, като firewalls, gateways и други защитни решения. Високо скоростните канали в софтуера на Sophos позволяват всички видове вируси да бъдат откривани с минимален разход на системни ресурси и висока скорост на действие. При откриване на вирус, SAV interface предоставя възможност за дезинфекция и подробна информация за открития вирус.

## Начин на работа

SAV interface се инсталира като част от Sophos Anti-Virus.

Във Windows NT се интегрира като COM-съвместим DLL, а в останалите платформи като споделени библиотеки. Нуждае се от едно единствено копие на вирусната база данни за да отговори на всичките стандартни изисквания и условия за подобен command line вирус скенер. Това води до чувствително повишаване на производителността.

## enterprise manager

**Sophos Enterprise Manager** обобщава пакет от мощни инструменти даващи възможност на всеки администратор да управлява и конфигурира Sophos Anti-Virus за кратко време и с минимални усилия.

Enterprise Manager се грижи за автоматизираното изтегляне на последните вирусни дефиниции от централните сървъри на Sophos. След това поема тяхното разпространение по работните станции и сървърите в локалната мрежа, а също така генерира справки за откритите вируси.

## Начин на работа

Enterprise Manager обединява пет компонента:

- **Sophos Databank:** Интернет сайт съдържаш последните вирусни дефиниции и версии на Sophos Anti-Virus. Осигурява навременното и надеждно обновяване.
- **EM Library:** изтегля нови версии от базата данни при поискване или през оказани интервали от време. Записва ги в централната инсталационна директория от където работните станции и сървърите се обновяват самостоятелно и автоматично.
- **EM Reporter:** позволява лесно и бързо извличане на справки за състоянието на антивирусната защита на мрежата благодарение на автоматичното обработване и записване на всички сигнали за вируси генерирани от Sophos Anti-Virus по работните станции.
- **EM Console:** служи за конфигурирането на Enterprise Manager Library и EM Reporter.
- **SAVAdmin:** използва се за инсталиране на антивирусния софтуер по всички машини. Дава възможност за управление, контрол и извличане на справки от системата в реално време.



### Официален представител за България:

НЕМЕЧЕК ООД, 1202 София; ул. Индустриална №11;

Тел: 02/ 9178 690; Факс: 02/ 9178 696; e-mail: office@nemetschek.bg

# SOPHOS