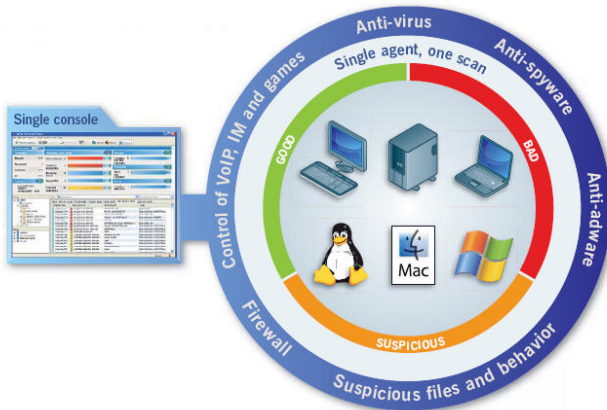


### endpoint security and control



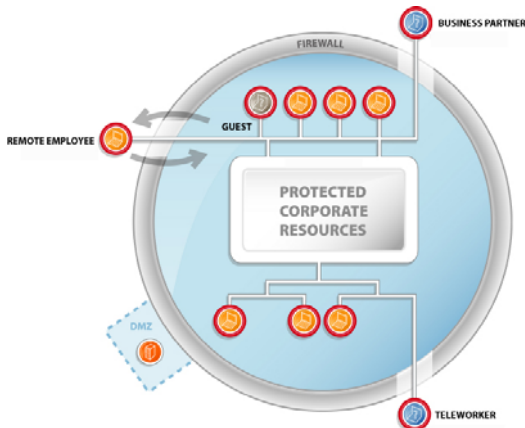
Sophos Enterprise Security สนับสนุนระบบปฏิบัติการ 25 Operation System platform, Single Scan Single Engine ประกอบด้วย 6 Modules ได้แก่

1. Anti Virus โดยใช้เทคโนโลยี Genotype และ Decision Caching โดยการ Update Virus Signature < 5 Kb
2. Anti Spyware/Adware ป้องกันโปรแกรมที่ไม่พึงประสงค์ที่ทำให้เกิดความเสียหายกับคอมพิวเตอร์
3. PUA (Potentially Unwanted Application) ตรวจสอบและป้องกัน (Remove) โปรแกรมต่างๆ ที่รบกวนการทำงาน
4. Client Firewall ซอฟต์แวร์ที่ทำหน้าที่เสมือนกำแพงป้องกันการบุกรุก เข้าสู่เครื่องคอมพิวเตอร์ บนเครื่อง Clients
5. Application Control ควบคุมการใช้งาน Application ได้แก่ Instance Messaging, P2P, VoIP ,Gaming Software , File Sharing (Bit Torrance , eMule)
6. HIPS (Host Based IPS) เทคโนโลยีขั้นสูงของ Sophos (Behaviour Genotype) ป้องกันการโจมตีแบบ Unknown Threat (Runtime Analysis, Buffer Overflow, Unique Pre-Execution Protection, Proactively Detecting Malware, Suspicious files and behavior)

### sophos nac

ADVANCED Software ควบคุมจำกัดสิทธิ์ การเข้าใช้งานทรัพยากรของ ระบบ Network ของ เครื่องคอมพิวเตอร์

ลูกข่าย ทั้งที่รู้จัก และไม่เป็นที่รู้จัก โดยสามารถควบคุมและตรวจสอบ ได้จากส่วนกลาง ประกอบด้วย



1. การตรวจสอบการ update, install โปรแกรมต่างๆ มากกว่า 148 antivirus from 25 vendors  
มากกว่า 41 anti-spyware from 18 vendors  
มากกว่า 32 firewall from 9 vendors
2. การกำหนดสิทธิ์ในการเข้าถึงระบบ network ตาม Group ที่กำหนด
3. การประเมินระบบความปลอดภัย โดยสามารถทำการ ตรวจสอบเครื่องคอมพิวเตอร์และแสดงผล

Sophos nac ง่ายต่อการติดตั้งใช้งาน เนื่องจากเป็น Software base (Server/Client) โดยไม่อ้างอิงอุปกรณ์ Network ชนิดใด ชนิดหนึ่ง โดยสามารถรองรับการทำงาน ที่เป็นระบบ Active Directory, LDAP, IEEE802.1x and Radius

### Genotype Technology:

Sophos ใช้เทคโนโลยีขั้นสูงที่เรียกว่า Genotype โดยทำการเก็บรวบรวม ข้อมูลของไวรัสแต่ละชนิด และแบ่งสายพันธุ์ต่างๆ ตาม Characteristics เช่น แบ่งตามลักษณะการทำงาน หรือการโจมตี เพื่อง่ายต่อการตรวจจับ แม้มีการเปลี่ยนชื่อ ไวรัส หรือเปลี่ยน Version ก็สามารถตรวจจับได้ โดยไม่จำเป็นต้องออก Signature Virus ใหม่

### Decision Caching Technology:

เป็นการจดจำ File ที่ได้ทำการ scan ไว้แล้ว ซึ่งเมื่อ มีการ Scan File ในครั้งต่อไปกรณีไฟล์ ไม่มี การเปลี่ยนแปลง หรือไม่ได้เปิดใช้งาน จะทำการ Skip ข้ามการ Scan จึงทำให้ระยะเวลา Scan File ทำได้อย่างรวดเร็ว

### Endpoint Security and Control:

- ป้องกันระบบทุก Platform ได้แก่ Windows , Windows Mobile, Macintosh, Linux, NetWare, UNIX and NetApp Storage Systems
- Management Console 1 เครื่อง สามารถ ควบคุม anti-virus, client firewall, HIPS Application Control โดยสามารถจัดการ เครื่องคอมพิวเตอร์ลูกข่ายได้มากถึง 50,000 เครื่อง และสามารถ ควบคุม การใช้งานข้ามระบบ Platform ได้แก่ เครื่องคอมพิวเตอร์ ที่เป็น Mac และ Linux

### Sophos NAC Advance:

- จำกัดสิทธิ์เครื่องคอมพิวเตอร์ ที่ไม่ได้รับอนุญาต เข้าใช้งานในระบบเครือข่าย แบบ Real Time
- ควบคุมจากส่วนกลาง ในการกำหนด Policy การเข้าถึง ทรัพยากรระบบของเครื่องคอมพิวเตอร์
- Install Agent บนเครื่องคอมพิวเตอร์ที่ต้องการ ควบคุมหรือผ่านทาง Web Agent เพื่อตรวจสอบ เครื่องคอมพิวเตอร์ที่ไม่เป็นที่รู้จักและ ตรวจสอบ สิทธิ์ ในการใช้งานทรัพยากรระบบ
- ป้องกันเครื่องคอมพิวเตอร์ที่ไม่ได้รับอนุญาต ให้ ใช้งานระบบ โดยผ่าน ทาง DHCP Server

## Sophos Solutions

### sophos email security APPLIANCES



Sophos Email Security Appliance ประกอบด้วย

- Sophos Antivirus Engine / Sophos Spam Engine
- Sophos IP Block list
- Active Directory integration
- Postfix MTA (mail transfer agent)

End-to-end message forensics ง่ายต่อการค้นหา Message log และ Quarantine Message มีการจัดเก็บข้อมูล การรับเข้า-ส่งออก email ของผู้ใช้งาน ภายในตัวอุปกรณ์

### puremessage

FOR UNIX โปรแกรมป้องกัน Email Gateway โดยติดตั้งบนเครื่องคอมพิวเตอร์ที่มีระบบ

ปฏิบัติการตระกูล UNIX มีความยืดหยุ่นสูงในการใช้งาน รองรับระบบที่มีขนาดใหญ่ ประกอบด้วย

- Sophos Antivirus Engine / Sophos Spam Engine
- Sophos IP Block list
- LDAP Support
- Postfix MTA (mail transfer agent)
- More 800 Perl Script สำหรับตรวจสอบ Spam Mail
- Sub-domain delegation สามารถกำหนดสิทธิ์ผู้ควบคุมระบบได้ในระดับ domain ย่อยได้
- Extended policy สามารถกำหนด email policy สำหรับแต่ละกลุ่มของผู้ใช้งานได้
- Quarantine Digest การส่งจดหมายแจ้งเตือนไปยัง ผู้ใช้งานระบบ เพื่อให้ทราบถึง Spam Message ที่ทำการ quarantine ไว้ โดยสามารถกำหนดระยะเวลาตามที่กำหนด
- end-user-quarantine สามารถทำการค้นหา ตรวจสอบ Message Quarantine ได้ด้วยตนเอง รวมทั้งการทำ black list/ write list

### web security and control

ป้องกันเครื่องคอมพิวเตอร์จากการใช้งาน Internet ประกอบด้วย

Full-Spectrum detection ป้องกันการใช้งาน HTTP, HTTPS, FTP โดยสามารถตรวจจับ

- Virus, Spyware/Adware
- Trojans, Worm, Phishing
- Unwanted offensive word
- Application Control

URL filtering จำแนกแยกแยะ website

ที่ไม่พึงประสงค์ เพื่อป้องกันการเข้าใช้งาน

Sophos Web Security ง่ายต่อการติดตั้งโดยสามารถติดตั้งในรูปแบบ Explicit proxy, Transparent proxy,

Bridged proxy. ป้องกันการเข้าใช้ Website ที่ไม่เหมาะสม จากฐานข้อมูลของ Sophos ตาม catalog

ดังนี้ Entertainments, Communication, Media, Search, Questionable



### Sophos Email Security Appliance:

- ป้องกัน Spam mail ได้ 99%
- Update อัปเดตอัตโนมัติ ทุกๆ 5 นาที
- ป้องกัน Spam, Virus, Spyware and Trojans ทั้ง inbound and outbound.
- ป้องกัน Images Spam, PDF Spam
- ระบบปฏิบัติการ Hardened FreeBSD Operating System
- Management ผ่านทาง Web Interface ง่าย ต่อการติดตั้ง และใช้งาน
- End user interface for message quarantine

### Sophos Pure Message for Unix :

- ป้องกัน Spam, Virus, Spyware and Trojans ทั้ง inbound and outbound
- Software base สามารถติดตั้งใช้งานในระบบปฏิบัติการที่เป็น Linux, Sun Solaris, FreeBSD ทั้ง 32bit และ 64bit
- Automatic update from Sophos Labs หากค้นพบ virus หรือ new spam
- รองรับการใช้งาน Postfixหรือ Sendmail
- บริหารจัดการผ่าน Web-based หรือ command line
- รองรับการทำงาน multiple server สามารถบริหารจัดการจากส่วนกลาง รวมทั้ง quarantine message จากส่วนกลาง

### Sophos Web Security:

- Full-Spectrum detection Single engine one pass URL, Spyware, AV
- ระบบปฏิบัติการ Linux Operating system ที่ทำการ optimized for Sophos
- Management ผ่านทาง Web Interface ง่าย ต่อการติดตั้ง และใช้งาน
- Active Directory Integration
- Build in on board Proxy , Caching
- URL filtering แบ่งระดับการ Scan จากฐานข้อมูลของ Sophos โดย แบ่งระดับ High, medium, Lower Site เพื่อความรวดเร็วในการ Scan และใช้งาน

Z DNA Corporation Co., Ltd.



2549/43 Phaholyotin Park Place Building Tower E, 1<sup>th</sup> Floor,

Phaholyotin Rd., Lardyao, Chatuchak Bankok 10900

Tel. +66 2942 7093-4 Fax. +66 2 942 7096

www.zdna.co.th

SOPHOS  
WWW.SOPHOS.COM

