MUCH MORE THAN ANTI-VIRUS

Our business security solutions bring in the best technologies and tools to keep your business safe against all threats.

Protection technology	Why	Benefits
Security Cloud	New threats are created at an ever-growing pace. Endpoint protection technologies need to be intelligent and efficient in order to block these threats. By utilizing cloud technologies, as new threats appear, endpoints are instantly protected.	• Global malware behavior tracking enables us to examine how suspected malicious programs behave globally and are spread between computers, countries and continents • Sharing threat data forms a protective network and all users will subsequently benefit from this data and receive protection faster and more accurately
DeepGuard	DeepGuard 5 introduces enhanced behavior-based detection logic, including monitoring the runtime behavior of commonly targeted programs and potential attacks. This broad behavioral analysis approach allows DeepGuard to identify and intercept exploit-based attacks, regardless of the specific vulnerability targeted.	• Proactive, on- the-fly monitoring and interception serves as the final and most critical line of defense against new threats, even those targeting previously unknown vulnerabilities • Recognizes and blocks suspicious activity at multiple layers of operation • Reduces potential loss of sensitive data or privacy due to malware infection
Hydra	Allowing the malware to execute to detect its nefarious behavior is dangerous, and executing each file in a sandboxed environment before allowing it to be accessed is slow. Hydra detections based on scripted reverse engineering of the file content allow us to detect and block malware in a very fast and efficient manner.	• Hydra enables us to create highly generic malware and exploit kit family detections by very fast scripted reverse engineering of files • Hydra exists for Windows, Mac OS X and Linux, and any version of it can detect malware for all three platforms

F-Secure

KEY SECURITY FEATURES

Feature	Why	Benefits
Software Updater	Outdated software is the cause of up to about 85% of cyber security incidents. Keeping all software up to date is an easy way to avoid breaches based on known vulnerabilities.	• Unique way to easily and automatically deploy security updates for third party software • Automatic protection against known threats – no more unnecessary gaps in your protection
Web Content Control	About 90% of normal attacks come through the web. Certain sites are very typically sources for malware attacks, therefore blocking out certain pages based on category (e.g. gambling, entertainment) will enhance security.	• Helps prevent malicious content from entering the organization's network. • Reduce productivity losses, bandwidth consumption, and legal risks caused by unauthorized employee access to inappropriate or distracting web content
Connection Control	The weakest link of e.g. an online banking session is usually the web browser session. By blocking other connections, banking Trojans and other malware cannot send your private information, such as user credentials, to criminals.	• Improve security through controlled and safe access to business critical assets • Allows connections during the session to sites which are verified safe by F-Secure • The administrator can configure it to be enabled not just for the online banking sites but to whatever HTTPS website (e.g. CRM)
Web Traffic Scanning Advanced Protection	Certain technologies, such as Java, Flash, Windows, Silverlight, executables, and Active X components are typical targets for exploit kits. By blocking these contents the organization can already stop quite a lot of incidents.	• Provide an extra layer of protection to block out typical potentially harmful content • Block 100% of Java applets and Windows malware that come from unknown sources you do not trust • Protects the user from typically vulnerable content from websites
Virtual Security / Offload Scanning Agent	Traditional scanning in virtual environments takes up a lot of resource from the hardware, is difficult to manage, and has higher costs and a high performance impact.	• Offloading the resource-heavy scanning to a dedicated Scanning and Reputation Server offers optimized performance for all virtual environments • Virtual Security offers the same top-quality protection level to virtual environments as the F-Secure client solutions offer for onsite environments
Botnet Blocker	Most malware attacks are based on botnets. Botnets need to be able to communicate, usually through the Command & Control domains. Administrator can prevent network activity relating to known botnets by blocking access to malicious domains.	• Botnet Blocker stops criminals aiming to control compromised assets by preventing communication to Command & Control domains • It adds a layer of protection to catch malware at different stages • This results in an effective way to disable Botnet operations

F-Secure