F-SECURE BUSINESS SUITE

Solution description

F-Secure

CONTENTS

DISCLAIMER: This document gives a high-level overview of the key security components in Business Suite.

F-Secure is constantly improving its services. F-Secure reserves the right to modify features or functionality of the Software in accordance to its product life cycle practices.

1. EXECUTIVE SUMMARY

Cyber security is a process that starts with prediction – understanding the risks, knowing the attack surface and uncovering the weak spots. A layered security model minimizes your attack surface and prevents cyber security incidents.

Today's cyber security is built on layers that stop cyber attacks at different stages of the chain of compromise. Layered security, or defense in depth, protects your infrastructure and assures a fast and cost-effective reaction to cyber security incidents. Endpoint security is a core element of cyber security today in protecting the public cloud, private clouds, and on-premises infrastructure and workloads.

Business Suite offers the best protection for businesses of all sizes, as proven by its success in several external tests over the years. In addition, Business Suite provides scalability for large organizations with complex company structures and IT environments.

The advanced and automated features of Business Suite are built to offer control over the security of the whole environment. Administrators are able to control what is allowed within the organization's network, private and public clouds, and the automated tools make everyday security management easy and efficient, saving time for other tasks. Our certified partners offer support and services for customers all over the world. We, together with our partners, have flexible and transparent licensing models to suit your business needs.

Endpoint at the core of cyber security

The endpoint is the new perimeter, and humans are often the weakest link. Because of the human factor, companies no longer own their perimeter as a whole, and that's why endpoint protection really is the cornerstone of cyber security that can make or break your business protection.

There's no going around it – business security is something that needs to be at its best at all times, day to day, month to month, and year to year.

And we can proudly state that F-Secure is the only company that has taken home the Best Protection award from AV-Test Institute in six years during the award's eight-year history. No other company even comes close to this accomplishment.

The various technologies used together provide top-notch, yet cost-efficient protection for your company assets via the endpoint. For example, file and content reputation data is utilized by our products to control web usage or block selected, typically harmful content. Automated and integrated tools, such as Software Updater, help keep the environment more secure by automatically updating any 3rd party software used by your organization. The combined effort of the various technologies working together means that end-users do not come into contact with most threats at all, which of course diminishes the chances of one of the biggest risks – human error.

On a practical level, our business security solutions are built on several layers that enhance each other and provide the best protection available. This is emphasized by the fact that, since the beginning of 2014, we have achieved the full 6 out of 6 points for protection in AV-Test's independent evaluation of business security products. No company would be able to achieve this today using just "traditional" anti-malware technologies. To achieve efficient security, you need to select a solution with a consistent track record of detecting malware and other threats and protecting against them.

Preventative protection is the key to stopping ransomware and other malware. Therefore, you need a solution that consistently provides the best protection levels on the market, is simple to use, updates automatically, and does not put too much pressure on system performance.

World-class technologies from a proven cyber security company

F-Secure is a European cyber security company with decades of experience in defending enterprises against everything from opportunistic ransomware infections to advanced cyber attacks. Our comprehensive set of services and award-winning products use F-Secure's patented security innovations and sophisticated threat intelligence to protect tens of thousands of companies and millions of people.

F-Secure's security experts have participated in more European cyber crime scene investigations than any other company in the market, and our products are sold all over the world by thousands of resellers and hundreds of operators.

Ransomware: How to prevent, predict, detect & respond https://blog-assets.f-secure.com/wp-content/uploads/2019/11/20112058/ransomware_ppdr_2019.pdf

2. BUSINESS SUITE - MANAGE BUSINESS SECURITY WITH COMPLETE CONTROL

Business Suite is a solution that continuously offers the best protection for organizations. It covers the essential parts of security – protection against known vulnerabilities as well as new, emerging threats. Business Suite is a full protection bundle for organizations of all sizes, with advanced control features and support for physical, virtual, as well as private and public cloud environments through one central management tool. Business Suite is designed to cater to the demanding security needs of today´s organizations. It provides security from servers to endpoints.

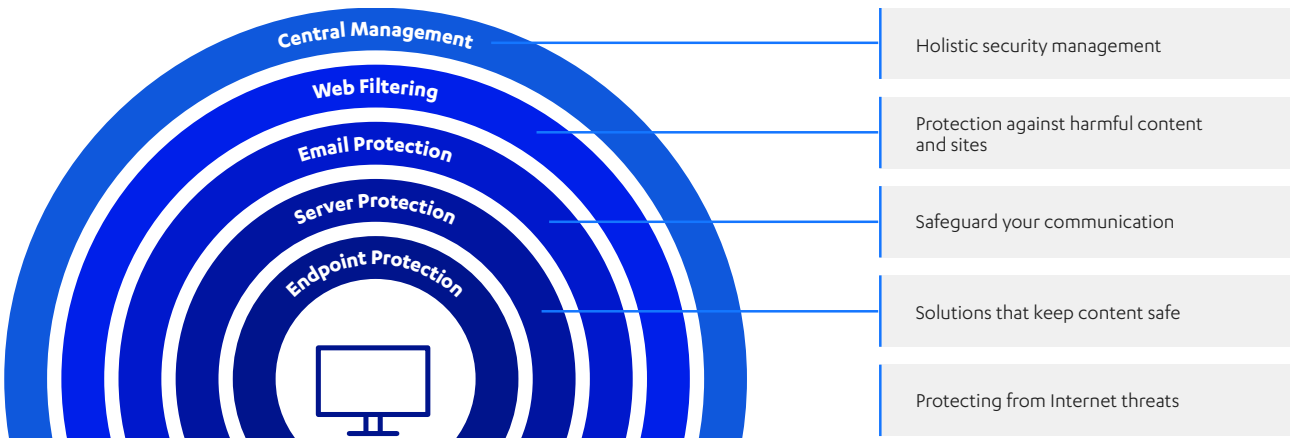
Business Suite in a nutshell

- Control the whole IT environment with one versatile tool.
- Advanced management features even for complex environments.
- Complete, uncompromised security to ensure safe business.
- Performance and scalability for companies of all sizes and different structures.
- Reliable security that lets you focus on your core business.
- Optimized performance for virtual and cloud environments by offloading scanning.
- Proven, best security for your business year after year.
- Designed to have minimal impact on system performance.
- Simple to use, update, and purchase.

The answer to keeping your environment secure

Management is the key to effective security. Centralized management gives you full control of the assets to improve security, while allowing your employees to work flexibly. And full visibility and transparency of the security status of your system at all times allows you to be sure that your organization is secured against all threats.

This makes Business Suite ideal for companies with demanding security needs in terms of functionality, control, and integration. The best way to stop cyber attacks is to stop them before they enter the organization's network. Business Suite offers layered protection against cyber threats.



Everything for business security in one package

Protection for	Business Suite Standard	Business Suite Premium
Windows workstations	•	•
Linux workstations	•	•
Mac workstations	•	•
Microsoft Windows Servers	•	•
Microsoft Exchange Servers	•	•
Microsoft SharePoint Servers	•	•
Linux Servers	•	•
Virtual desktop and server protection	•	•
Private and public Cloud Workload Protection	•	•
Microsoft Terminal Servers	•	•
Citrix Servers	•	•
EMC Storage Servers (CAVA/ICAP)	ICAP	CAVA & ICAP
F-Secure Proxy	•	•

Features	Business Suite Standard	Business Suite Premium
DeepGuard	•	•
Web traffic scanning	•	•
Browsing protection	•	•
Botnet Blocker	•	•
Spam control	•	•
Advanced protection	•	•
DataGuard		•
Application control		•
Software Updater		•
Web content control		•
Connection control		•
Offload Scanning Agent for Virtual environments and cloud workloads		•

Business Suite is a full protection bundle for organizations. The Premium version covers all the added-value features in a package with transparent licensing.

Benefits

- Advanced management features, suitable even for complex environments
- Easy control of all IT assets for enhanced security
- Reduced administration due to automation of daily operations
- Optimized performance for virtual environments by offloading scanning
- Scalability to fit the demands of large organizations

Business Suite is a solution for high-security requirements, with advanced management features for demanding IT environments.

Extra benefits with Business Suite Premium

- Powerful Application control to manage installed software and file access
- Support for automated patch management – Software Updater - to secure your business against known threats
- Better productivity and security with Web Content Control
- Protect business-critical data by securing connections to trusted sites with Connection
- Control, for superior security and ease of work
- Performance-optimized protection for virtual and cloud environments

3. SMART, ON-SITE ENDPOINT SECURITY MANAGEMENT

Business Suite brings best-of-breed security features together seamlessly, leaving no place for vulnerabilities. At its heart is Policy Manager, a scalable control center that enables you to manage all security applications in one place. It delivers ultimate control, time-saving automation, and advanced policy management features for both physical and virtual environments, as well as private and public clouds.

Policy Manager helps you define and distribute security policies and monitor your company's overall security. The best business security software consists of layered protection that's easy to manage and control. You can automate all daily tasks and maintain close control over what users are allowed to do.

Policy Manager can be used for:

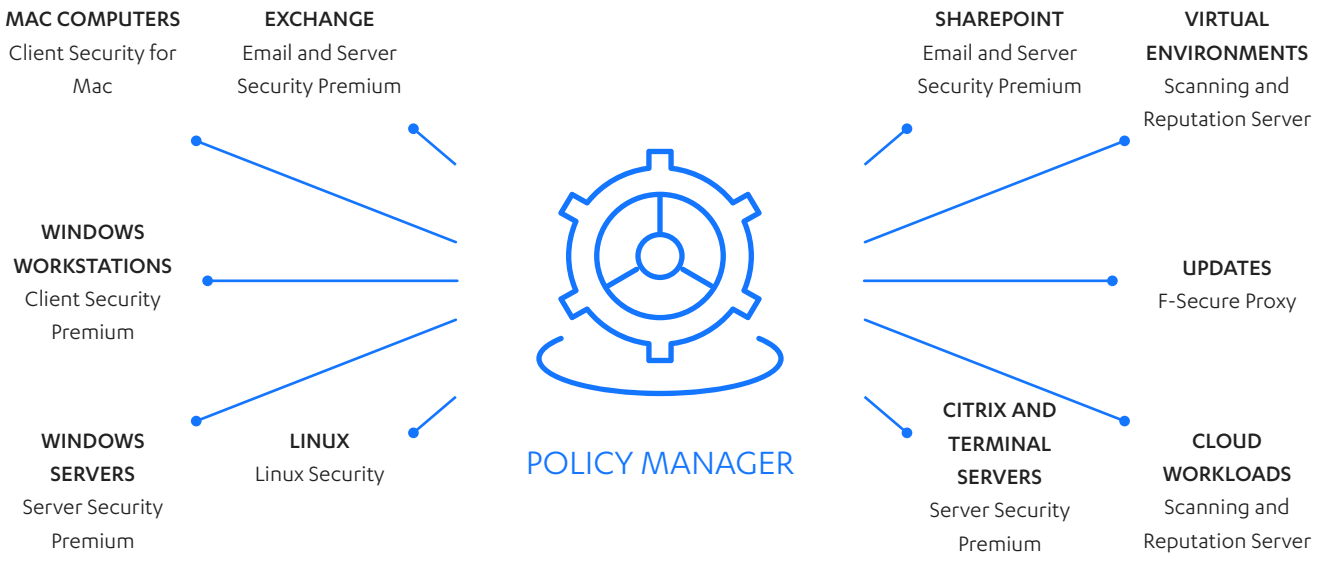
- getting a centralized view of end point status and alerts,
- defining and distributing security policies,
- installing and updating security software to remote systems,
- updating 3rd party software used in your network,
- easy reporting, and
- monitoring the activities of all systems in the enterprise to ensure compliance with corporate policies and centralized control.

When the system has been set up, you can see status information from the entire managed domain in a single location. In this way, it is very easy to make sure that the entire domain is protected, and to modify the protection settings as necessary. You can also restrict the users from making changes to the security settings, and be sure that the protection is always up to date.

Manage Business Security with complete control

F-Secure Policy Manager gives you complete control over all aspects of network security. Simply deploy, and take action. Manage everything from endpoint security and server access to email, browsing, and software security and updates — all with customized, automated controls and policy enforcement capability. You can even leverage advanced management features for complex environments.

Policy Manager also allows you to simplify environment monitoring using security policies, a set of well-defined rules that regulate how sensitive information and other resources are managed, protected, and distributed. The management architecture of F-Secure software uses policies that are centrally configured by the administrator for optimal control of security in a corporate environment.



Policy Manager Console

Policy Manager Console provides a centralized management interface for the security of the managed hosts in the network. Policy Manager can be run on both Windows and Linux platforms, and it gives administrators a centralized tool to organize the network into logical units for sharing policies, install security software, and distribute the defined policies to the managed hosts.

Settings - security management on the highest level, simplified

When the system has been set up, you can see the status of the entire managed domain in Policy Manager. By having the summary in a single location, it is very easy for you to make sure that the entire domain is protected, and to modify the protection settings according your needs. The security settings are presented in an intuitive layout with the possibility to define all required parameters for the optimized protection of all clients in your network.

In the Settings tab, you can restrict users from making changes to the security settings, and with Automatic Update Agent, you can be sure that the protection on managed hosts is always up to date.

Policy Manager can be used to control:

- Centralized management
- Automatic updates
- Real-time scanning
- Manual scanning
- Spyware control
- Quarantine management
- Email scanning
- Firewall security levels
- Firewall rules
- Firewall services
- Application control
- Device Control
- Software Updater
- Web traffic scanning
- Browsing protection
- Web content control
- Alert sending

Status - a clear overview of the complete company network at a glance

On the Status tab in the Console, you can see the status of updates to the malware, spyware and DeepGuard definition databases on the server.

You can check the status of these parts of the protection shield at any time:

- Overall protection
- Automatic updates
- Virus protection
- Internet Shield
- Software Updater
- Installed software
- Centralized management
- Host properties

Software Updater - configure and manage 3rd party software updates

Programs with known, unpatched vulnerabilities have been a critical contributing factor in up to 85% of cyber security incidents. Exploit-based attacks that target these flaws continue to be the biggest cause for network breaches and loss of sensitive data.

Yet 70% of companies have no solution for patch management. According to the SANS Institute's 2015 "State of Application Security Report" report, 26% of internal security teams took two to seven days to deploy patches to critical apps in use, while another 22% took eight to 30 days.

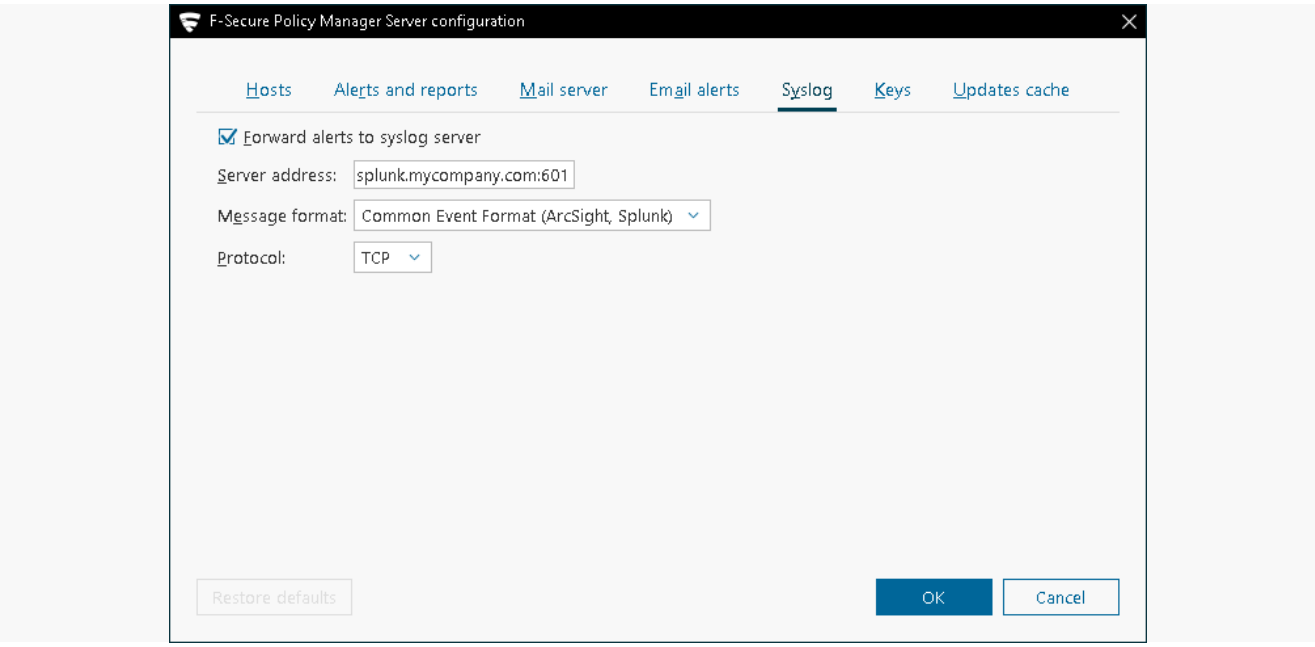
Business Suite Premium and Policy Manager simplify the processing of managing software updates for all hosts that have Software Updater installed. With Policy Manager, you can check the status of all software updates in the network and automatically install software updates to Windows computers and servers. You can also exclude specific software updates from being automatically installed, and do so manually at your own discretion, to accommodate non-standard or edge cases that require special attention.

Alerts - time-saving in solving issues thanks to a clear alert overview

You want to be able to sort out any kind of issues quickly and without complications. Policy Manager Console gives you an overview of all alerts from the complete network, from a single server or a specific workstation. As further comfort, you can set the alerts to be forwarded via email or to your organization's Syslog server.

Alert forwarding for easy SIEM integration

With Policy Manager, you can forward security alerts to integrate Business Suite protection with your organization's existing security information and event management (SIEM) systems. This gives you immediate information on the security of your managed network with minimal impact on your current monitoring setup.



Active Directory - simplify the management of the entire network structure through synchronization

Active Directory, Microsoft's directory service, is widely used as a centralized system to automate the network management of user data and distributed resources. With Policy Manager, you have multiple options to connect your existing Active Directory structure to F-Secure's centralized security management:

- If you want to fully replicate your Active Directory tree in Policy Manager and automatically synchronize it, you can create a synchronization rule that automatically updates Policy Manager with any changes in Active Directory.
- If you want to replicate your Active Directory in Policy Manager but not have it automatically synchronized, you can create a notification rule that informs you of any new unmanaged hosts, which you can then add to the Policy Manager domain tree at your discretion. This option allows you to monitor the network for unprotected hosts.
- If you only want to import the Active Directory tree without synchronizing or monitoring any future changes, you can import the Active Directory structure on a one-time basis.

Operations - update malware definitions and run scans

On the Operations tab, you can remotely initiate malware scans for selected hosts or domains, and also check the status of the latest malware definitions and distribute them throughout your network. You can also launch F-Secure's diagnostic tool remotely on any host, and the diagnostics package is automatically available in Policy Manager. In addition, you can isolate problematic or suspicious hosts, so that you can investigate them more closely before they can pose a more widespread threat to the security of your network.

Policy Manager Proxy

F-Secure Policy Manager Proxy offers a solution to bandwidth issues in distributed installations of F-Secure products. It significantly reduces the load on networks with slow connections by retrieving database updates from a local update repository rather than from F-Secure Policy Manager Server. F-Secure Policy Manager Proxy resides on a computer in the remote network. There should be one Policy Manager Proxy in every network that is connected to slow network lines, retrieving database updates from F-Secure Policy Manager Server, and distributing them locally to the workstations. Workstations in remote offices communicate with Policy Manager Server in the main office directly too, but this communication is restricted to remote management and alerting. The heavy database updates are redirected to the Policy Manager Proxy in the same local network.

Next-gen Policy Manager Proxy

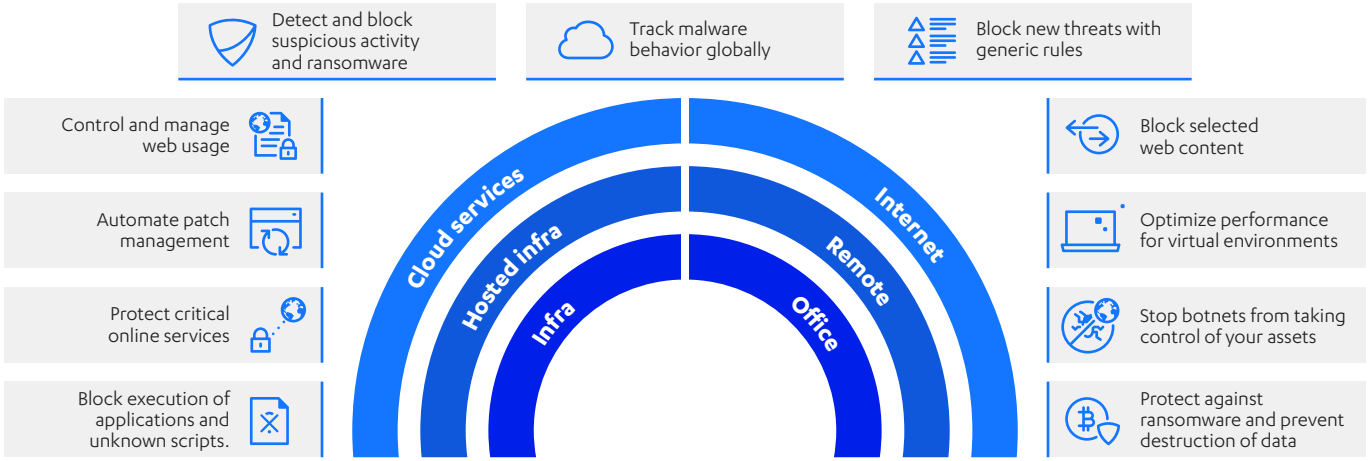
Policy Manager Proxy is a role of Policy Manager Server, in which it proxies certain requests to a master server while serving software updates locally. This way, the heaviest traffic is offloaded from the master server, also allowing you to optimize the amount of costly, high-latency traffic.

Secure connections are used both between hosts and proxy, and proxy and master server. For that to function, the proxy node certificates should be pre-configured.

Summary

Policy Manager gives you complete control over all aspects of network security. Simply deploy...and take action. Manage everything from endpoint security and server access to email, browsing, and software security and updates—all with customized, automated controls and policy enforcement capabilities.

4. CLIENT AND ENDPOINT PROTECTION



Designed for physical,virtual, and cloud environments, F-Secure Client Security offers pioneering security for all Windows workstations; both desktops and laptops. Its numerous protection layers, pioneering technologies, and value-added functionalities ensure unprecedented protection. With Client Security, you prevent business interruptions, save time with automatic patch management, and boost security and productivity with enforceable web content controls. Client Security provides total endpoint protection to prevent malware from reaching your network.

F-Secure Client Security is available in Standard and Premium versions and includes excellent, award-winning protection, heightened security for sensitive activities like banking, automated software patching for more than 2,500 3rd party applications, and much more.

Multi-layered endpoint protection

Given the various challenges present in today's more complex computing reality and more fluid threat landscape, file scanning engines are now just one layer in a multi-tiered approach to endpoint security. Cloud-based file and web reputation checking, behavioral analysis, and a Host-based Intrusion Prevention System (HIPS) have all become integral components of the modern proactive protection system.

F-Secure's multi-layered approach to security comprises the following modules, each designed to address a particular aspect of the threat landscape and work together to provide a complete solution:

A whole lot more than endpoint protection

Software Updater
Automatically update Microsoft and 2500+ 3rd party software apps.

DeepGuard
An intelligent, heuristic anti-malware engine offering 0-day detection capability.

F-Secure DeepGuard
Read the white paper

Web content control
Improve security and productivity with controlled access to websites. Prevent access to websites based on categories.

Connection control
Activate additional security for sensitive transactions such as online banking.

Real-time protection
F-Secure Security Cloud protects against new malware as it utilizes threat details seen by other protected machines, making responses far more efficient.

Multi-engine anti-malware
Provide unmatched protection with highly advanced, multi-engine anti-malware.

Firewall
Additional rules and management functionality integrated with Windows Firewall.

Browsing protection
Proactively prevents employees from accessing harmful sites that contain malicious links or content.

Device control
Control USB device access.

Botnet Blocker
Stop criminals aiming to control compromised assets by preventing communication to Command & Control domains.

DataGuard
Provides additional protection against ransomware, and prevents the destruction and tampering of data.

Application Control
Blocks execution of applications and scripts according to rules created by our penetration testers, or as defined by the administrator.

Enhance security - control internet use

As mentioned before, most attacks and malware downloads today take place online. Ideally, protection should begin before the machine environment is reached, by preventing exposure to possible infection points - and so, enter Browsing protection.

To prevent users from inadvertently visiting compromised legitimate or outright malicious sites, Browsing protection provides a critical assessment of a website's security. If the site is known to be malicious, or it contains features that render it suspect, the user is cautioned against entering it. To deal efficiently with the millions of sites available on the internet and their constantly fluctuating changes in security, Browsing protection's functionality is based on lookup queries to F-Secure's Security Cloud, which includes a database of known safe and malicious websites and files. The entries are updated automatically in real time based on machine learning and artificial intelligence by F-Secure Labs.

Web Traffic Scanning

Certain technologies, such as Java, Flash, Windows, Silverlight, executables, and Active X components are typical targets for exploit kits. In 2015, Flash accounted for >80% (100% according to some sources) of top 10 exploits used by various exploit kits. And so far, the trend of exploiting established, widespread components has continued.

Advanced protection

By blocking this content, you are protecting the users in your company from typical vulnerabilities on websites, and therefore already stopping quite a lot of incidents.

Web Traffic Scanning Advanced Protection allows the administrator to block selected content from websites that do not have confirmed reputation data or are known to be suspicious by F-Secure. Administrators can also whitelist certain trusted websites.

Botnet Blocker

Most malware attacks are based on botnets. Botnets need to be able to communicate, usually through the Command & Control domains. These domains are often used by cyber criminals to penetrate the company network wider with the help of botnets. Botnets are like automated backdoors to the corporate network, and can even be rented for an affordable price. Once in the system, the botnets perform various tasks, such as collecting data, monitoring the user's actions and so on.

Botnet Blocker is an added security feature that allows you to repel botnets and ransomware effectively. Botnet Blocker adds a layer of protection to catch malware at different stages. This results in an effective way to disable botnet operations.

Botnet Blocker is a security feature that aims to prevent botnet agents from communicating with their command and control servers. It brings down botnet activities in your network by blocking Domain Name System queries to domains with malicious reputation.

In this way, botnets are not able to perform their intended actions if access to the C&C is blocked. Also, most attackers rely on disposable domains as part of their infection chain. Botnet Blocker prevents resolution of such unique domains and thus prevents the attacker from being able to infect the victim in the first place.

Web Content Control

Up to 89% of employees admit to wasting time at work every day, and 4% waste up to half of the working day on social media and other non-work-related issues. Unrestricted internet access impacts productivity in the workplace, which is a concern to many companies.

With Web Content Control, you can limit internet usage to business-related content and eliminate a large portion of the attack surface. To do this, websites are categorized based on their content, such as 'gambling' or 'entertainment'. You can then selectively block those with unwanted content. When users try to access a site with prohibited content, they see a page in their browser saying that the site has been blocked by IT administration.

Connection Control

With a few exceptions, almost all banking malware requires an active, real-time internet connection to their command and control (C&C) server. They use the connection to receive commands from the operators using the malware to perform an attack, most importantly for instructions on where to transmit any data they steal from an infected machine. This real-time connection is vital for the banking malware to succeed, as any fixed connections encoded in the malware's binary or configuration files would be very easy to track down and close.

To counter this behavior and cripple banking malware, Connection Control blocks any unrelated connections from opening during a secured online banking or payment transaction. By doing so, any data transmitted during the transaction is shielded from interception and theft by banking malware.

5. SERVER MANAGEMENT

On average, 90% of malware attacks are stopped by traditional anti-malware solutions. But malware is becoming more sophisticated, actively resisting traditional detection technologies.

With 75% of attacks based on opportunity, anyone can be a target. Servers and email systems are still very common targets for attack. As the consequences of a security breach can be staggering, even putting your whole business in danger, it's crucial to stop attacks before they can enter the company network.

F-Secure Server Security is a server solution that protects your on-site, virtual, and cloud-based servers from malware and software vulnerabilities without slowing the system down.

Server Security provides enhanced real-time protection against viruses, spyware, and riskware, and offers behavior-based, proactive detection for new threats with F-Secure's award-winning DeepGuard technology. With the Software Updater feature, Email and Server Security keeps the operating system and 3rd party server software updated and protected against vulnerability-based threats.

With Policy Manager and Server Security, you have a powerful, centralized solution to protect your server, email, and collaboration systems. You can watch over your whole business IT, both physical and virtual, and ensure smooth operation. Server Security comes in two versions: Standard and Premium. The Premium version includes Software Updater, a turnkey solution that automatically updates 3rd party software installed on the servers.

Feature	F-Secure Server Security	F-Secure Server Security Premium	F-Secure Email and Server Security Standard	F-Secure Email and Server Security Premium	F-Secure Linux Server Security
Malware & spyware protection	•	•	•	•	•
DeepGuard™	•	•	•	•	
Web traffic scanning	•	•	•	•	•
Browsing protection	•	•	•	•	
Offload Scanning Agent for Virtual environments and cloud workloads	•	•	•	•	
Spam Control			•	•	
Email Quarantine Manager			•	•	
Software Updater		•		•	
Integrity checking ●					•
Firewall	•	•	•	•	•
Anti-Malware for Microsoft® Exchange			•	•	
Anti-Malware for Microsoft® SharePoint			•	•	
EMC CAVA support				•	

F-Secure Email and Server Security includes the following features:

Malware & spyware protection

Protect your computer against viruses, trojans, spyware, rootkits and other malware.

DeepGuard™

Proactive, instant protection against unknown threats. It monitors application behavior and stops potentially harmful activities in real time.

DeepGuard – Proactive on-host protection against new and emerging threats

https://www.f-secure.com/documents/996508/1030745/deepguard_whitepaper.pdf

Web traffic scanning

Detect and block malicious content in web traffic (HTTP protocol) to provide additional protection against malware.

Browsing protection

Protection for your terminal users against web browser exploits and rogue web sites.

Offload Scanning Agent for virtual environments and cloud workloads

Allows offloading the malware scanning to F-Secure Scanning and Reputation Server in Virtual and Cloud Environments.

Spam Control

Detect and filter spam messages from email traffic, providing real-time protection against all types of spam, regardless of its content, format, or language.

Email Quarantine Manager

Allow dedicated users to manage the email quarantine: to release, reprocess, or delete quarantined emails or attachments.

Software Updater

Keep your system and applications up-to-date by installing patches as they are released by vendors.

Integrity Checking

Protects Linux Servers against unauthorized modifications.

Firewall

Protects servers and computers against unauthorized connection attempts.

Protection for Microsoft® Exchange

Protects incoming, outgoing, and internal mail traffic and Exchange public folders from malware and other security threats and provides content and attachment filtering.

Protection for Microsoft® SharePoint

Real-time protection for Microsoft® SharePoint servers, scanning the uploaded and downloaded content for malware and other security threats.

Citrix® XenAPP

Provides Anti-Malware protection when working in Citrix® XenAPP environments.

EMC CAVA & Isilon support

Provides Anti-Malware protection when working in EMC storage servers with Celerra Anti Virus Agent or Isilon support.

6. MICROSOFT® EXCHANGE, MICROSOFT® SHAREPOINT AND CITRIX® SECURITY

F-Secure Email and Server Security is a robust, full-service solution designed to protect your company's mail and groupware servers and to shield the company network from any malicious code that travels over HTTP or SMTP. In addition, it protects your company network against spam.

Most importantly, Email and Server Security acts as the first line of defense against zero-day threats and known vulnerabilities.

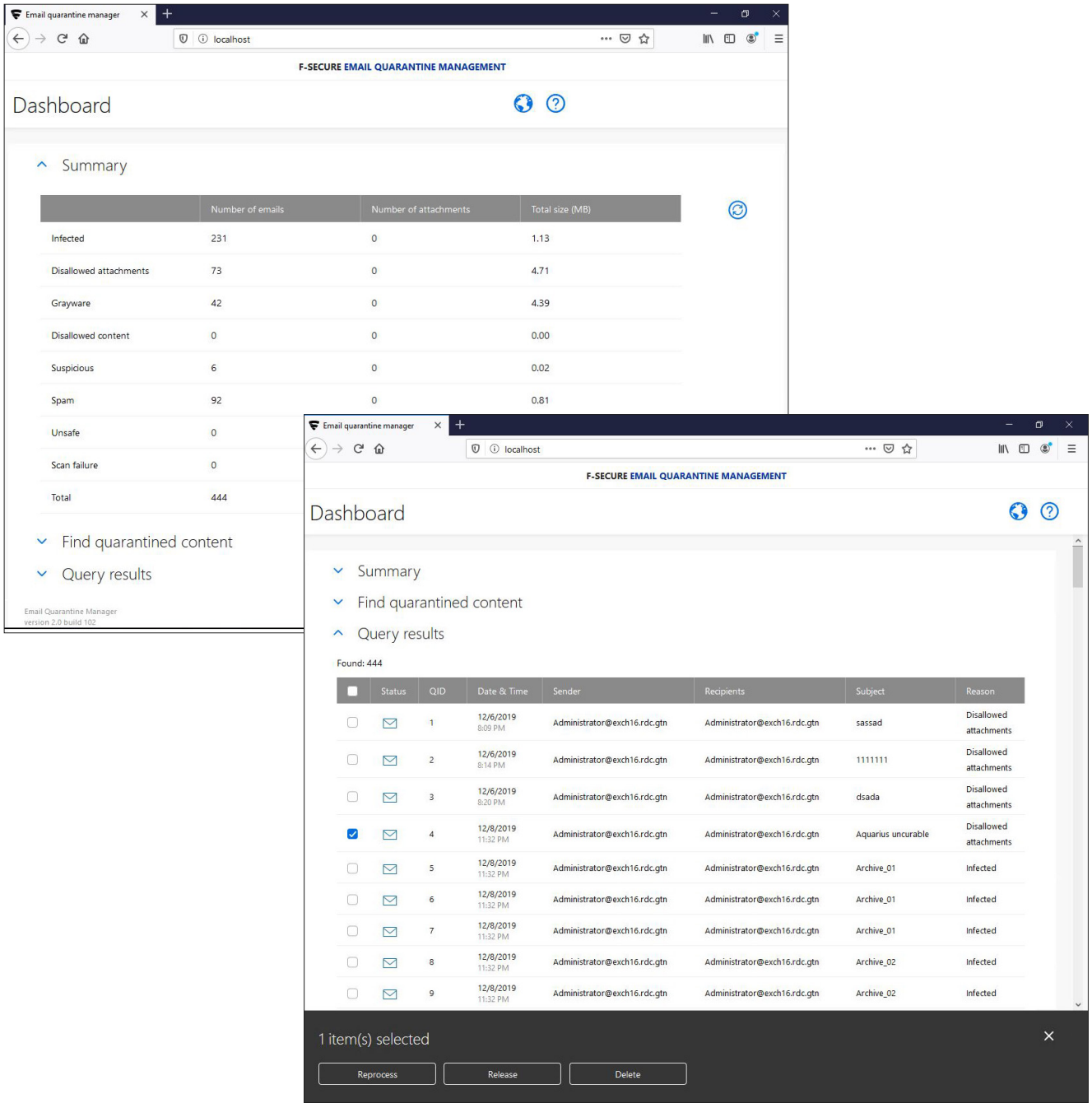
Email and Server Security contains anti-malware and Spam Control for Microsoft® Exchange mail servers, anti-malware for Microsoft® Terminal Servers and Citrix® servers, Microsoft® SharePoint, and EMC CAVA support.

When used on an Exchange mail server, Email and Server Security scans attachments and message bodies for malicious code. Email and Server Security is installed directly on a Microsoft® Exchange Server, and it intercepts mail to and from mailboxes and public folders. If the intercepted mail contains malicious code, Email and Server Security can be configured to disinfect or drop the content. Any detected malicious code and attachments can be placed in quarantine, where they can be further examined. Email and Server Security can also be instructed to remove particular attachments according to the file name or the file extension.

7. EMAIL QUARANTINE MANAGEMENT

F-Secure Email Quarantine Manager allows nonadministrator personnel to handle messages and attachments that Email and Server Security places in quarantine, which is a safe repository for files that may be harmful. Any malware, spyware, or riskware in quarantine can no longer spread or cause harm to your computers. If you need to allow access to any quarantined applications, files, or email messages, you can restore them.

Email Quarantine Manager enables you to distribute the workload and roles for handling quarantined content within your organization. Instead of just administrator-level roles accessing the quarantine to manage the content, you can provide access for all helpdesk staff, for example, without giving them access to the full range of Email and Server Security settings.



8. LINUX SECURITY

Linux Security can be used to protect both servers and workstations. Both Linux servers and workstations can be administrated centrally with Policy Manager (or if required, as standalone installations through a local web user interface).

Linux Security protects the system against viruses and potentially unwanted applications.

Real-time scanning gives you continuous protection against viruses and potentially unwanted applications as files are opened, copied, and downloaded from the web. Real-time scanning functions transparently in the background, looking for viruses whenever you access files on the hard disk, removable media, or network drives. If you try to access an infected file, the real-time protection automatically stops the virus from executing.

When real-time scanning has been configured to scan a limited set of files, manual scanning can be used to scan the full system, or you can use scheduled scanning to scan the full system at regular intervals.

Automatic Updates keep the virus definitions up to date at all times. The virus definition databases are updated automatically after the product has been installed. The virus definitions updates are signed by F-Secure.

The Host Intrusion Prevention System (HIPS) detects any malicious activity on the host, protecting the system on many levels.

Integrity Checking protects the system against unauthorized modifications. It is based on the concept of a known good configuration - the product should be installed before the computer is connected to the network to guarantee that the system is in a known good configuration.

You can create a baseline of the system files that you want to protect and prevent the use of any modified files for all users.

The Firewall component is a stateful packet filtering firewall, which is based on Netfilter and iptables. It protects computers against unauthorized connection attempts. You can use predefined security profiles that are tailored for common use cases to select the traffic you want to allow and deny.

If an attacker gains shell access to the system and tries to add a user account to log in to the system later, the Host Intrusion Prevention System (HIPS) detects modified system files and alerts the administrator.

If an attacker has gained access to the system and tries to install a userspace rootkit by replacing various system utilities, HIPS detects the modified system files and alerts the administrator.

Key features and benefits

Superior protection against viruses and worms.

The product scans files on any Linux-supported file system. This is the optimal solution for computers that run several different operating systems with a multiboot utility.

Transparent to end-users.

The product works totally transparently to the end-users.

Protection of critical system files.

Critical information within system files is stored and automatically checked before access is allowed.

Easy to deploy and administer.

The default settings apply in most systems and the product can be taken into use without any additional configuration.

Extensive alerting options.

The product has extensive monitoring and alerting functions that can be used to notify any administrator in the company network about any infected content that has been found.

Ready for cloud workloads.

Supporting a wide range of Linux distributions including Amazon Linux.

9. VIRTUAL SECURITY AND CLOUD WORKLOAD PROTECTION

Virtualization offers a lot of benefits, such as flexibility, resource optimization, and operational efficiency. On the other hand, virtualizing your IT assets creates new challenges, such as limited hardware capacity and shared hardware usage. These have an impact on desktop and server virtualization.

Security and compliance are a shared responsibility between the various public cloud service providers and the customer. When moving workloads to the cloud it's still the customer's responsibility to take care of vulnerabilities, exploits and malware protection.

Virtual Security and cloud workload protection allow offloading resource-intensive scanning operations to dedicated Scanning and Reputation Servers (SRS), reducing the CPU and memory consumption on virtual machines and cloud workloads.

F-Secure Virtual Security is available for the most popular virtualization platforms: VMware, Citrix®, Hyper-V, and KVM. The solution is hypervisor-agnostic, so it can be deployed in private or public cloud environments.

The virtual machines are secured through standard installations of F-Secure Client Security (workstations), Server Security (file servers), or Email and Server Security. To improve performance, the solution uses the Offload Scanning Agent (OSA) to move resource-heavy scanning tasks to a dedicated Scanning and Reputation Server.

Doing so allows you to run full scans on virtual hosts without fear of cluster-wide memory and CPU utilization spikes.

A single F-Secure Scanning and Reputation Server (SRS) can handle the scanning load for up to 130 virtual machines.

Virtual Security can be deployed on a single physical host or as a clustered deployment.

- **Single physical host:** the simplest F-Secure Virtual Security setup involves a single physical host computer running a number of virtual Windows workstations.
- **Clustered:** more than one physical host behaving as a single computer. A physical host or cluster may be running more than one isolated group of virtual machines.

Benefits

- Hypervisor-agnostic, can be deployed in any virtualization environment (VI or VDI)
- Offloads CPU-intensive scanning operations to a dedicated Scanning and Reputation Server
- Proactive, behavior-based protection against malware, exploits, phishing, and network-based attacks
- Reduced memory, CPU, and disk space consumption on virtual machines bring cost savings in large environments
- A simple pricing model and affordable total cost as one package serves physical, virtual as well as private and public cloud environments

REFERENCES

1. DeepGuard – Proactive on-host protection against new and emerging threats | https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163346/F-Secure_DeepGuard.pdf

2. F-Secure Security Cloud – Purpose, function and benefits | https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163353/F-Secure_Security_Cloud.pdf

3. Ransomware: How to prevent, predict, detect & respond | https://blog-assets.f-secure.com/wp-content/uploads/2019/11/20112058/ransomware_ppdr_2019.pdf

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure