SOFTWARE UPDATER

Keep known vulnerabilities out of your system

Version 1 - 04 July 2016
SOFTWARE UPDATER

SUMMARY

This whitepaper explains software updates as an integral part of endpoint protection. F-Secure Software Updater offers automated updates for both Microsoft and third-party software, integrated in our endpoint clients for ease of use and affordability.

KEY FEATURES

- Software Updater works by scanning for missing updates, creating a vulnerability report based on missing patches, and then downloading and deploying them automatically.
- Best detection, automatic updates and integrated management for an affordable package price
- Unique patch management not just for Windows but also for 3rd party products
- Automatic deployment of security updates

BENEFITS

- 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
- With 85% of vulnerabilities originating from third-party software, patch management for such software is essential
- Software Updater is integrated in F-Secure security software, thus offering best detection, automatic updates and integrated management for an affordable package price
- Administrator can define exclusions for the automatic mode

CONTENTS

Summary ................................................. 2
Key Features ............................................. 2
Benefits .................................................... 2
The case for software updates ................. 3
Scanning and Reporting missing updates .... 3
Software Updater is a critical security component 4
Software Updater is integrated into F-Secure security clients ........................................ 4
Status Check .......................................... 5
Software Updater on machines with Protection Service for Business .......................... 5
Software Updater on machines with Business Suite Premium ................................. 5
THE CASE FOR SOFTWARE UPDATES

Most modern malware exploit known software vulnerabilities to infect IT systems. Exploits are in the wild only a few moments after the fix to a vulnerability is published. Most infections could be avoided with applying security fixes already available. In fact, about 85 per cent of malware could be avoided with up-to-date software. However, most corporate end points lack critical software updates. Administrators currently don’t have visibility to what 3rd party software is installed on managed endpoints unless very strict user account restrictions are in use. Another issue is the time it takes to keep up and update all different software in use every time there is an update available.

SCANNING AND REPORTING MISSING UPDATES

F-Secure’s Software Updater scans and reports missing updates for 3rd party software and deploys security updates automatically.

This includes Microsoft updates for the operating system and Microsoft applications, in addition to a comprehensive list of 3rd party applications that are commonly used and prone to vulnerabilities.

Software Updater regularly downloads the definition files that include information about software updates, their versions, security bulletin IDs, links to knowledgebase articles, locations of installation packages, etc. It then compares these to the installed software and identifies missing updates.

Scanned software includes Microsoft updates for the operating system and MS applications, in addition to over 3500 third party applications from about 70 vendors, such as Adobe Flash, Java, OpenOffice, archive managers, media players, image viewers and so on, which are common vectors of attack due their popularity and larger number of vulnerabilities.

The required definition files are downloaded periodically. They include information about software updates, their versions, security bulletin IDs, links to knowledgebase articles, locations of installation packages, etc. Then it compares these to what software is installed and identifies missing updates. The scanning for missing updates happens in system startup and when new software update definitions are downloaded, or once a day as a minimum if neither of the previous events occur.

DISCLAIMERS

• The purpose of this document is to help customers better understand how F-Secure products function, and the benefits F-Secure Software Updater provides. This document is not designed to be a legally binding agreement that defines the content of products and services provided by F-Secure Corporation.

• F-Secure Software Updater, as with any of our other products and services, is a constantly evolving set of software, systems and processes. This document may become partly inaccurate as this evolution takes place. F-Secure Corporation will update this document every time major changes are made to our products, systems or processes. The latest version will always be available on F-Secure’s website.

• Any metrics or diagrams presented in this document are valid at the time of publication. Metrics or diagrams may change over time. Presented metrics should therefore be interpreted as approximate figures.
SOFTWARE UPDATER IS A CRITICAL SECURITY COMPONENT

It is the first layer of protection when malicious content arrives on the endpoint itself.

As the vast majority of attacks utilize known vulnerabilities in their attacks, Software Updater can block up to 85% of attacks simply by virtue of preventing vulnerabilities from being exploited in the first place.

SOFTWARE UPDATER IS INTEGRATED INTO F-SECURE SECURITY CLIENTS

Therefore, there is no need to install separate agents or management servers or consoles, unlike with traditional patch management solutions.

Administrator can define exclusions for the automatic mode based on software names or bulletin IDs and they can be filtered out from Console interface to avoid clutter.

This is important for customers who rely on certain versions of some software, for example Java Runtime, where a certain version of the software is used to run some business applications. Also, since updates for selected software (for example Microsoft) can be taken care of with other products, exclusions can be used to avoid overlaps with Software Updater.

Critical and important security updates are minor version upgrades. This means they can safely be installed automatically as they are very unlikely to break product compatibility, cause problems with features or introduce any other unexpected, unwanted issues.

Service Packs are always excluded from automatic deployment, as they might change product behavior and result in changed functionality or compatibility issues. This is why an administrator needs to initiate the deployment of these updates.

87% of corporate computers are missing critical updates

Software Updater is integrated into F-Secure Workstation Security clients. Therefore, there is no need to install separate agents or management servers or consoles, unlike with traditional patch management solutions.

Administrator can define exclusions for the automatic mode based on software names or bulletin IDs and they can be filtered out from Console interface to avoid clutter.

This is important for customers who rely on certain versions of some software, for example Java Runtime, where a certain version of the software is used to run some business applications. Also, since updates for selected software (for example Microsoft) can be taken care of with other products, exclusions can be used to avoid overlaps with Software Updater.

In order to deliver to outmost standards, workstation security utilizes a multi-layered approach to security, leveraging various modern technologies such as Heuristic Analysis and Security Cloud.

- It is comprised of several independent modules that each address a particular aspect of the threat landscape. Furthermore, they are designed to work together to provide greater protection that could be achieved by individual layers only.

In order to deliver to outmost standards, workstation security utilizes a multi-layered approach to security, leveraging various modern technologies such as Heuristic Analysis and Security Cloud.

- It is comprised of several independent modules that each address a particular aspect of the threat landscape. Furthermore, they are designed to work together to provide greater protection that could be achieved by individual layers only.

Critical and important security updates are minor version upgrades. This means they can safely be installed automatically as they are very unlikely to break product compatibility, cause problems with features or introduce any other unexpected, unwanted issues.

Service Packs are always excluded from automatic deployment, as they might change product behavior and result in changed functionality or compatibility issues. This is why an administrator needs to initiate the deployment of these updates.
STATUS CHECK

Missing updates are reported back to the management site of our business products and the aggregated number of missing updates is shown on the client statistics view.

The installation status is visible in the overview site, and possible installation failures are reported so that they can be retried. The managed systems are only restarted if the application updates require it. On the other hand, if multiple applications that require a restart are updated at the same time, only one restart is needed, making life easier for the users. Clients download the updates directly from the 3rd party vendor’s site and install them silently in the background. No internal distribution points need to be set up.

Updates can be cached with transparent proxies, as with normal web traffic from the endpoints, if such proxies are in use. Installed updates can be found from the web reports to show what was done.

SOFTWARE UPDATER ON MACHINES WITH PROTECTION SERVICE FOR BUSINESS

- Server Security
- E-mail and Server Security
- Workstation Security

Operating System: Windows

SOFTWARE UPDATER ON MACHINES WITH BUSINESS SUITE PREMIUM

- Server Security Premium
- E-mail and Server Security Premium
- Client Security Premium

Operating System: Windows

The software update status is checked on system startup and when new software update definitions are downloaded, but at least once a day.

- Administrators can review the missing updates for the whole environment and for specific endpoints from the managing site and from web reporting.

- The administrator can drill down to the details of missing updates. Reports of missing software updates, their severity and the number of affected hosts can be easily accessed with a web browser.

- For sales partners, the installed updates report is useful for monitoring achieved results and billing.