Whitepaper

WithSecure™ Ultralight

Intelligent world-class endpoint protection and threat discovery

Contents

Summary

The unique and advanced technologies behind WithSecure™ Ultralight provide several benefits that can be summarized as follows:

Better protection

By offloading scanning and analysis of suspicious objects to WithSecure's™ Security Cloud, Ultralight is not only able to perform a more thorough evaluation of a potential threat, it is also able to minimize CPU and memory usage on the device itself. Once there is a verdict on an object, that information is immediately provided to all users, which in case of false positives means immediate whitelisting. As number of customers in the network grows, so do the performance improvements.

Better performance

By offloading scanning and analysis of suspicious objects to WithSecure's™ Security Cloud, we are not only able to perform a much more thorough analysis of a potential threat than we could on the endpoint; we are able to save precious resources on the device itself. Once we have a verdict on an object, we immediately provide that to all of our customers, which in the case of clean files means simply skipping the files. As our network of customers grows, so do the performance improvements.

Better user experience

Ultralight installation takes just seconds and, once it is completed, the user is fully protected through the latest components and threat intelligence available via endpoints the WithSecure™ Security Cloud. As a customer, you will receive new and improved protection components quickly and frequently.

Key principles

The Ultralight operating model is based on the following three key principles that protect the customer against cyber-attacks:

- Prevent the attacker from being able to contact the target in the first place
- Prevent the attacker from delivering an exploit or other hostile content to the target
- Prevent the target from running or executing hostile content

Key benefits

Ultralight, as a set of technologies, provides the following benefits:

- Drastically decreased volume of successful attacks against the endpoint
- Drastically decreased client resource usage by moving performance-heavy processes to the cloud
- A combination of intelligent technologies that share information and work together to protect the endpoint

The case for modern protection technologies

To face this ever-changing landscape, security solutions must not only constantly evolve, they must be capable of protecting the customer proactively.

Threats are opportunistic and dynamic. Wherever online trends go, threats will follow. As the online ecosystem is continuously changing, the threats that people and companies are facing today, will differ from what they will encounter tomorrow. Current threats facing people and companies are rarely the same as those they will face in the future.

In a day, we see about 7 billion events, 6 billion online reputation queries, 1 million suspicious URLs, 500 000 samples for analysis, and around 10 000 new malware.[1]

Endpoint protection solutions have transformed over the years. Early protection solutions employed anti-virus scanners designed to detect malware in files by checking for simple signatures stored in a local database. By 2006, this approach started to dwindle in effectiveness due to the rise in server-side polymorphic malware. The signature approach of yesteryears was easy to defeat; it was trivial to test samples against a scan engine and modify them until they were no longer detected.

The traditional file scanning approach is still in use in most endpoint protection solutions to this day as part of a wider toolset of protection technologies. Scanning engines have evolved to augment the simple signature approach with more complex detection logic based on parsers, disassemblers, and emulators. File scanning engines can still be an effective tool against the ever-expanding pool of known threats. Nowadays, they are even optimized for speed, and is the remaining protection layer when no network connection is available on the local device.

Modern endpoint protection suites employ a multi-layered approach to providing security. Technologies such as network filtering and scanning, behavioral analysis, and URL filtering augment traditional file scanning components. These different protection features are built into WithSecure™ Ultralight in a multi-layered design, so that if a threat escapes one layer, there is still another layer that can catch it. And as the threat landscape changes, some layers may be removed or new ones may be added both in the endpoints and in the WithSecure™ Security Cloud.

Our approach

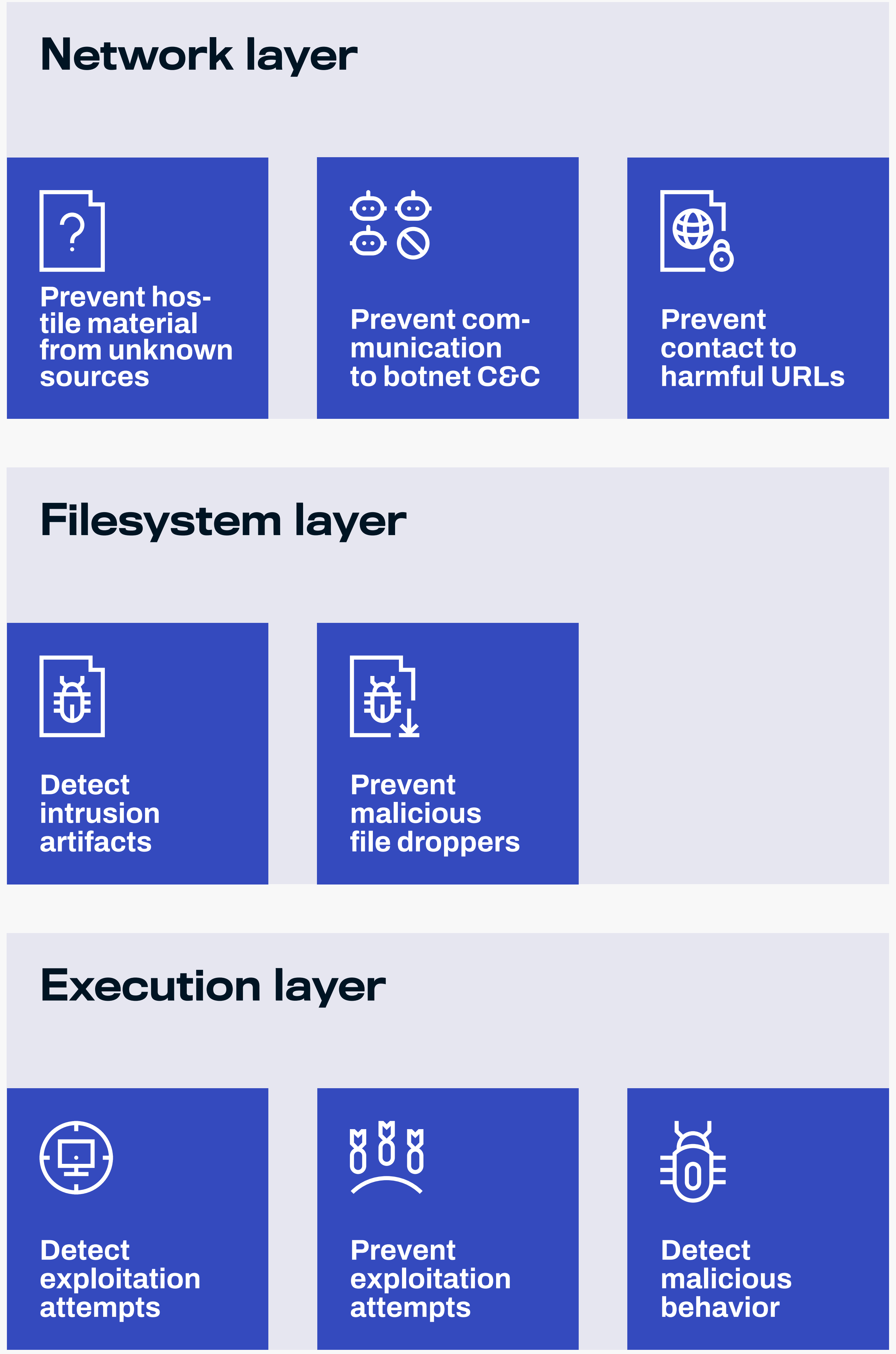
Our approach to endpoint protection is to rely on a combination of several protection technologies that communicate with each other and work in tandem to identify and block attacks. Our modern protection techniques are designed to understand how attackers work, and concentrate on denying them the resources they need to succeed so an attack cannot take place.

Our solution utilizes data science techniques capable of selecting targets and would-be threats. This approach allows us to proactively block zero-day threats that traditional signature-based scanning would miss and prevents attackers from being able to establish a point of contact necessary to execute an attack. This combination of protection techniques is vital in providing comprehensive protection against everything from crimeware to Advanced Persistent Threats.

Our customers get the full package: technologies that have been tested and proven in the field for decades, combined with state-of-the-art, next-generation security features developed by a company that has been fighting cyber threats for over 30 years. Ultralight's intelligent combination of protection technologies represents the same approach that allowed us to take home the prestigious AV-Test Institute's "Best Protection" award six times in the past eight years.

To keep our customers safe, we constantly collect data from many different sources to feed our backend threat intelligence systems. Ultralight itself can provide data to these systems. However, we never collect private data or data that can be used to identify a user. Here at WithSecure™, privacy is one of our key principles. We promise to remain completely transparent about any data we send to Security Cloud and how we handle it. For more information on WithSecure's™ privacy policies, please read our Privacy Principles.[2]

Ultralight's intelligent combination of protection technologies represents the same approach that allowed us to take home the prestigious AV-Test Institute's 'Best Protection' award six times in eight years.



Network layer

Prevent hostile material from unknown sources

Prevent communication to botnet C&C

Prevent contact to harmful URLs

Filesystem layer

Detect intrusion artifacts

Prevent malicious file droppers

Execution layer

Detect exploitation attempts

Prevent exploitation attempts

Detect malicious behavior

What is WithSecure™ Ultralight?

Ultralight is an all-in-one package that contains WithSecure's full endpoint protection stack. Ultralight provides a new, modern take on protecting devices in an intelligent and proactive way against the threats we see in the real world. It represents a fundamental breakthrough, not only in the way we protect our customers, but also in the way we work here at WithSecure™. With the introduction of Ultralight, we have gained a wealth of new possibilities for protecting our customers now and in the future.

Ultralight fully leverages the intelligence of WithSecure's Security Cloud[3] at the endpoint. Security Cloud is a threat analysis and repository system operated by WithSecure™ Corporation that provides a wide range of services to security products. Unlike traditional anti-virus solutions that receive periodic database updates and can go hours or days before they are protected against new threats, Ultralight's direct connection to WithSecure's cloud provides minute-to-minute protection for all users.

Ultralight has allowed us to do things we have never been able to do before. We are building a knowledge base from every connected device and feeding that information to forensics and behavioral analysis systems. These intelligent systems are far more effective at catching and preventing attacks than the traditional file scanning approach that most anti-virus solutions use.

Ultralight is about performance. If one user sees an application, the results of the analysis of that application can be made available to everyone else immediately. If Ultralight sees an suspicious object, that object is uploaded to our cloud where it goes through extensive analysis - something we cannot do on the endpoint. Majority of verdicts are delivered to the endpoint either via fast, lightweight reputation queries to Security Cloud, or from our own advanced white-listing techniques. These mechanisms ensure that uploading a full file for backend analysis does not happen often. This results in a barely noticeable and low-impact client component.

Ultralight is fast and lightweight. Installation takes just seconds and, once it is completed, the user is fully protected with the latest components and threat intelligence. The activation of the functionality is speedy and non-intrusive, to minimize any disruption of the user's routine.

With Ultralight, we have streamlined our processes for providing new protection features and component updates. This allows us to keep up to date with the threat landscape and keep your devices well protected.

"Ultralight provides a new, modern take on protecting devices in an intelligent and proactive way against the threats we see in the real world."

The Ultralight story

About twelve years ago, we started to think about how we could better use our backend infrastructure to improve our endpoint protection technologies. It was during those discussions that the idea of Ultralight was born. We realized that, by utilizing our own extensive sample collections and backend automation, coupled with up-to-the-minute intelligence from our own customers' devices, we could build a solution that would keep all of our customers better protected with faster reaction times and in a much more flexible and lightweight manner. We then took this idea and combined it with our preventative approach to endpoint protection to create Ultralight as we know it today.

When we started to build the Ultralight endpoint protection package, we realized that, by revamping the architecture and modernizing the individual components and their interactions with each other, we could create a more modular system that is not only easier for us to improve and update, but that, when combined with our new cloud-based services, is able to protect the endpoint in completely new ways.

How does Ultralight work?

Ultralight combines all of the technologies present in WithSecure's full endpoint protection stack into a single package. It consists of a number of drivers, engines, and system services that provide mechanisms to protect both a device and its users. Ultralight provides traditional anti-virus functionality, such as real-time file scanning and network scanning. In addition, it includes modern, proactive protection technologies that aim to stop zero-day exploits and stay ahead of new attacks. WithSecure's™ Security Cloud provides Ultralight components with real-time information as the threat landscape changes.

The Ultralight package consists of a series of modules, all of which are updateable on the fly. During installation, the Ultralight updater fetches and installs all of these modules. This ensures that any system running Ultralight contains cutting-edge protection the moment installation finishes. Ultralight is able to dynamically adapt, bringing in new modules where needed and reconfiguring itself as the situation dictates. All of this happens behind the scenes and is completely managed by Ultralight itself.

The design of Ultralight's protection technologies is driven by in-depth analysis of methodologies used by attackers. Instead of simply trying to detect new malware and exploits, we study how attackers operate and use that knowledge to devise generic protection methods that catch the sort of behavior they would use, but normal users would not. This approach allows us to stay ahead of the sort of zero-day threats that traditional anti-virus solutions fail to detect.

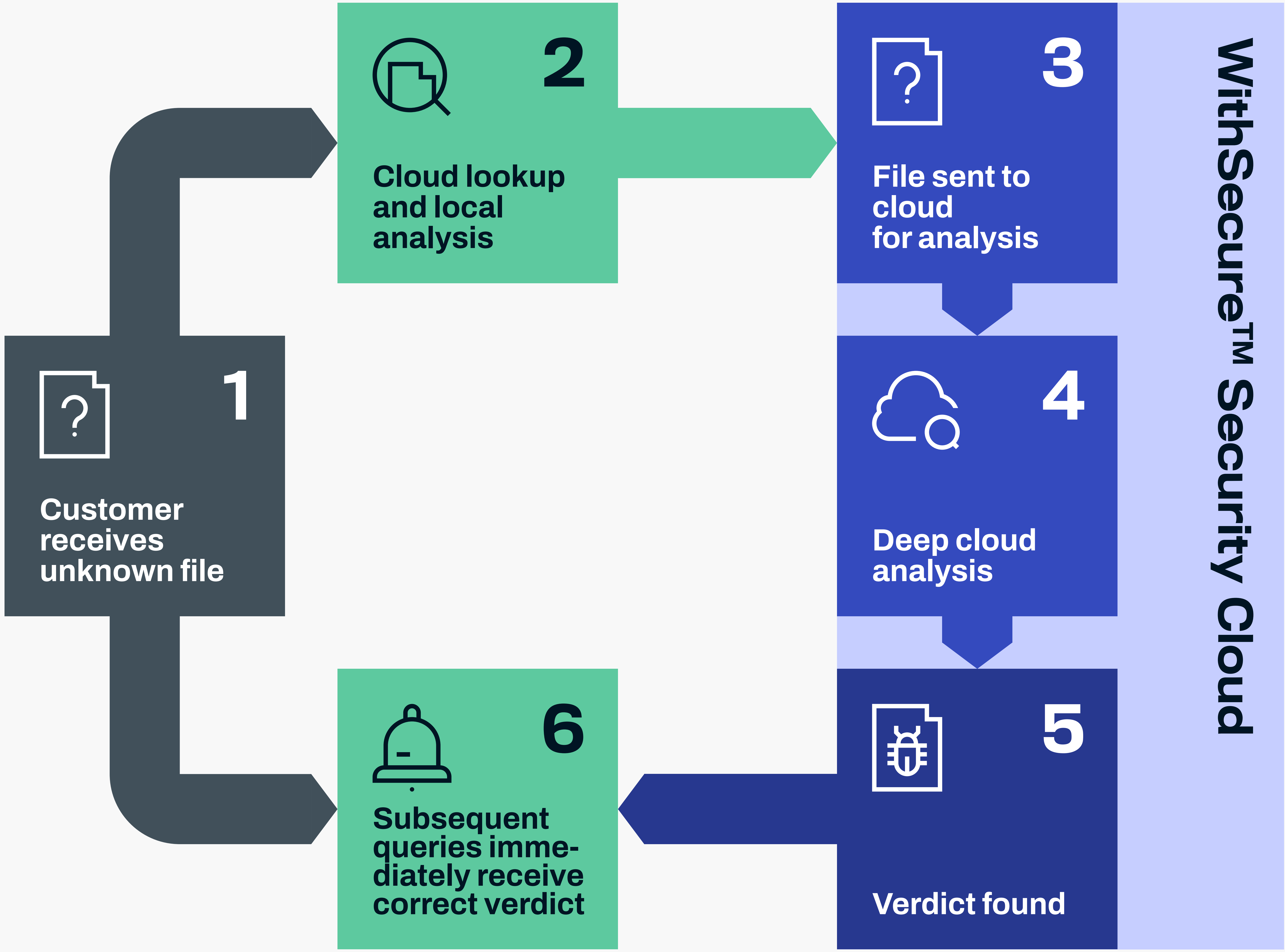
Features

Ultralight contains the following key features:

- Detects and blocks exploits, common malware, and other identifiers in any hostile content sent by attacker
- Detects and blocks exploitive behavior occurring in an application designed to open potentially harmful content (PDF reader, office software, Java runtime, JavaScript interpreter, etc.)
- Detects and blocks suspicious or malicious behavior both in running applications and in the system itself
- Prevents compromised applications from performing hostile actions, such as dropping malware onto a system
- Detects and blocks malware with a traditional file scanning engine
- Detects and blocks memory-resident malware
- Removes or quarantines malicious artifacts from the system
- Disinfects objects that have been modified by file infectors
- Utilizes WithSecure's™ Security Cloud to detect anomalies in files or file metadata
- Sends suspicious executable files to WithSecure's™ Security Cloud for extended analysis
- Prevents malware from contacting a C&C server
- Uses automatic forensics and computer ecosystem anomaly detection to detect malware that other techniques are unable to prevent or detect

Benefits

- Proactive security against zero-day attacks and unique malware.
- Zero-day exploits have been detected before they have been public knowledge.
- Effective protection against custom malware.
- The more a malicious file has been modified to evade signature-based scanning, the more suspicious it looks to us.
- Our exploit protection focuses on prevention of the exploit phase itself.
- The way exploit writers typically modify their code to evade signature-based scans cannot bypass our exploit detection techniques.
- Exploit protection is constantly improved and tweaked as we collect more samples and refine the behavioral detection.
- Automatically deployed forensics algorithms generated by Security Cloud's AI systems.



1 Customer receives unknown file

2 Cloud lookup and local analysis

3 File sent to cloud for analysis

4 Deep cloud analysis

5 Verdict found

6 Subsequent queries immediately receive correct verdict

WithSecure™ Security Cloud

An overview of the components that make up Ultralight

Ultralight Core

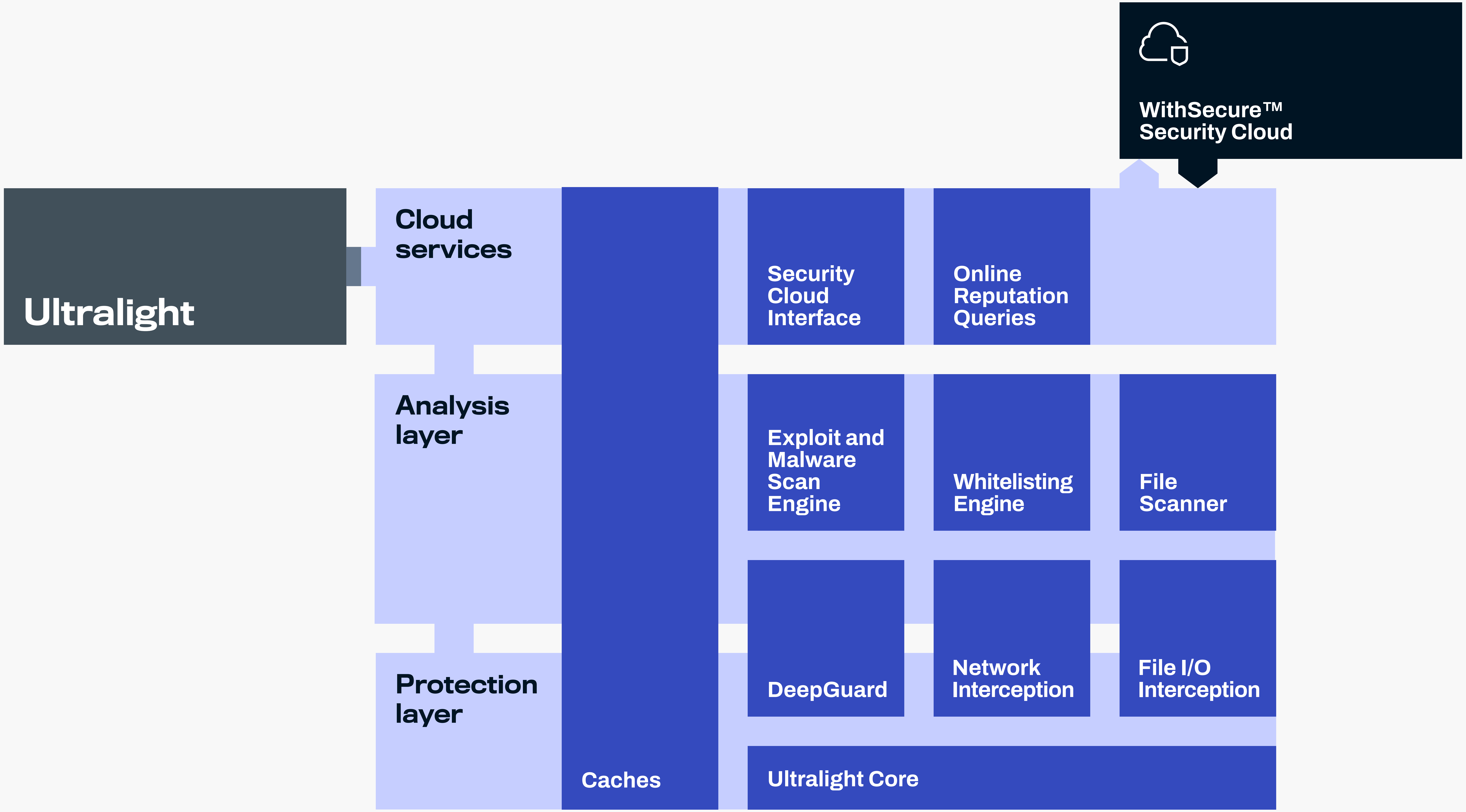
Ultralight Core consists of a set of components including a driver (Gatekeeper) responsible for filesystem interception and a set of services and components that host all other Ultralight technologies. In addition, it provides a common communication layer between all components, performance optimization mechanisms, and several basic protection services. As the name suggests, Ultralight Core supplies all the underpinnings required for Ultralight's technology stack to run.

- Provides on-access file scanning functionality.
- Provides on-demand file scanning functionality.
- Provides memory scanning functionality.
- Provides a "quick system scan" mechanism that runs forensics to determine if the system has been infected.
- Provides a filesystem interception driver.
- Provides malware and PUA remediation services and quarantine functionality.
- Provides persistent and non-persistent cache mechanisms.
- Provides several scanning performance optimizations.
- Hosts Ultralight components and technologies.
- Provides communication between Ultralight components.

Network Interception Framework (NIF)

Our Network Interception Framework is responsible for analyzing network traffic. It is used primarily to prevent exploit technologies from working and to prevent bots from connecting to command and control infrastructure.

- Utilizes cloud URL reputation queries to prevent a customer machine from contacting malicious or compromised sites.
- Prevents unknown sites from serving Flash, Java, Silverlight, or PDF files (exploit kits and other attack servers commonly use totally unknown fresh domains).
- Scans network traffic for exploits and known malware.
- Detects and blocks SSL MITM attacks performed by invasive governments by using SSL certificate reputation and analysis.
- Rapid detection of new exploit kit hosting sites via co-operation with Security Cloud and URL reputation rapid feedback mechanisms.
- Prevents known botnet command and control domains from working by querying URL reputation before allowing the DNS query.
- Facilitates banking protection functionality by isolating only trusted content during a banking session.
- Prevents users from accessing webpages associated with malicious certificates.
- Prevents users from accessing unwanted or disturbing content.
- Exploit and malware scan engine
- WithSecure's™ advanced scan engine. It is primarily used for exploit detection, file scanning and memory scanning.
- Detects malware from active process memory.
- Detects exploits and exploit kits.
- Detects prevalent malware and attack scripts.
- Detects on-the-wire exploits and malware (via NIF).
- Identifies file types.
- Provides several parsers for file formats commonly used by malware.
- Provides file unpackers and de-obfuscators.
- Provides archive traversal mechanisms.



WithSecure™ Security Cloud

Ultralight

Cloud services

Security Cloud Interface

Online Reputation Queries

Analysis layer

Exploit and Malware Scan Engine

Whitelisting Engine

File Scanner

Protection layer

DeepGuard

Network Interception

File I/O Interception

Caches

Ultralight Core

Exploit and malware scan engine

WithSecure's™ advanced scan engine. It is primarily used for exploit detection, file scanning and memory scanning.

- Detects malware from active process memory.
- Detects exploits and exploit kits.
- Detects prevalent malware and attack scripts.
- Detects on-the-wire exploits and malware (via NIF).
- Identifies file types.
- Provides several parsers for file formats commonly used by malware.
- Provides file unpackers and de-obfuscators.
- Provides archive traversal mechanisms.

Deepguard behavioral analysis engine

DeepGuard[4] provides exploit protection and malware detection by analyzing the behavior of processes in the system.

Features:

- Detects if MSOffice, Acrobat, Java or other common attack vectors are being exploited and blocks the exploit.
- Blocks malicious behavior of legitimate operating system applications such as PowerShell, Command Prompt and other commonly abused applications which are used for initial breaches and fileless attacks.
- Detects malware based on its actions in the system and blocks those actions.
- Does not need signatures, and thus is able to detect binary-unique malware.
- Provides zero-day exploit protection based on behavioral detections.

Online reputation queries and security cloud interface

vBoth Online Reputation Query and Security Cloud Interface components provide seamless file reputation and advanced file analysis capabilities. Ultralight components use Security Cloud services to enhance their decision-making and to avoid false alarms.

Features:

- Provides file, URL and metadata reputation services which provides protections to new threats in minutes.
- Provides a mechanism to offload resource-intensive file scanning operations.
- Provides advanced file analysis.

Whitelisting engine

This engine runs on the endpoint and is used to whitelist objects on the system. Whitelisting is used to improve the performance of our solution and as a mechanism to suppress false positives. It queries the Security Cloud to identify whitelisted objects. It also has a frequently updated local database to be able to function in offline situations.

Features:

- Provides intelligent local and network-based whitelisting.
- Provides certificate-based whitelisting (both embedded and from catalogue).
- Since our whitelisting engine has its own certificate reputation system, we are not affected by CA breaches or misbehavior.

File scanner

WithSecure™ uses an OEM file scanner from a third-party partner. Its main role is to detect file-based threats from crimeware to advanced implants and provide local disinfection capabilities. It is lightweight since it does not carry a complete database of malware signatures, rather it works with various internal and third-party services within the WithSecure™ Security Cloud for reputation queries, false positive mitigation and AI-based analysis. WithSecure™ Security Cloud ensures privacy by ensuring that the data being sent are anonymized and Personally Identifiable Information filtered out.

Features:

- Fully featured file scanning engine.
- Provides risk profile to unknown samples to identify whether more advanced analysis in the Cloud is needed

Ultralight updater

Ultralight Updater is a component that manages the configuration, installation and updating of all modules and components that make up Ultralight. Ultralight Updater works in the background and requires no configuration.

Features:

- Provides a fast, lightweight update mechanism for all Ultralight modules.
- Fully manages all component installations, updates, and uninstallations.
- Validates all component downloads, installations and update procedures.
- Requires no configuration.

References

1 Pilkey, Adam; F-Secure Blog; F-Secure's people, technologies help earn best protection accolades; published 21 Feb; https://blog.f-secure.com/people-technology-protection/

2 WithSecure™ Legal website; https://www.withsecure.com/en/about-us/legal/privacy

3 WithSecure™ Labs; WithSecure™ SECURITY CLOUD: https://www.withsecure.com/content/dam/with-secure/en/resources/withsecure-security-cloud-whitepaper-en.pdf

4 WithSecure™ Labs; DeepGuard: https://www.withsecure.com/content/dam/with-secure/en/resources/withsecure-deepguard-whitepaper-en.pdf

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.