

Solution overview



Part of WithSecure™ Elements
Extended Detection and Response (XDR)

WithSecure™ Elements Endpoint Protection

Protect all your endpoints from a single cloud-native platform



WITH®
secure

Contents

Introduction to WithSecure™ Elements	3
1. Part of WithSecure™ Elements XDR.....	5
2. Solution overview	6
3. Elements Security Center.....	10
4. Computer protection	12
5. Mobile protection	16
6. Server protection	19
7. APIs and Integrations	22
8. Technical support	23
9. Data security.....	24
Who We Are.....	26

Last updated: September 2025

Information security classification: Public

Disclaimer: This document gives a high-level overview of the key security components in WithSecure™ Elements Endpoint Protection.

Details are omitted in order to prevent targeted attacks against our solutions. WithSecure™ is constantly improving its services.

WithSecure™ reserves the right to modify features or functionality of the Software in accordance to its product life cycle practices.

Introduction to WithSecure™ Elements

WithSecure™ Elements Endpoint Protection (EPP) is part of our modular WithSecure™ Elements Cloud platform, bringing Extended Detection and Response (XDR), Exposure Management, and Co-Security Services to a unified pane of glass. WithSecure™ Elements EPP helps companies prevent threats like ransomware and data breaches across workstations, laptops, mobile devices, and servers.

WithSecure™ Elements allows flexibility to build resilient cyber security


In today's agile business environment, the only constant is change. WithSecure™ Elements offers companies all-in-one security that adapts to changes in both the business and the threat landscape, growing along with the organization. It offers flexibility in licensing models and in its pick-and-choose security technology modules. Moreover, customers can easily shift from self-managed to a fully managed service, or choose something in between. In other words, companies that struggle to find employees with cyber security skills can stay protected amid the ever-developing attack landscape.

WithSecure Elements provides customers with complete protection in one unified platform and easy-to-use security center. It provides you with proactive and reactive security capabilities from a single platform. The centralized platform combines powerful predictive, preventive, and responsive security capabilities into intelligent protection against threats from ransomware to targeted attacks. Our unparalleled simplicity lets customers focus on what is the most valuable to them. WithSecure™ Elements can be part of the customer's eco-system. It can easily be connected with their SIEM, SOAR, security management, monitoring or reporting systems.

Software Modules



Exposure Management



Extended Detection and Response


Endpoint Security

Collaboration Protection


Identity Security

Cloud Security

Co-Security Services



Elements Infinite



Managed Detection and Response

Co-Monitoring

Elevate

Incident Response

Incident Readiness

Benefits of the integrated solutions

Elements protects you against known threats, allows you to detect and investigate advanced attacks, and proactively secures your environment by identifying threats that could be exploited. The modular WithSecure™ Elements solution adapts to your company's changing needs. Unified cyber security means easier licensing, fewer security management tasks and more productivity without sacrificing your company's cyber security posture. The cloud-based console – WithSecure™ Elements Security Center – provides centralized visibility, insights and management across all endpoints and cloud services. It is fully managed by one of our certified Managed Service Providers, or self-managed with on-demand support from WithSecure™ for tough cases.

All our endpoint solutions use a single software agent that is required to deploy only once. The add-on solutions can then later be activated without having to deploy additional solutions. WithSecure™ Elements Collaboration Protection and WithSecure™ Elements XDR Cloud Security are cloud-based solutions that do not require installations to company endpoints. In addition to deployment and management benefits, the WithSecure™ Elements solutions are designed to work together, maximizing the security benefits for the company.

Elements Endpoint Security for Endpoint Protection, Detection and Reponse

WithSecure™ Elements Endpoint Security is a key component of our Elements XDR offering. Endpoint Security combines Elements EPP and WithSecure™ Elements Endpoint Detection and Response (EDR) into one consolidated package. It keeps your endpoints protected against sophisticated attacks with our award-winning advanced endpoint security. Elements Endpoint Security combines our EPP's essential security capabilities and automated patch management with our EDR's Broad Context Detections™ to enable quick detection and response even to the most advanced threats.

- **WithSecure™ Elements Endpoint Protection:** WithSecure's multiple AV-TEST Best Protection winner, cloud-native, AI-powered endpoint protection solution can be deployed in easy and flexible way to manage the security of all your endpoints, keeping your organization fenced in from attacks. Integrated patch management helps keep your software resilient against the latest threats. WithSecure™ Elements EPP covers mobiles, desktops, laptops and servers.
- **WithSecure™ Elements Endpoint Detection and Response:** Gain full visibility to advanced threats with our endpoint detection and response. With our unique Broad Context Detection™, you can minimize alert noise and zero in on incidents, and with automated response you can effectively stop breaches around the clock. WithSecure™ Elements EDR covers desktops, laptops and servers.



Award-winning Endpoint Protection

Our ability to provide better, more consistent protection than our competitors is proven year-by-year by testing done by independent industry experts and analysts.

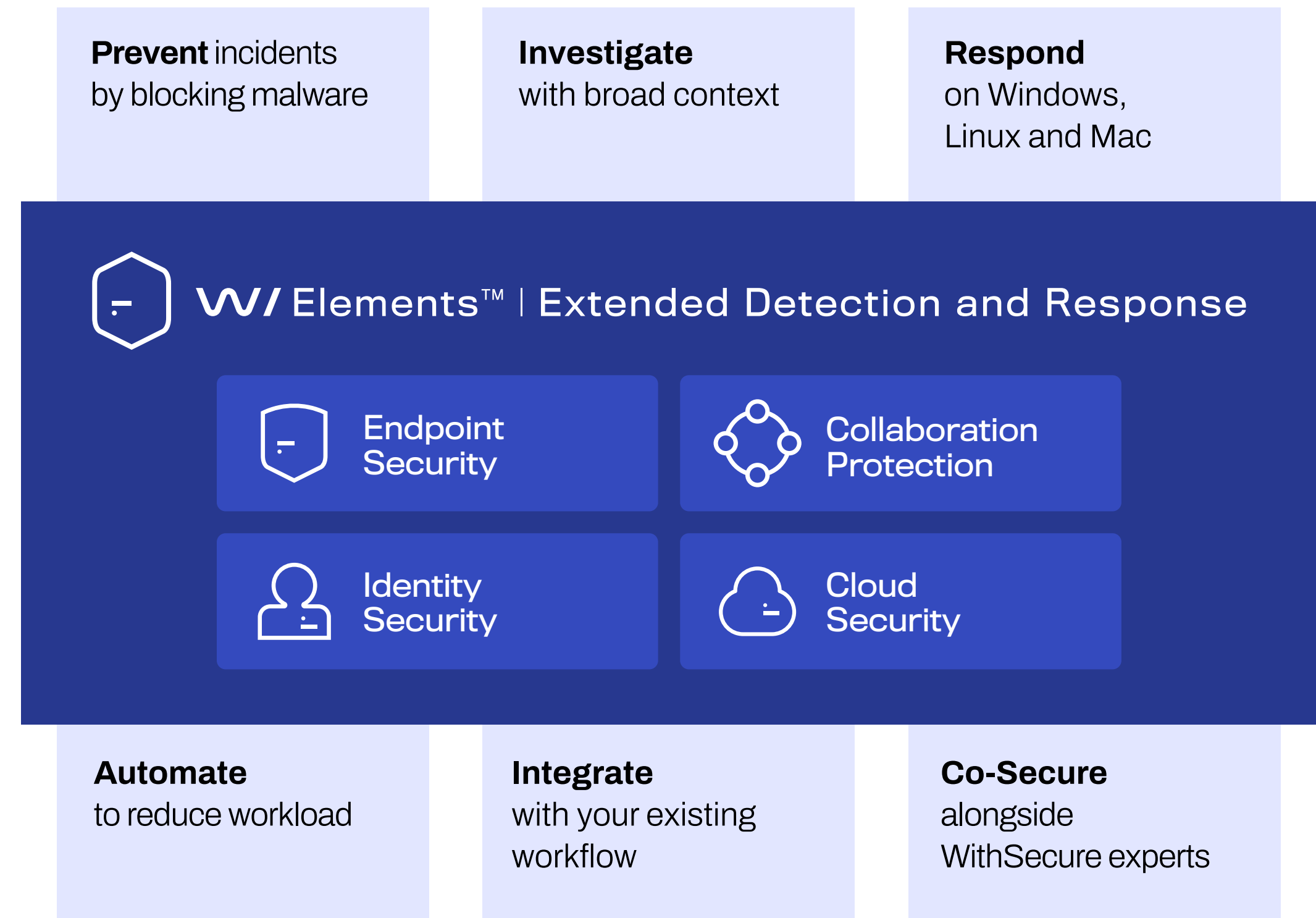
WithSecure™ has demonstrated its consistency in independent tests by winning the prestigious annual AV-TEST 'Best Protection' awards for business products 7 times since its inception with 100% protection against ransomware, data stealers, and zero-day malware attacks. AV-Test is making comparison tests continuously throughout the year so in order to reach this precious award one needs to consistently show good results in protection tests. To meet these demanding standards, the solution utilizes a multi-layered approach to security and leverages various modern technologies, such as heuristic and behavioral threat analysis, and real-time threat intelligence provided via the WithSecure™ Security Cloud.

This ensures that you're at the forefront of security.

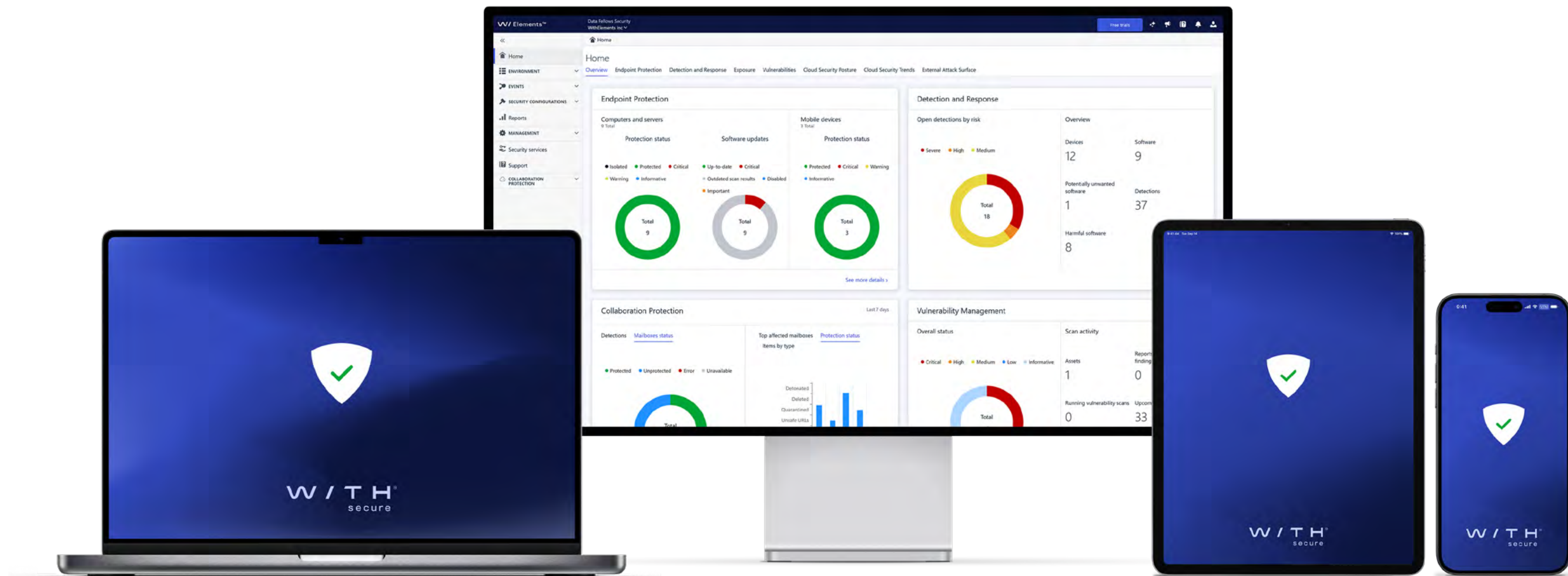
1. Part of WithSecure™ Elements XDR

WithSecure™ Elements Endpoint Security is a module of WithSecure™ Elements Extended Detection and Response (XDR) that has been designed for modern IT estates.

Not only does Elements XDR enable organizations to understand and respond to advanced threats across endpoints, identities, emails and collaboration tools, but its automated advanced preventative controls keep incident volumes and lower-level attacks at bay. Elements XDR enables you to recognize the entire attack chain that poses a threat to your business, extending beyond endpoints. Recognizing attacks early not only gives you a head start in reacting but can also save money by reducing the repercussions that follow from a compromised security posture.



2. Solution overview



Companies are facing challenges in minimizing the business risk brought on by cyber threats like ransomware. WithSecure™ Elements Endpoint Protection is designed from the ground up to solve challenging business security needs with minimum maintenance and management overhead. It offers award-winning best protection for Windows and Mac computers, iOS and Android mobile devices and a variety of server platforms. With integrated patch management, layered protection, and advanced behavior and heuristic analysis, Elements Endpoint Protection stops tomorrow's cyber threats – today.

WithSecure™ Elements Endpoint Protection delivers:

- **Best protection** in the industry improves business continuity and saves time in incident recovery
- **Proactively minimizes business risk** of cyber breaches with fully integrated patch management
- **Cloud-native solution** saves time in deploying, managing and monitoring security

WithSecure™ Elements Endpoint Protection is also available as a fully managed service. WithSecure™ certified service providers can use Partner Managed or SaaS version of the solution to leverage many unique service provider features, like multi-company dashboard, reporting and subscription management. The SaaS version of the solution allows service providers to utilize flexible business models, e.g. Usage Based Invoicing for all the WithSecure™ Elements products.

2.1 Solution packages for endpoints

Elements Endpoint Protection solution's Computer and Server Protection are available as standard and premium packages. Standard features include advanced anti-malware, patch management and many other endpoint security capabilities. Premium features add even better protection against ransomware along with application control.

Both Endpoint Protection packages can be complemented with Elements Endpoint Detection and Response. The detection and response features bring improved visibility, detection and automated response into advanced threats and breaches.

WithSecure™ Elements Exposure Management helps to discover and manage critical vulnerabilities in the endpoints. It provides system and third party patch status and automated updates by using Elements EPP's Software Updater. In other words, it has been designed to seamlessly integrate with our EPP to enable the quick patching of exposures.

WithSecure™ Elements for endpoints



WithSecure™ Elements Endpoint Protection (Standard)

Advanced anti-malware and patch management



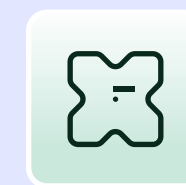
WithSecure™ Elements Endpoint Protection (Premium)

EPP Standard features plus additional protection including DataGuard, endpoint encryption, and application control



WithSecure™ Elements Endpoint Detection and Response

Advanced threat detection and response



WithSecure™ Elements Exposure Management

Proactive digital exposure management, with integration for quickly patching endpoints (requires Elements EPP)

The different protection feature packages can be activated without having to re-install client software.

More information on [WithSecure™ Elements](#)

2.2 Feature Highlights of Elements EPP

Software Updater

Automated patch management to update Microsoft and Mac and 2500+ 3rd party software apps.

DeepGuard

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

For more information: [WithSecure™ DeepGuard whitepaper](#)

Web content control

Improve security and productivity with controlled access to websites. Prevent access to websites based on categories and enforce your corporate policy.

Connection control

Activate additional security for sensitive transactions such as online banking.

Real-time protection

WithSecure™ 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

Device Control prevents threats from entering your system via hardware devices such as USB sticks, CD-ROM drives, and web cameras. This also prevents data leakage, by allowing read-only access, for example.

DataGuard (Premium)

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

Application Control (Premium)

Blocks execution of applications and scripts according to rules created by our penetration testers, or as defined by the administrator. In addition, Application Control can be used to block loading of DLL's or other files for additional security.

XFENCE

Unique security capability for protecting Macs against malware, trojans, back doors, misbehaving applications, and other threats by preventing applications from accessing files and system resources without explicit permissions.

Endpoint Encryption (Premium)

Monitor and manage the status of your Windows computers' disc encryption. You can turn Bitlocker encryption on and off, and get recovery keys directly from WithSecure™ Elements Security Center.

Outbreak Control

Outbreak Control provides ability to automatically change EPP profiles to be more restricted, if they have open medium, high or critical severity EDR detections or a Dynamic Risk Score above a certain threshold in Exposure Management. Once the issue has been resolved, the endpoint returns to its original profile.

2.3 Solution components

The solution is composed of four main components, each described in this document:

1. **Elements Security Center** as a cloud-based management portal (*always included*)
2. **Computer Protection** as a dedicated security client for workstations (Windows, Mac, Linux*)
3. **Mobile Protection** for mobile devices (iOS, Android)
4. **Server Protection** for a variety of server platforms (Windows, Citrix, Linux)

2.4 Solution deployment

Endpoint security clients can be deployed by email, batch scripting, local installation, enterprise management systems (SolarWinds, Kaseya, Datto) or with an MSI package via domain-based remote installation tools (provided by you or a third party). Similarly, Mac clients are deployed as packages using macOS Installer or Mobile Device Management tools and can be configured with additional deployment steps into custom signed packages.

For normal deployments, all endpoint security client deployments can be initiated from the portal via an email flow. For larger environments, you can create an MSI package that can be deployed with your own remote installation tools. The Windows client also contains built-in program flags, which can be used to automate client deployment via batch scripting.

Whenever the Windows client is deployed on systems with a conflicting security solution, our sidegrade feature detects it and automatically uninstalls it before continuing with the installation of WithSecure™ software. This ensures a much smoother and faster transition from one vendor to another.

When a new computer is added to Elements Endpoint Protection, a default configuration (profile) can be assigned automatically based on its location in an Active Directory hierarchy. A default profile can also be assigned based on network information or a hostname. This streamlines the deployment process and reduces risks for misconfiguration.

Mobile Protection features are commonly deployed by using a third-party Mobile Device Management (MDM) available with a subscription that supports the use of external MDM solutions.

The patch management capabilities are fully integrated into Windows server and workstation clients and Mac clients, and can be controlled via the management portal. As a hosted solution, there is no need to install separate agents or management servers or consoles, unlike with traditional patch management solutions.

WithSecure™ Elements Connector is provided by WithSecure™ in order to minimize the bandwidth usage while downloading updates to Computer Protection clients. This proxy caches malware signature database updates as well as software updates of the Computer Protection client itself and patch

management software updates. In addition, the connector can be used as an interface between WithSecure™ Elements and your SIEM systems.

Endpoint protection client software update malware signature databases and the client software itself automatically without administrator having to worry about the updates or upgrades manually.

WithSecure™ partners can customize both the endpoint protection client software and the Elements Security Center with their logo and support link.

Please find the most up-to-date information on solution deployment details and other technical requirements in our [User Guide for Elements EPP](#).

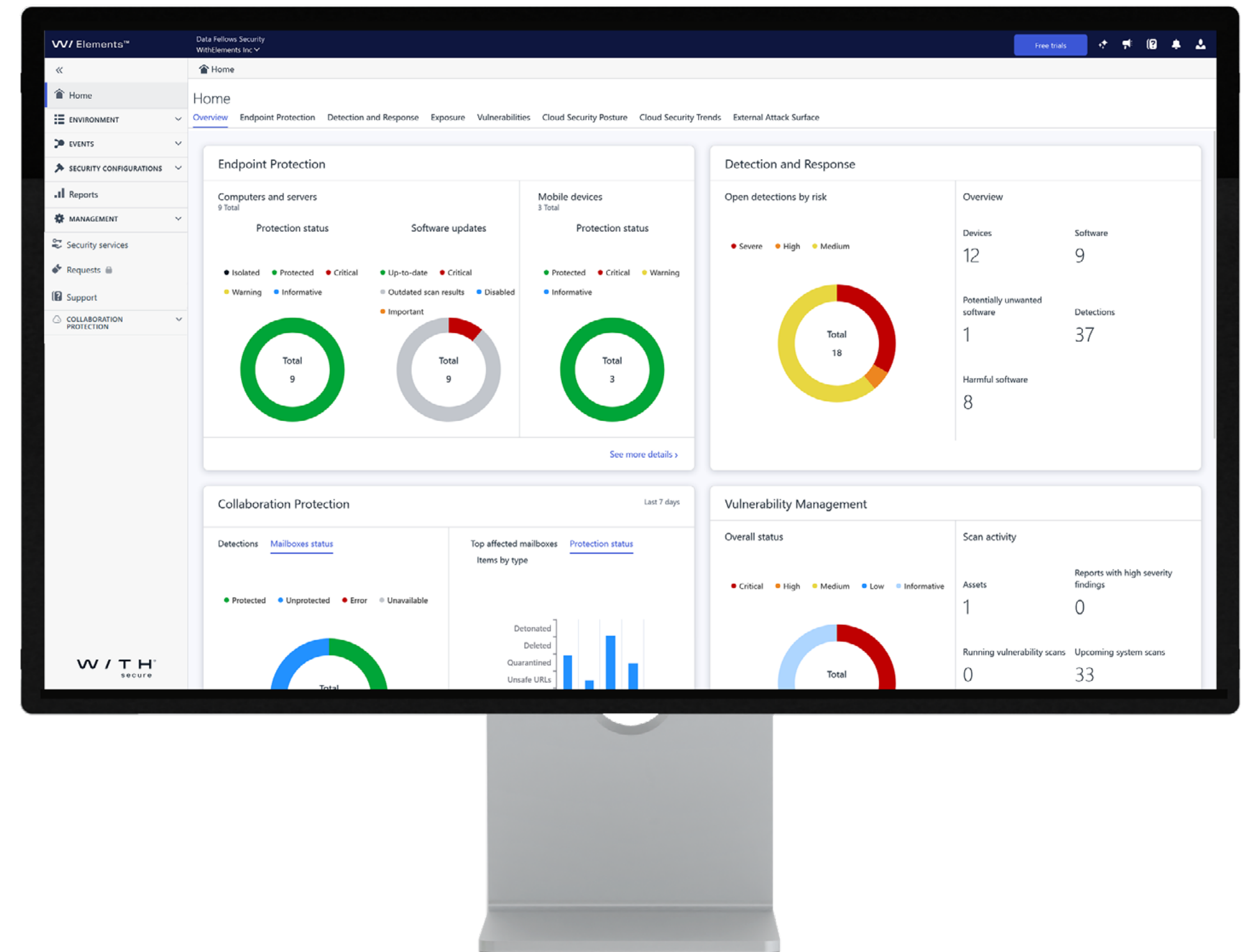
* Conditions apply. Please contact your sales representative.

3. Elements Security Center

WithSecure™ Elements Endpoint Protection makes it easy to deploy, manage, and monitor the security of your endpoints from a single, intuitive console. It gives you excellent visibility into all of your devices.

The Security Center was designed from the ground up to simplify and accelerate security management in demanding, multi-device and multi-site environments. Below are some examples of how the solution considerably reduces the amount of time and resources needed for security maintenance and management:

- Endpoint clients automatically receive client, security, and database updates, minimizing the time needed for updates and maintenance
- By consolidating the security management of various endpoints and tools into one portal, the overall management is streamlined considerably, saving time
- Patch Management can be set up to deploy missing security patches automatically as soon as they are available, saving time from manual software updates
- As a hosted service, there is no server hardware or software to install or maintain – all you need is a browser
- The portal has been designed to utilize the most optimal user journeys, greatly increasing user efficiency
- The console-endpoint communication works in real time. This allows IT admins to manage and monitor the security of the environment without disruptions or delays caused by polling intervals.



In essence, it allows IT admins to configure, deploy, and validate changes in one go. And if there is a security incident that needs to be solved ‘right now’, you can deploy a fix immediately.

You can create and customize individual security policies (profiles) and assign them either individually or in groups to computers, and servers by using labels. All settings and policies can be enforced down to the individual level if needed, so that end-users cannot change them. Policies can be created e.g. per Active Directory group and assigned automatically to devices attached to the group.

The management portal gives you a complete overview of the security status of your entire environment. This includes potential software vulnerabilities, missing security updates, and the status of security features like real-time scanning and firewall. By using Security Events, IT admins can easily see all alerts in one central location.

For example, you can track the number of blocked infections and pay closer attention to the devices that are attacked the most. You can set automatic email alerts so that specific infection parameters get your attention first. If you need more information on any particular infection, you can obtain it directly from our security database.

The management portal delivers a wide range of graphical reports in an intuitive format, making data easier and faster to digest and understand—and more appealing for stakeholders to read. Device security details can also be exported as CSV files if required.



4. Computer protection

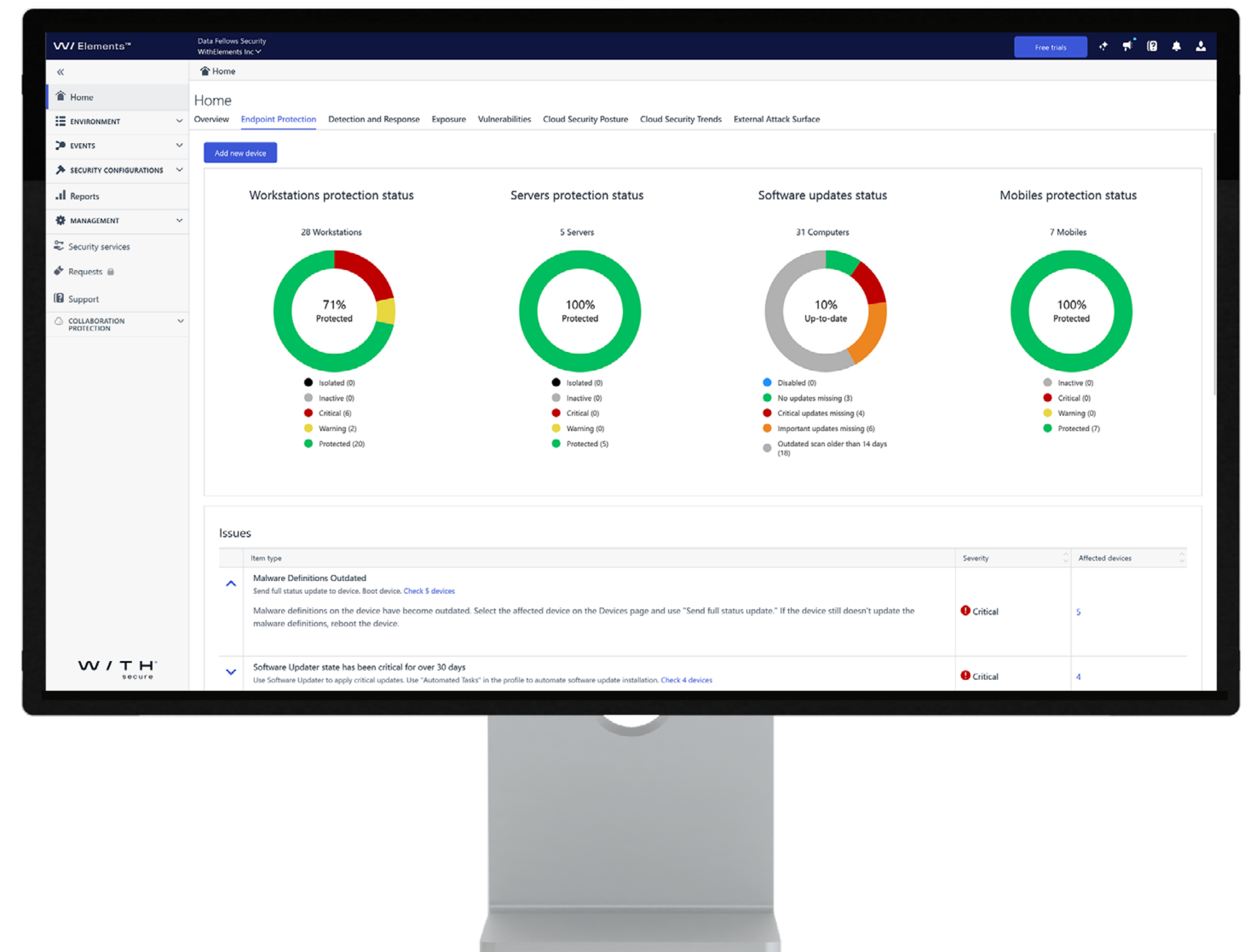
Endpoint Protection for Computers forms the cornerstone of any secure environment. In today's security landscape, it is vital to ensure that protection goes well beyond traditional anti-malware. WithSecure™ Elements Endpoint Protection for Computers delivers simple, powerful, and resource-friendly security for Windows, Mac, and Linux laptops and other workstations.

4.1 Combining endpoint protection stack into one

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 cloud.

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.

For more information: [WithSecure™ Ultralight technical whitepaper](#)



4.2 Heuristic and behavioral threat analysis

Heuristic and behavioral threat analysis, done by WithSecure™ DeepGuard, is critical in identifying and blocking the most sophisticated malware prevalent today. DeepGuard provides immediate, proactive, on-host protection against new and emerging threats by focusing on malicious application behavior rather than static identification of specific, known threats.

This shift in focus allows it to identify and block previously unseen malware based on their behavior alone, neatly providing protection until security researchers are able to analyze and issue a detection for that specific threat.

By communicating with our WithSecure™ Security Cloud, DeepGuard is also able to use the latest reputation and prevalence information available for any previously encountered object to fine-tune its security evaluations, reducing the risk of false positives or redundant analyses that can interfere with the user experience.

The on-host behavioral analysis also extends to intercepting attacks that attempt to exploit vulnerabilities in popular programs in order to install malware onto the machine. DeepGuard is able to identify and block routines that are

characteristic of an exploit attempt, preventing exploitation – and in turn, infection. Exploit interception safeguards users from harm, even when vulnerable programs are present on their machine.

For more information: [WithSecure™ DeepGuard technical whitepaper](#)

4.3 Real-time threat intelligence

The security client uses real-time threat intelligence provided by WithSecure's Security Cloud, ensuring that all new or emerging threats are identified, analyzed, and prevented within minutes. A cloud-based threat analysis service affords many benefits over traditional approaches. WithSecure™ gathers threat intelligence from tens of millions of client nodes, building a real-time picture of the global threat situation.

For example, if heuristic and behavioral threat analysis identifies a zero-day attack on another endpoint on the other side of the world, the information is shared with all protected devices via WithSecure™ Security Cloud—rendering the advanced attack harmless mere minutes after initial detection.

For more information: [WithSecure™ Security Cloud technical whitepaper](#)

4.4 Designed specifically for macOS

WithSecure™ Elements EPP Computer Protection for macOS includes XFENCE, a unique security tool for Macs. The product takes advantage of modern macOS security capabilities enhancing the protection against malware, trojans, back doors, misbehaving applications, and other threats without sacrificing usability and performance. The powerful XFENCE protection prevents errant processes, ransomware and other malware from accessing your files and system resources without explicit permission.

Elements EPP for macOS computers leverages advanced rule-based analysis to monitor apps that attempt to access confidential files and system resources, enhanced by the threat intelligence provided by Security Cloud to minimize false positives and user interaction through allow/disallow prompts.

In addition, WithSecure™ Elements EPP Computer Protection for macOS provides application layer firewall that can configure and control network access on application level. It can be used to isolate hosts, to allow network access only to trusted signed applications, and to blacklist/whitelist applications by bundle id. The solution comes with admin tools for easy deployment and management of the Mac clients.

4.5 Protection for Linux endpoints

WithSecure™ Elements Endpoint Protection includes protection for Linux in WithSecure™ Server Protection. The product can be used to protect endpoint devices as well.*

4.6 Integrated patch management

Elements Endpoint Protection for Windows and Mac computers includes an automated patch management feature that is fully integrated with the clients. There is no need to install separate agents, management servers, or consoles.

It works by scanning for missing updates, creating a vulnerability report based on missing patches, and then downloading and deploying the patches automatically. You can also choose to install updates manually if needed. Security patches include Microsoft OS updates and 2500+ third-party applications such as Google Chrome, Firefox, Zoom, Java, OpenOffice, and others that commonly serve as attack vectors due to their popularity and larger number of vulnerabilities. Availability of third-party patches varies depending on whether you use Elements EPP for macOS or Windows computers.

Administrators can define detailed exclusions for the automatic mode based on software names or bulletin IDs. Some updates are excluded by definition, such as Service Packs. Administrators can also flexibly define the day and time when installations should be performed, as well as how

restarts are forced and the grace time before forcing a restart after installation.

4.7 Multi-engine anti-malware

Our computer component utilizes a proprietary, multi-engine security platform to detect and prevent malware. It offers superior protection compared to traditional signature-based technologies:

Patch management is a critical security component. It's the first layer of protection when malicious content reaches endpoints and can prevent up to 80% of attacks simply by installing software security updates as soon as they become available.

- Detects a broader range of malicious features, patterns, and trends, enabling more reliable and accurate detections, even for previously unseen malware variants
- By using real-time look-ups from WithSecure's Security Cloud, it can react faster to new and emerging threats in addition to ensuring a small footprint
- Emulation enables detection of malware that utilize obfuscation techniques, and offers another layer of security before a file is run.

4.8 Location based profiles

WithSecure™ Elements EPP can be configured to trigger different configurations based on the endpoint's location. For example, the admin can set up network locations and rules so that when a device is at home, the Patch Management and firewall are on, but when at the office, both Patch Management and firewall are off.

4.9 Assign automated tasks

WithSecure™ Elements Endpoint Protection can be configured to run certain automated tasks in a very granular manner. For example, product updates can be configured to be run at a specific time and missing critical and other security updates can be installed immediately. You can scan for missing security updates every day, and run a full system scan for malware on every weekday. By using the automated tasks, you can configure endpoint protection to fit into your company's security needs with minimal performance impact.

* Conditions apply. Please contact your sales representative.

4.10 Extensive web protection

Furthermore, the solution offers extensive and proactive web protection, ensuring the most exploited attack vector is well defended.

- It proactively prevents access to malicious and phishing sites even before they are accessed (e.g. on Google search and when clicking on a web link). This is particularly effective, as early intervention greatly reduces overall exposure to malicious content and therefore to attacks.
- It prevents the exploitation of active content that is utilized in the vast majority of online attacks. These components, that are used for example in Java, are automatically blocked on unknown and suspicious sites based on their reputation data, with the option of setting exclusions.
- The solution can also be used to restrict inappropriate web usage, granularly denying or allowing access to non-work-related destinations, such as social media sites and adult sites, to maximize efficiency and avoid malicious sites.
- After the initial layers of web protection, the content in HTTP web traffic is also subjected to analysis in order to provide additional protection against malware, before it gets into contact with the endpoint itself.
- IT admins can also designate business-critical web activities that utilize HTTPS (like intranets or sensitive cloud services, for example CRMs) to use an additional security layer. When active, it closes all untrusted network connections, preventing attacks and exfiltration of data from the services during the session.

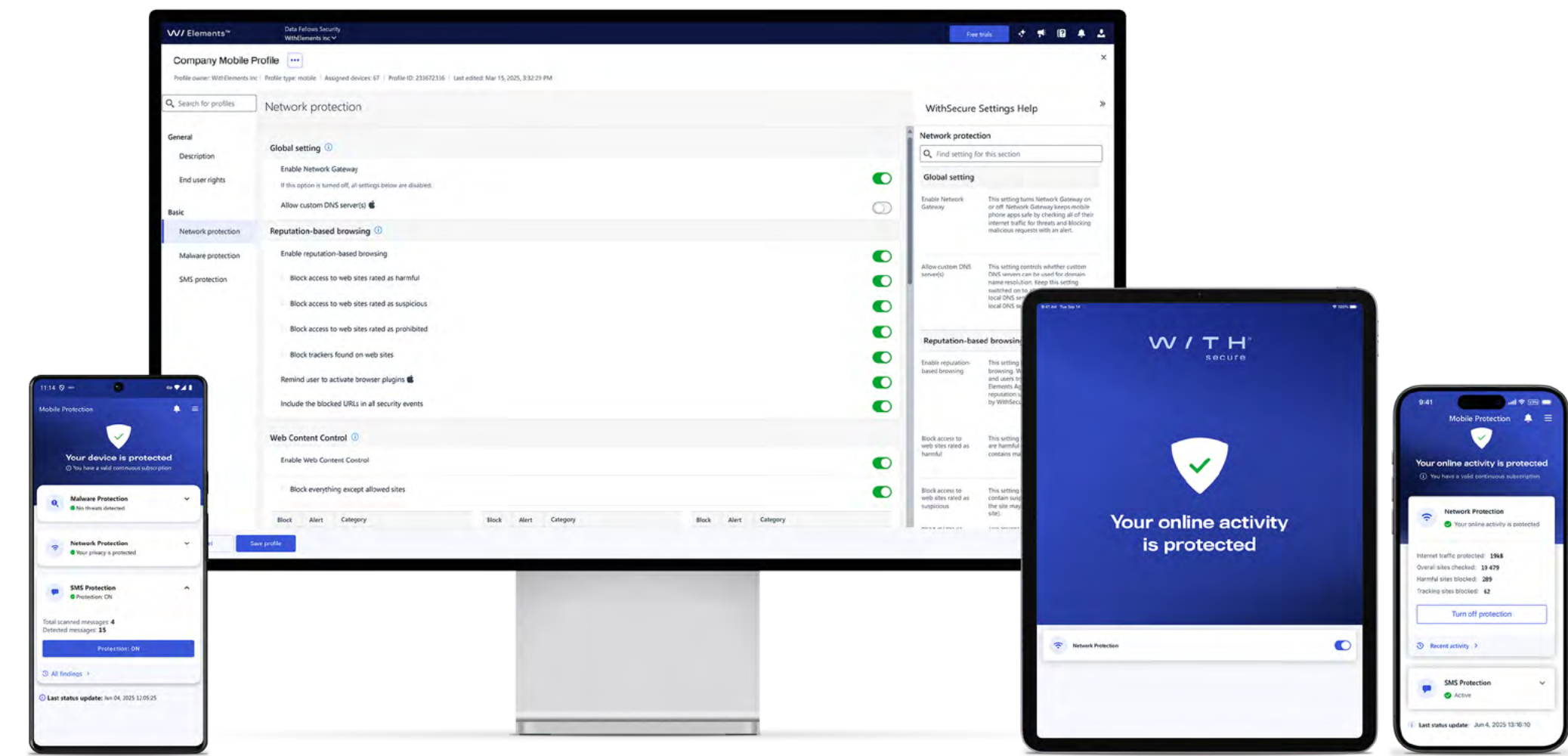
The security features vary depending on the chosen operating system. Here is an overview of the feature comparison between Windows, macOS, and Linux.

	Windows	macOS	Linux**
Anti-malware	✓	✓	✓
DeepGuard	✓	—	—
DataGuard (Premium)	✓	✓*	—
Security Cloud	✓	✓	✓
Patch management	✓	✓	—
Application control (Premium)	✓	—	—
Browsing protection	✓	✓	—
Web traffic scanning	✓	—	—
Web content control	✓	✓	—
Content type filtering	✓	—	—
Connection control	✓	✓	—
Firewall	✓	✓	—
Integrity checking	—	—	✓
Endpoint Encryption (Premium)	✓	—	—
System Event Detection (Premium)	✓	—	—

* Part of the functionality provided by XFENCE.

** Conditions apply. Please contact your sales representative.

5. Mobile protection



Maintaining control over mobile devices is a fundamental aspect of modern cyber security. WithSecure™ Elements Mobile Protection allows IT admins have an easy way to secure and control mobile devices, both Android and iOS.

The components delivered by WithSecure™ Elements Mobile Protection include everything that is needed for exceptional mobile protection in one package: Network Gateway, browsing protection, and proactive application (Android) and web protection. The mobile client is also designed to complement and be deployed via third-party MDM solutions.

5.1 Network Gateway

Using a Network Gateway, Elements Mobile Protection can check every website visited. By using WithSecure's Security Cloud, it is able to limit or block access to dangerous websites.

The Security Cloud provides a URL reputation service, powered by machine learning, which analyzes many millions of URLs to check what kind of content those provide. By using a Network Gateway, Elements Mobile Protection evaluates the reputation of URLs before the websites are loaded. Harmful websites are fully blocked and sites containing certain categories of content, for example adult or gambling content, can be optionally blocked.

Network Gateway's innovative architecture eliminates latency and buffering, ensuring a seamless browsing experience. Network Gateway provides enhanced security and advanced control for both iOS and Android devices:

- For iOS, the Safari extension seamlessly integrates with existing VPN setups, ensuring that all iOS users can enjoy the same level of protection, regardless of their VPN preference.
- For Android, Network Gateway offers a variety of features to protect devices from malicious websites and content.

5.2 Security Cloud

The security client uses real-time threat intelligence provided by WithSecure™ Security Cloud, ensuring that all new or emerging threats are identified, analyzed, and prevented within minutes.

A cloud-based threat analysis service affords many benefits over traditional approaches. We gather threat intelligence from tens of millions client nodes, building a real-time picture of the global threat situation. For example, when an APK or file is downloaded, it is scanned and additionally its reputation is checked in the Security Cloud. Malicious files are prevented from running and unknown files or apps are uploaded for deeper analysis. Scan results benefit all users, for example by minimizing false positives and rendering new attacks harmless in a matter of minutes.

5.3 Application protection

When the Network Gateway is active, mobile devices are automatically protected against malware and malicious content. WithSecure™ service nodes scan the traffic at the network level, utilizing the full extent of available security analytics. This allows us to provide better security than traditional mobile security solutions:

- Security is not hampered by limited mobile device resources
- Resource-intensive processes do not impact device performance and battery life
- Network-level scanning prevents contact with malicious content in the first place.

For Android devices, security is further enhanced with local scanning including real-time reputation checks from the WithSecure™ Security Cloud.

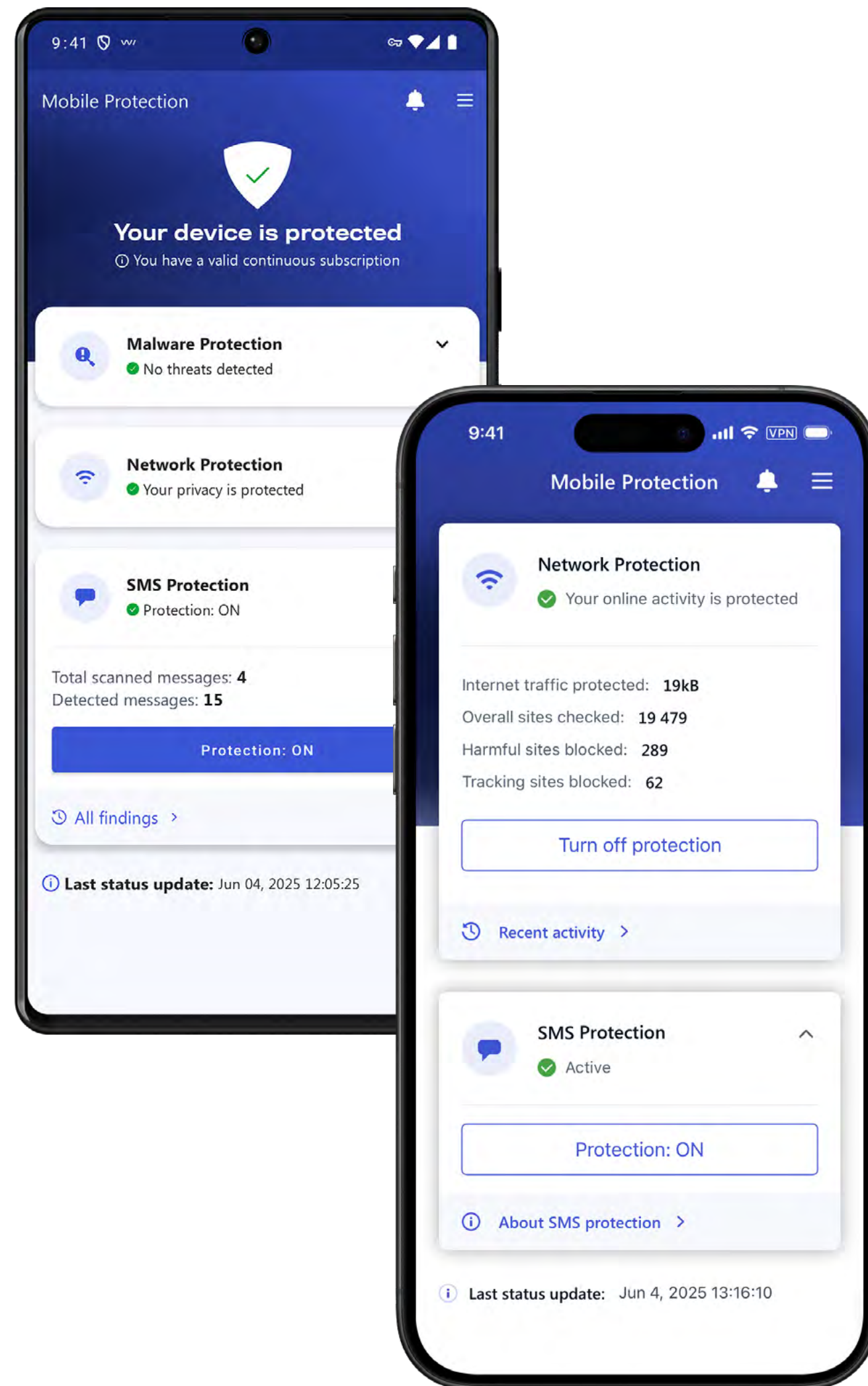
5.4 Browsing protection

Browsing protection is a key security layer that proactively prevents end-users from visiting malicious sites. This is particularly effective, as early intervention greatly reduces overall exposure to malicious content - and therefore to attacks.

For example, Browsing protection prevents end-users from being tricked into accessing seemingly legitimate phishing sites, accessing malicious sites through an email link, or getting infected through malicious third-party advertisements on otherwise legitimate sites.

5.5 Faster browsing and less data use

The component is designed to have a minimal impact on mobile performance and battery life. In fact, by using traffic compression and preventing online tracking and advertising with Anti-Tracking, it increases browsing speed.



5.6 SMS Protection

Block malicious and phishing SMS messages with SMS Protection. SMS messages are scanned for malicious URLs and next for iOS, the scanned malicious messages are moved to junk and for Android, you will get suspicious SMS message alerts. You also have the option to manually check messages (incl. QR codes) for unsafe content in WhatsApp and Telegram via Sharetools.

SMS Protection analyzes messages locally on your device for security threats, so that your messages never leave your device and are not transmitted to external servers.

Detection details can be investigated both in the mobile app and in the Elements Security Center. Corporate admins can manage the SMS phishing protection related configuration in Elements Security Center and will receive security events related to phishing protection from individual devices.

5.7 Third-party MDM deployment

The mobile client is also designed to complement and be deployed via third-party Mobile Device Management (MDM) solutions.

Supported MDM solutions:

- VMware Workspace ONE
- IBM Security MaaS360
- Google Workspace MDM
- Microsoft Intune
- Miradore
- Ivanti Endpoint Manager
- Samsung Knox

By using a dedicated security component on top of the basic capabilities provided by the MDM solution, IT admins can significantly increase the security against malware, data theft, and phishing attempts that target mobile devices.

6. Server protection

Servers are critical to a company's communication, collaboration, and data storage. WithSecure™ Elements EPP for Servers provides security for servers while enabling them to run at peak performance. The solution provides security for Windows, Citrix, and Linux servers.

Here is an overview of the core capabilities for different server platforms.

	Windows	Citrix	Linux
Core security			
Anti-malware	✓	✓	✓
DeepGuard	✓	✓	—
Security Cloud	✓	✓	✓
Patch management	✓	✓*	—
Browsing protection	✓	✓	—
Web traffic scanning	✓	✓	—
Firewall	✓	—	—
Integrity checking	—	—	✓
Remote management via portal			
Security management	✓	✓	✓
Security monitoring	✓	✓	✓

* Includes Windows OS and 3rd party application updates (the Citrix platform uses a Windows client).

6.1 Heuristic and behavioral threat analysis

Heuristic and behavioral threat analysis, done by DeepGuard, is critical in identifying and blocking the most sophisticated malware prevalent today. DeepGuard provides immediate, proactive, on-host protection against new and emerging threats by focusing on malicious application behavior rather than static identification of known threats. This allows it to identify and block previously unseen malware based on behavior alone, providing protection until security researchers are able to issue a detection for that specific threat.

By communicating with our Security Cloud, DeepGuard is also able to use the latest reputation and prevalence information available for any previously encountered object. This enables DeepGuard to fine-tune its security evaluations, reducing the risk of false positives or redundant analyses that can interfere with the user experience.

The on-host behavioral analysis extends to intercepting attacks that attempt to exploit vulnerabilities in popular programs in order to install malware onto the machine. DeepGuard is able to identify and block routines that are characteristic of an exploit attempt. Exploit interception safeguards users from harm even when vulnerable programs are present on their machine.

6.2 Real-time threat intelligence

The security client uses real-time threat intelligence provided by WithSecure's Security Cloud, ensuring that all new or emerging threats are identified, analyzed, and prevented within minutes.

A cloud-based threat analysis service affords many benefits over traditional approaches. WithSecure™ gathers threat intelligence from tens of millions of client nodes, building a real-time picture of the global threat situation. For example, if the heuristic and behavioral threat analysis identifies a zero-day attack on another endpoint on the other side of the world, the information is shared with all protected devices via Security Cloud — rendering the advanced attack harmless mere minutes after initial detection.

6.3 Integrated patch management

The component includes an automated patch management feature that is fully integrated with Windows server clients. There's no need to install separate agents, management servers, or consoles.

The patch management works by scanning for missing updates, creating a vulnerability report based on missing patches, and then downloading and deploying them automatically. You can also choose to install updates manually if needed. Security patches include Microsoft updates and

2500+ third-party applications such as Google Chrome, OpenOffice, and others that commonly serve as attack vectors due to their popularity and large number of vulnerabilities. Availability of third-party patches varies depending on which server platform you are protecting with Elements EPP for Servers.

6.4 Multi-engine anti-malware

Our computer component utilizes a proprietary, multi-engine security platform to detect and prevent malware. It offers superior protection compared to traditional signature-based technologies:

- Detects a broader range of malicious features, patterns, and trends, enabling more reliable and accurate detections, even for previously unseen malware variants
- By using real-time look-ups from the WithSecure™ Security Cloud, it can react faster to new and emerging threats
- Emulation enables detection of malware that utilizes obfuscation techniques, and offers another layer of security before a file is run.

6.5 Proactive web protection

Furthermore, the solution offers extensive and proactive web protection for terminals, ensuring the most exploited attack vector is robustly defended.

- Proactively prevents access to malicious and phishing sites even before those are accessed. This is particularly effective, as early intervention greatly reduces overall exposure to malicious content, and therefore to attacks.
- After the initial layer of web protection, the content in web traffic (HTTP) is also subjected to analysis, in order to provide additional protection against malware, before it gets into contact with the endpoint itself.

6.6 Server Share Protection

Sharing files on local file servers is exposing organizations to risks of ransomware attacks, especially whenever devices out of the organization's full control can access the server shares and end up encrypting large amounts of important files — making the files unusable.

You can safely continue using Windows file shares by having Server Share Protection as an additional layer for ransomware protection, designed to immediately identify and rollback any encryption or other unintentional destruction of files. This safeguards your organization from spreading ransomware.

6.7 Citrix and Terminal Servers

On top of the same core security capabilities as for Windows servers, the Citrix component provides additional protection for Citrix environments by extending the integrated patch management capabilities for published applications. The client is Citrix Ready -certified, ensuring that it works flawlessly in Citrix environments. Similarly, Server Protection provides protection for Windows terminal servers. Please note that customers using Server Protection in remote desktop environments need a license for WithSecure™ Remote Desktop Protection as well.

6.8 Linux

Linux Protection provides core security capabilities for Linux clients: multi-engine on-access scanning, scheduled and manual scans, and integrity checking. It is designed to detect and prevent both Windows and Linux-based attacks, making it particularly useful in mixed environments, where an unprotected Linux machine can be used as an easy attack vector.

6.9 Integrity checking

The component comes with a built-in integrity checker, which detects and prevents attackers from tampering with kernels, system files, or configurations. It is a vital security feature, as it protects the system against unauthorized modifications, which could otherwise go unnoticed.

Integrity checking can be configured to send alerts to the administrator of any attempts to modify the monitored files. This makes unauthorized changes easy to detect, ensuring that any incident response actions can be taken without delay. If changes are needed on the baseline, for example due to OS, security, and software updates, admins can use a protected installation tool to make the necessary updates without any hassle.

7. APIs and Integrations

WithSecure™ Elements Endpoint Protection may be integrated using three different methods:

1. WMI (Windows Management Instrumentation)

WMI integration collects read-only status information on WithSecure™ client applications. The integration can be used for example to integrate with Remote Monitoring and Management (RMM) tools. On a service provider level, WMI integration is often used to provide better management of several functions, such as asset discovery and management, configuration, process and service automation, security services, and backups. Typically, an application (e.g. RMM, VPN Client) running on the device validates that the Elements Agent is running and that the device is protected.

There are more details about all the properties exposed through our WMI interface in [the Elements Endpoint Protection user guide](#)

2. Elements Connector

This is a one-way connector to easily forward Elements Security events to any SIEM (e.g. Microsoft Sentinel, Splunk, Qradar). Elements Connector requires no coding

work from you, it only needs to be deployed and configured. Once deployed, Elements Connector fetches security events per company or partner from Element API, and forwards them to your SIEM in a standard format (Syslog, CEF, LEEF). Elements Connector requires minimal maintenance, as it is managed from the Elements Security Center and it gets updated automatically.

3. Elements API

This REST API is a two-way API, designed to simplify integration with our Elements ecosystem. Elements API supports response actions and the management of EDR incidents. It is typically used by SIEM, SOAR, ITSM and other reporting tools to reduce workload and optimize how Elements is being used in serving your organization's specific needs.

Elements API not only provides a lot of information about security events, incidents, and devices but it can also be used to automate response actions. For example, you can trigger a scan, isolate a device, collect a diagnostic file and manage incidents by changing their status or adding comments – among many other actions and use cases.

Read more about our integrations at:

connect.withsecure.com



8. Technical support

WithSecure's additional support packages offer a collection of services for a more flexible and comprehensive support experience. Our support is available to you during business hours or even as a 24/7 service. We offer Advanced or Premium Support, with different levels of service to suit your needs.

Please contact our sales to find the right type of technical support for your business needs.



9. Data security

WithSecure™ Elements Endpoint Protection uses Amazon Web Services (AWS). This allows us to ensure high availability and fault tolerance, in addition to better response times and ability to scale as needed. Currently available geographic regions are Europe, North America, and APAC.

AWS states that each of their data centers are in alignment with Tier 3+ guidelines. For further information about the AWS datacenters, please see: <https://aws.amazon.com/compliance/>

WithSecure™ complies with the privacy regulations and laws in all the countries where it operates.

We take the security of the data centers very seriously, and keep them secure by using dozens of security measures, such as:

- **Security by design:** Our systems are designed from the ground up to be secure. We embed privacy and security in the development of our technologies and systems from the early stages of conceptualization and design to implementation and operation.
- **Rigorous access controls:** Only a small vetted group of WithSecure™ employees have access to the customer data. Access rights and levels are based on their job function and role, using the concept of least-privilege matching to defined responsibilities.
- **Strong operational security:** Operational security is an everyday part of our work, including vulnerability management, malware prevention and robust incident management processes for security events that may affect the confidentiality, integrity, or availability of systems or data.



Contact our sales to get comprehensive protection, detection, and response with Elements Endpoint Security.

[Contact sales](#)

Who We Are

WithSecure™, formerly F-Secure Business, is Europe's cyber security partner of choice. Trusted by IT service providers, MSSPs, and businesses worldwide, we deliver outcome-based cyber security solutions that protect mid-market companies.

Committed to the European Way of data protection, WithSecure™ prioritizes privacy, data sovereignty, and regulatory compliance.

Boasting more than 35 years of industry experience, WithSecure™ has designed its portfolio to navigate the paradigm shift from reactive to proactive cyber security. In alignment with its commitment to collaborative growth, WithSecure™ offers partners flexible commercial models, ensuring mutual success across the dynamic cyber security landscape.

Central to WithSecure's cutting-edge offering is Elements Cloud, which seamlessly integrates AI-powered technologies, human expertise, and co-security services. Further, it empowers mid-market customers with modular capabilities spanning endpoint and cloud protection, threat detection and response, and exposure management.

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

