**Brochure** 

Collaboration
Protection against
phishing and advanced
threats

WithSecure™ Elements Collaboration Protection





## Overview

It's each organizations' responsibility to verify that their cloud collaboration solution provides defenses against deception, social engineering, malicious content and targeted attacks. However, identifying and addressing potential gaps is a challenging task.

To mitigate cloud collaboration risks, you should consider using a purpose-built solution with the highest possible detection rates to protect users against advanced threats. Furthermore, a solution that can provide security from endpoints to the cloud is more cost-effective and weasier to manage.

As more and more users rely on Microsoft 385 protection, it's drawing attention from hackers to design and test their attacks to not get caught by standard Microsoft security.



Microsoft 365 is the world's most popular cloud collaboration service with 400 million mailboxes and more than 190 million SharePoint users.



Methods of attack are specifically tested and designed to go undetected by the standard Microsoft security measures.



Unusually convincing phishing campaigns are being launched via Microsoft 365 against companies of all sizes

# **Key Benefits**

## Minimize business disruption

Provides security powered by WithSecure's industry-leading threat intelligence technology against harmful content undetected by standard collaboration protection.

## More than email protection

Content types including email, calendar invites, tasks and sharepoint files are scanned for malicious content.

### **Cost-effective choice**

Offers a cost-effective choice for advanced security features such as sandboxing.

## Cloud deployment in just a few minutes

Leverages cloud-to-cloud integration that doesn't require any middleware or software to be installed and is extremely fast to deploy and easy manage.

## One integrated solution

Combined with WithSecure's endpoint protection and edr capabilities, the solution provides more comprehensive protection than any email security solution alone.

# WithSecure™ Security Cloud





Multi-engine antivirus



Smart cloud sandbox



WithSecure<sup>™</sup> Security Cloud is our cloud-based threat analysis and detection service. It utilizes real-time threat intelligence gathered 24/7 from tens of millions of security sensors across the globe. It forms the cornerstone of our award-winning\*, visionary products.



#### Threat intelligence check

By leveraging real-time threat intelligence gathered from tens of millions of sensors, we can identify new and emerging threats within minutes of inception, ensuring exceptional security against constantly evolving threats.



#### Multi-engine antivirus

When a file is unknown, WithSecure™ Security Cloud subjects it to deeper analysis. Multiple complementary behavioral and heuristic antimalware engines search for malware, zero-day exploits and patterns of advanced threats and targeted attacks.



#### **Smart cloud sandbox**

Suspicious files are subjected to further analysis in Smart Cloud Sandbox, which runs suspect files in several virtual environments and monitors behavior to detect malicious activity.

<sup>\*</sup>AV-Test & AV-Comparatives 2010-2019

# **End-user security**





#### Files & URLs

Malicious files and URLs are sent and received by M365 in various forms, such as emails, invites, notes and SharePoint uploads.



#### O365 exchange

WithSecure™ Elements for Microsoft 365 is connected and authorized to monitor all Exchange and SharePoint activity without hindering the use of email.



#### M365

The solution then subjects suspicious activity/content to a patented threat analysis and detection process supported by WithSecure™ Security Cloud.



#### Detect

Unsafe content is automatically deleted or quarantined, its further use is prevented, and users are told what to do next.

Detect compromised email accounts with comprehensive information about how, what, when and how severely.



#### Respond

Thanks to rich reporting, security analytics, and full audit trails, admins can respond to incidents efficiently.

#### Sandboxing

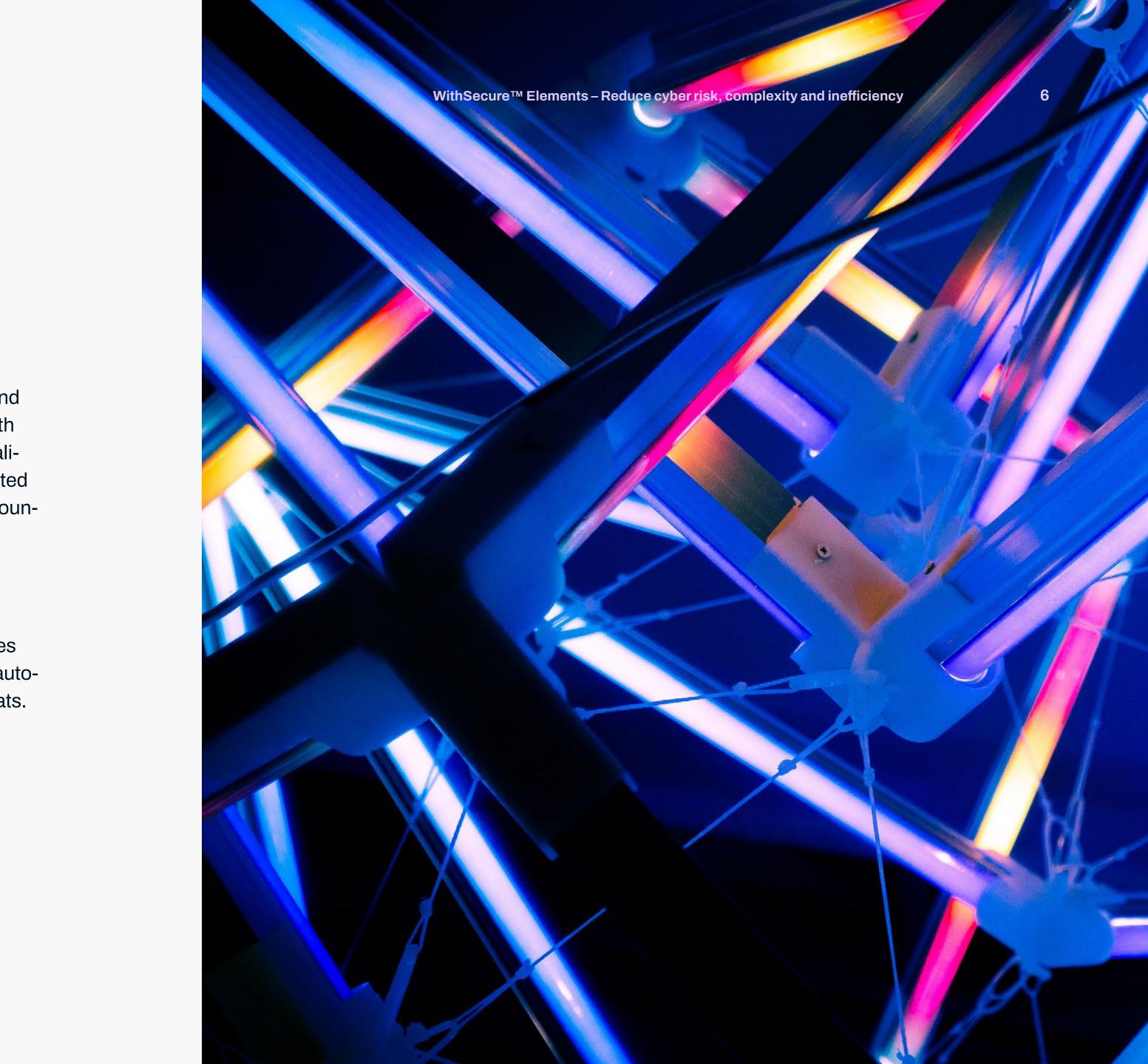
WithSecure™ Security Cloud employs multi-stage content analysis in a stepped process triggered by the risk profile of the content. Additionally, high-risk files are subjected to deeper analysis with our cloud sandboxing technology.

#### Global malware behavior tracking

Security products from WithSecure™ utilize reputation services for threat recognition. Client software calculates a cryptographic hash for an object and performs a network query with Security Cloud. This process provides us with a very granular picture of the worldwide distribution of software and how malicious programs spread. Security Cloud enables us to examine how suspected malicious programs behave globally and are spread between computers, countries, and continents.

#### **Automated analysis**

In order to keep up with today's rapidly changing threat landscape, automated processing and analysis of malware is required. This analysis feed enables Security Cloud to classify a significant amount of new malware quickly and automatically. This automation enables us to provide fast responses to new threats.

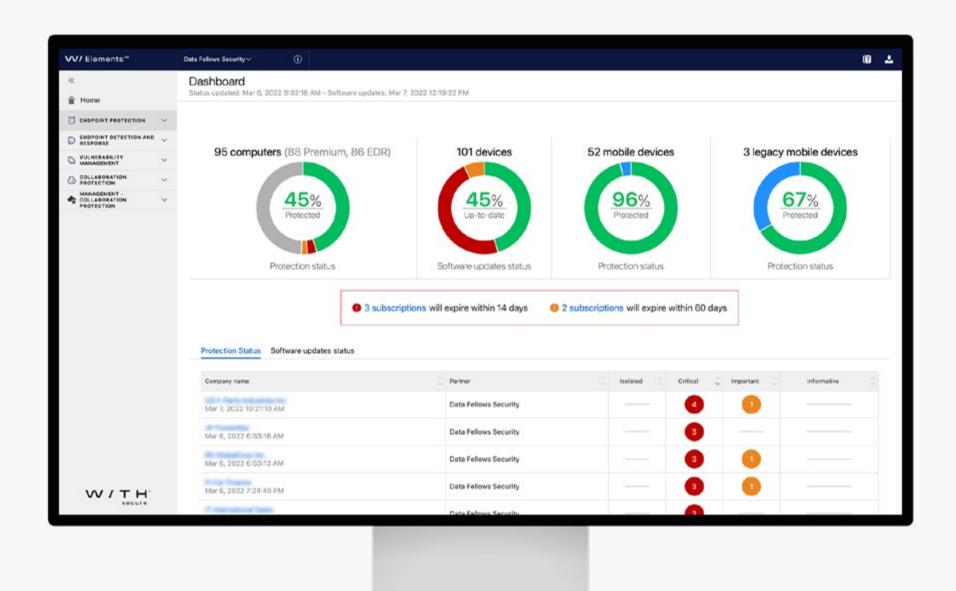


## Administration

WithSecure™ Elements for Collaboration protection gives full visibility to Collaboration protection usage.All security alerts for malicious or suspicious content found in in user mailboxes and Sharepoint folders are accessible on WithSecure™ Elements Security Center in a convenient table view. Elements Security Center provides a single pane of glass view into the unified platform. Information is presented clearly to give full situational awareness across security layers.

The quarantine view in the management portal allows administrators to view, release, or delete quarantined items as needed. The administrator can also use various sorting and searching criteria to fine-tune the view while handling the list of quarantined items for the managed environments.

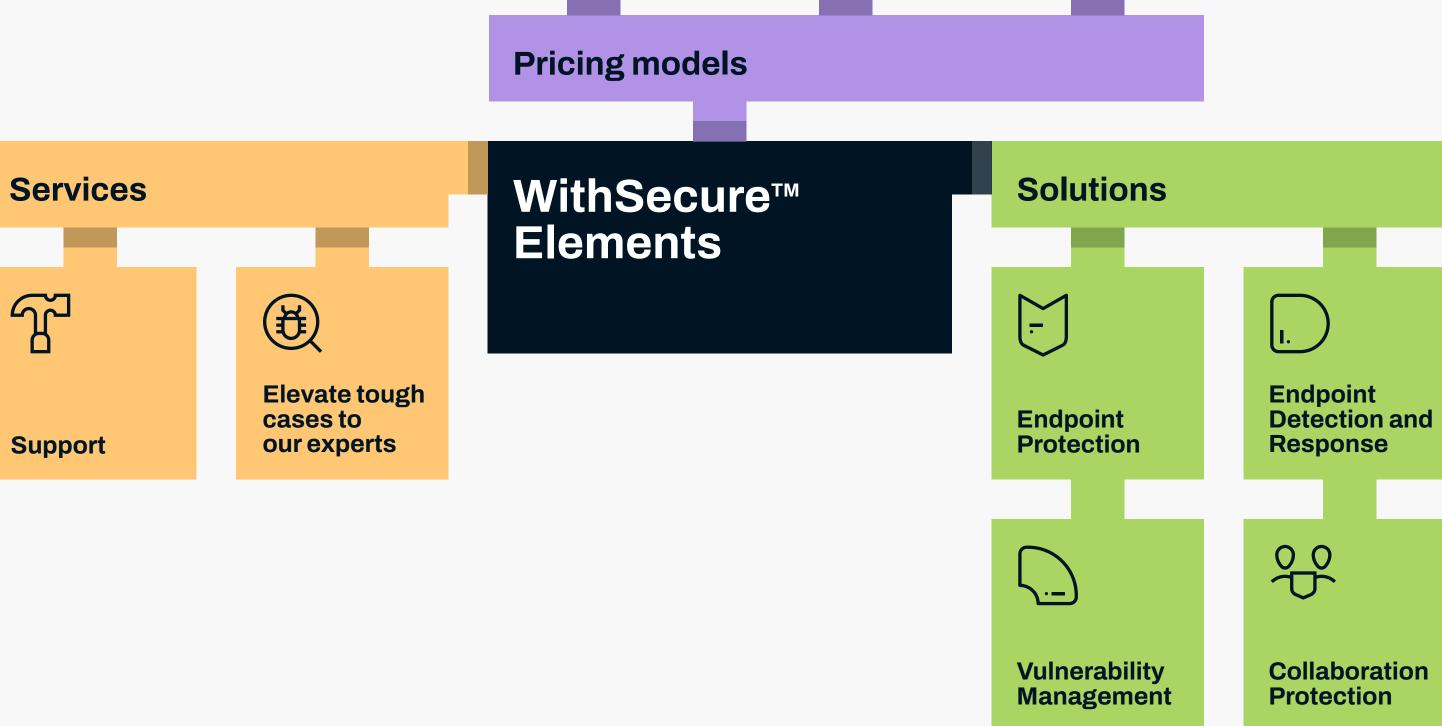
Rich reporting capabilities are available for administrators to report on the security status of the protected environment at any time in an easily sharable format.



# WithSecure™ Elements - Reduce cyber risk, complexity and inefficiency

WithSecure™ Elements for Collaboration protection is available as a standalone solution or as an integral capability in the modular WithSecure™ Elements cyber security platform.

Try it yourself today





# Who We Are

WithSecure<sup>TM</sup> 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 Aldriven protection secures endpoints and cloud collaboration, and our intelligent detection & response is 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<sup>™</sup> is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

