TRUST aWARE

Enhancing Digital Security, Privacy and TRUST in softWARE

Activity Monitor

WithSecure / Broderick Aquilino

March 27, Forum ABI Lab 2024 | 20th edition

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

WithSecure

- Who We Are
  - WithSecure is a European cyber security company serving the global B2B market. Our name isn't just a name. It's our promise. We will always be there for our partners—especially when it matters most
- Our Customers
  - Our customers include IT service providers, MSSPs and businesses, large financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers.
- Our Solutions
  - We offer a unified cloud-based cyber security platform, WithSecure Elements, that protects against Malware, Ransomware, Advanced Persistent Threats, and more. Our products and services include Endpoint Detection and Response, Exposure management, Collaboration protection, Cloud management, and more.
- Our History
  - While WithSecure as a company is relatively new, it was formerly the business unit of F-Secure. The two companies demerged in 2022 to put a higher strategic focus on serving the B2C and B2B markets separately.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

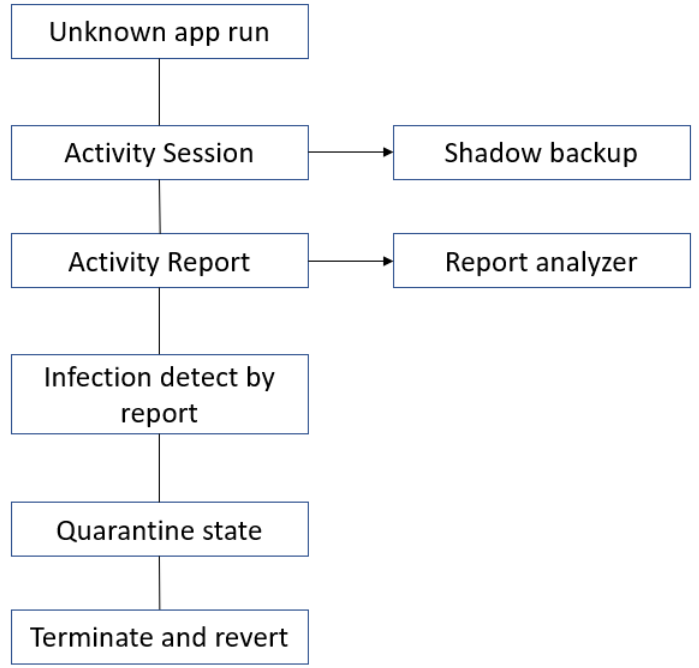
Activity Monitor – Positioning

- The Activity Monitor technology is being developed in Task 3.2 of TRUST aWARE: **“Dynamic attack detection”**
- It allows to detect and counter attacks that evade traditional anti-malware engines.
- Unlike many other endpoint detection and response (EDR) solutions, Activity Monitor does not need to send high volumes of data to security backend and does not require security expert supervision – so, very cost-efficient.
- Fighting ransomware is a major use case for Activity Monitor, so we selected it for this demo.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377

Activity Monitor – The approach

- Challenges: Threat actors implement very complex malware behavior which is hard to track with low noise. Early detection of malicious operations is difficult and often FP-prone, while late detection is … late (may result in irreversible damage).
- Activity Monitor by design: “System view" on an executed program. It follows the changes made by the program and all its "children" (through so-called Activity Sessions).
- Activity Monitor traces all relevant changes and creates shadow backups of file and system settings modifications.
- If the program behavior is recognized as malicious, the Activity Session terminates the malicious processes and reverts the changes to files, the Registry, and so on.



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377

Demo

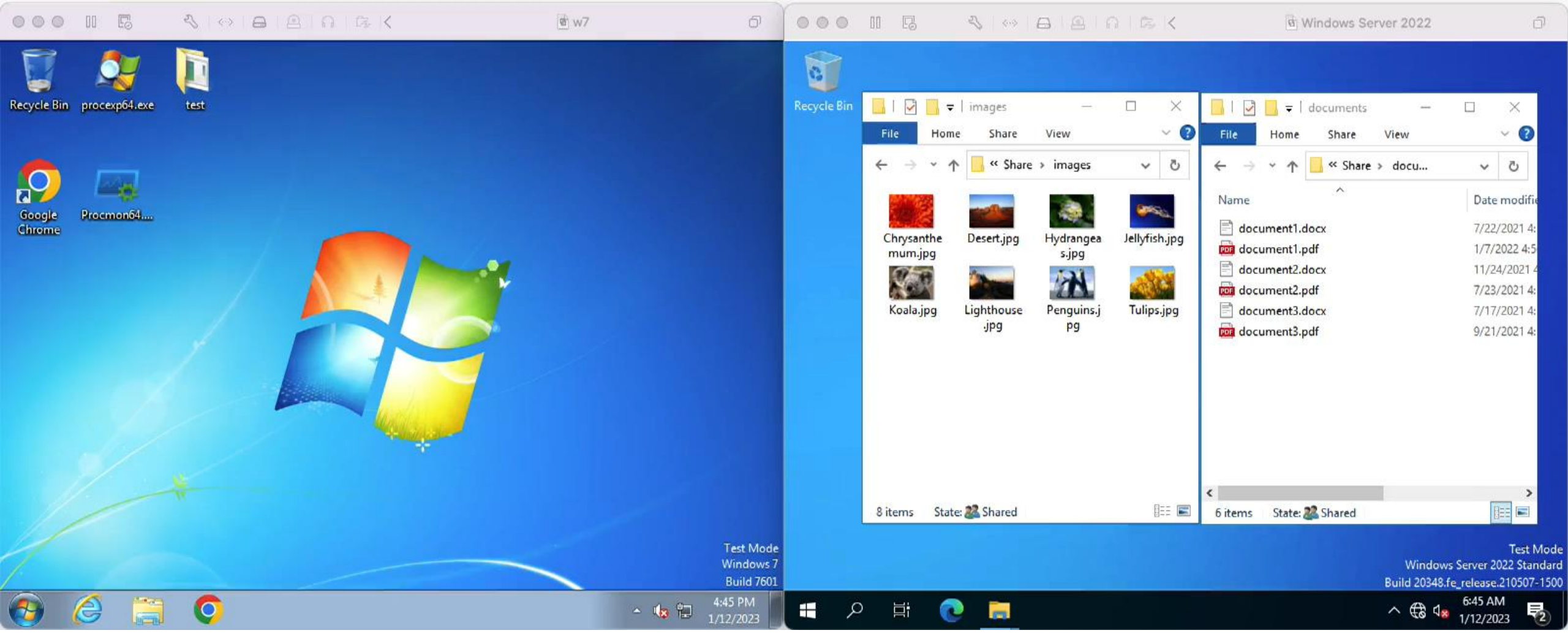
- Activity Monitor is now utilized by two critical features:
  - Server Share Protection - for file protection for shared folders use case
  - Rollback - for endpoint protection use case
- Both features are available to all WithSecure Elements EPP users but are not enabled by default at the moment.
- This is to enable us to carefully manage adoption rates, giving us the flexibility to identify and address any potential bugs or issues as they arise.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Server Share Protection demo

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

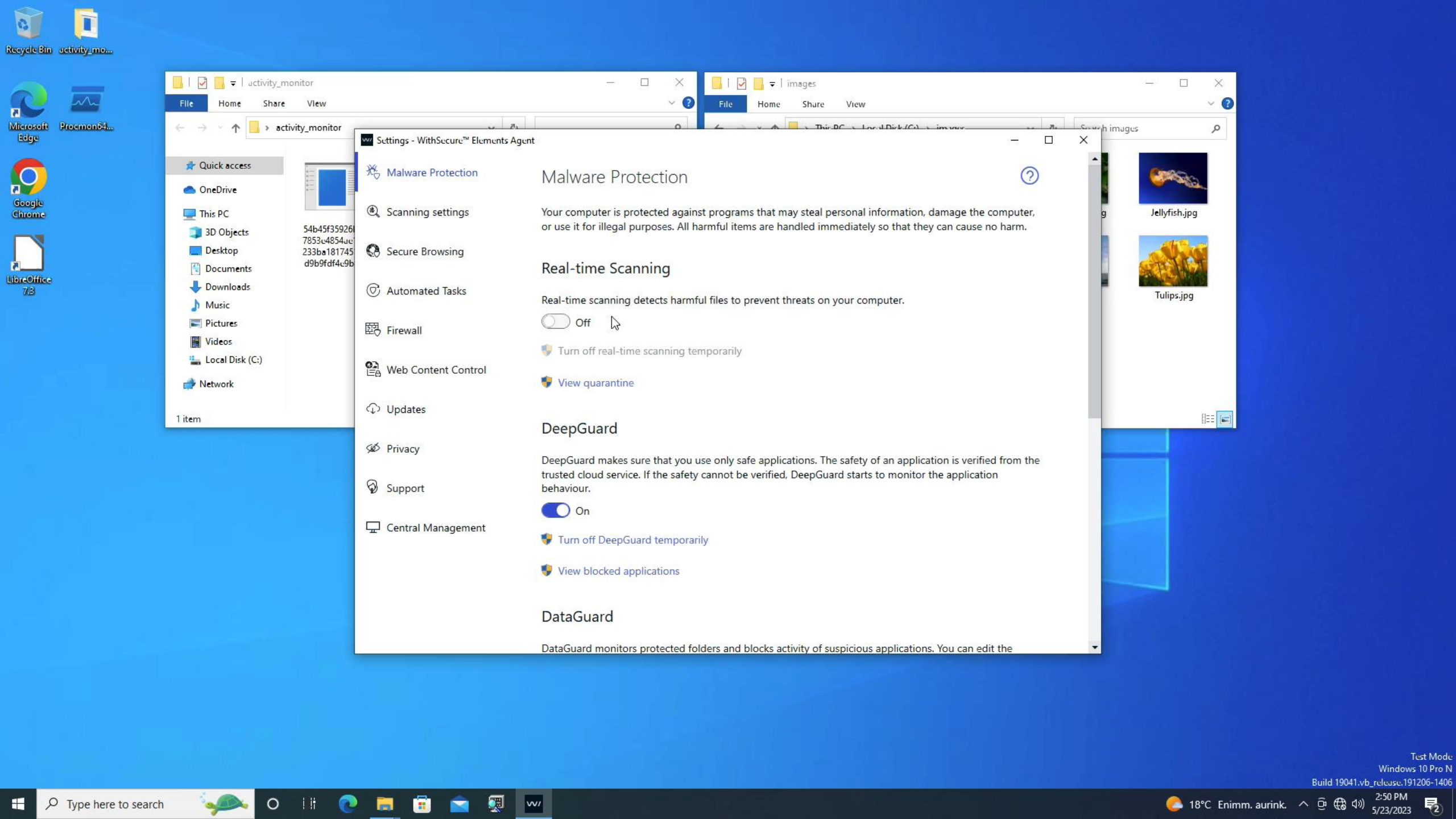
Server Share Protection demo



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Rollback demo

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377


Recycle Bin
uctivity_mo...
Microsoft Edge
Procmon64...
Google Chrome
LibreOffice 7.3
activity_monitor
File
Home
Share
View
Quick access
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
1 item
images
Jellyfish.jpg
Tulips.jpg
Settings - WithSecure™ Elements Agent
Malware Protection
Scanning settings
Secure Browsing
Automated Tasks
Firewall
Web Content Control
Updates
Privacy
Support
Central Management
Malware Protection
Your computer is protected against programs that may steal personal information, damage the computer, or use it for illegal purposes. All harmful items are handled immediately so that they can cause no harm.
Real-time Scanning
Real-time scanning detects harmful files to prevent threats on your computer.
Off
Turn off real-time scanning temporarily
View quarantine
DeepGuard
DeepGuard makes sure that you use only safe applications. The safety of an application is verified from the trusted cloud service. If the safety cannot be verified, DeepGuard starts to monitor the application behaviour.
On
Turn off DeepGuard temporarily
View blocked applications
DataGuard
DataGuard monitors protected folders and blocks activity of suspicious applications. You can edit the
Test Mode
Windows 10 Pro N
Build 19041.vb_release.191206-1406
Type here to search
18°C Enimm. aurink.
2:50 PM
5/23/2023

TRUST aWARE

Questions?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377