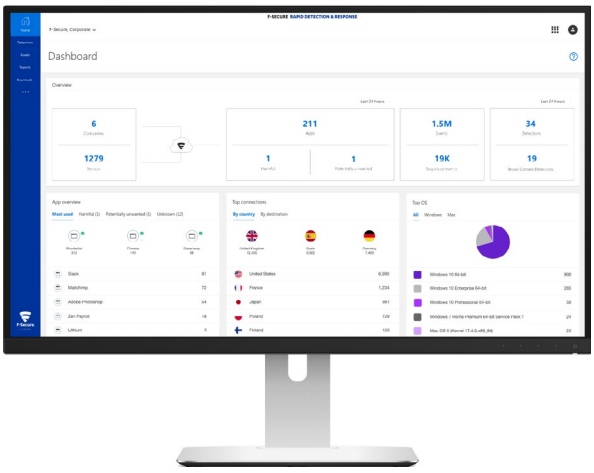
F-SECURE RAPID DETECTION & RESPONSE

Endpoint detection and response solution to stop targeted attacks with automation and guidance



KEY BENEFITS:

- **Gain immediate visibility** into potentially unwanted or harmful applications and cloud services
- **Identify automatically advanced threats** with risk levels and host criticality for easy prioritization
- **Visualize attacks in broader context** with all relevant detections and hosts on a timeline
- **Stop attacks fast** with built-in guidance or automated response actions based on predefined schedule
- **Resolve tough cases** with on-demand incident analysis and investigations by world-class threat hunters
- **Reduce management overhead** with cloud native and single-client endpoint security solution
- **Option to outsource advanced threat monitoring** to a certified managed service provider

Effective pre-compromise threat prevention is the cornerstone of cyber security, but you can't rely on preventive measures alone to keep your business and its data safe from the Tactics, Techniques and Procedures adversaries use in targeted attacks.

F-Secure Rapid Detection & Response is an industry-leading endpoint detection and response (EDR) solution that leverages the most advanced analytics and machine learning technologies to shield your organization against advanced cyber threats and breaches. With the solution's automatic advanced threat identification, contextual visibility into your security and built-in guidance with option to automate remote response actions, your team can detect and stop targeted attacks quickly and efficiently. The solution is managed either by your own IT team or a certified EDR service provider, and you are always backed by F-Secure's world-class threat hunters making even the toughest cases can be resolved.

F-Secure

HOW IT WORKS

Proactive visibility into your IT environment

Gaining extensive application visibility into your IT environment and cloud services will reduce exposure to advanced threats and data leakage. The EDR solution allows you to immediately list all active processes running on endpoints across your network to identify unwanted, unknown and harmful applications. You can easily restrict potentially harmful applications and cloud services, even before data breaches happen.

- Identifies all harmful or otherwise unwanted applications, and the foreign destinations of different cloud services
- Leverages F-Secure's reputational data to identify potentially harmful applications
- Restricts potentially harmful applications and cloud services even before data breaches happen

World-class threat hunters backing you up

Some detections require deeper threat analysis and guidance by specialized cyber security experts. For these tough cases, the solution has a unique built-in "Elevate to F-Secure" service. It offers professional incident analysis of methods and technologies, network routes, traffic origins, and timelines of a Broad Context Detection™ to provide expert advice and further response guidance whenever under attack.

- Built-in step-by-step response guidance and remote actions to stop attacks
- Certified managed service providers guide and support you through response actions
- Unique Elevate to F-Secure threat analysis and expert guidance service backs you up

Remote response actions with automation

Automated response actions can be used to reduce the impact of targeted cyber attacks by containing them around-the-clock whenever risk levels are high enough. The automation, based on predefined schedules, has been designed specifically to support teams only available during business hours, also taking the criticality of detections into account.

- Automated response actions based on criticality, risk levels and predefined schedule
- Criticality and risk levels provided by the solution allow prioritization of response actions
- Contain attacks quickly even if your team is only available during business hours

Single-client and cloud-based management

Lightweight, discreet monitoring tools designed for anomaly detection, deployable on all relevant Windows and macOS computers within your organization. The sensors are designed to work with any endpoint protection solution, and function with F-Secure's endpoint security solutions in a single-client and management infrastructure.

- Lightweight sensors are deployed on all relevant computers within your organization
- Single-client and management infrastructure with F-Secure's endpoint security solutions
- The sensors collect behavioral data from endpoint devices without compromising users' privacy

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure