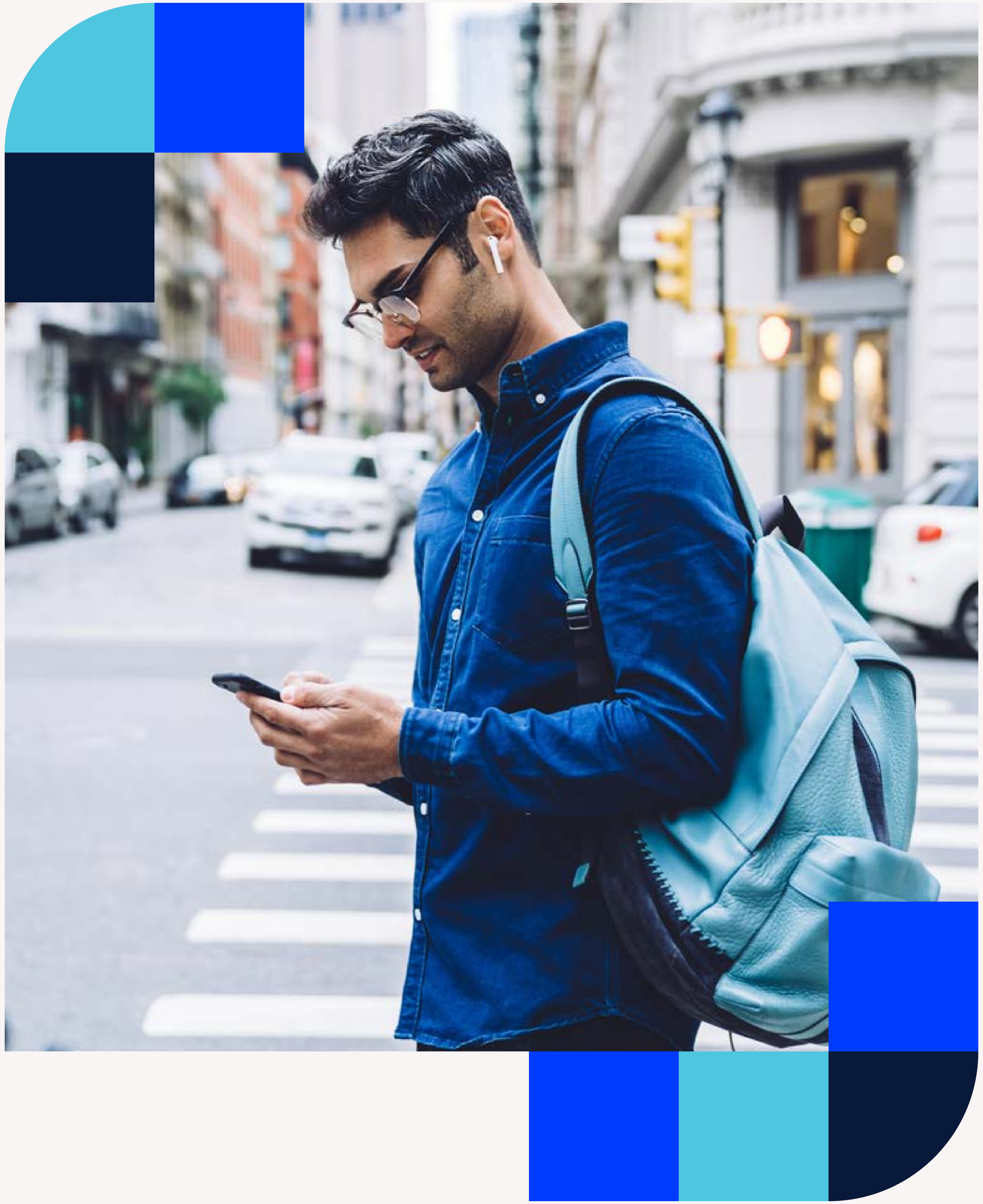
F-Secure®

# Artificial Intelligence at F-Secure

How we are using AI to protect digital moments



# Contents

1. Human intelligence finds a new challenger in AI
2. Sharks smell blood in the water - how cyber criminals are utilizing AI
3. AI is nothing new to the cyber security industry
4. How we use AI and Machine Learning at F-Secure
5. A new era for cyber security - how we plan to use AI going forward

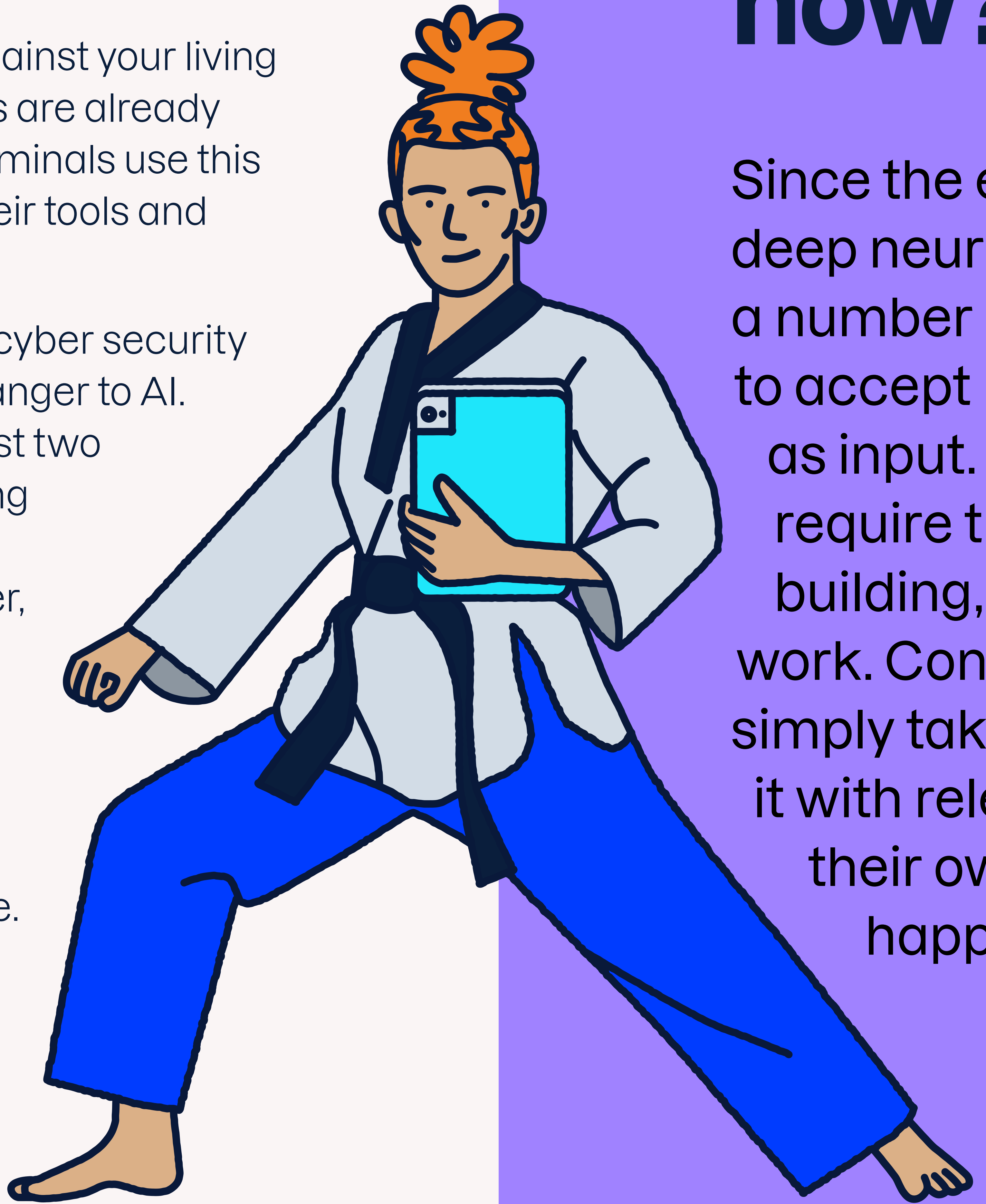
1

# Human intelligence finds a new challenger in AI

The advancements we're now seeing in Artificial Intelligence (AI) may be the biggest leap in technology since the introduction of the internet. Generative AI tools such as OpenAI's ChatGPT have gained a massive number of users in just a matter of months. And these users aren't just hardcore computer scientists – they're everyday people. What was once deemed distant science fiction only a couple of years ago is now available for virtually everyone, just a click away.

It's no secret that AI can support and enrich our daily lives in a multitude of ways – whether it's listing the implications of global warming for a school project or testing curtain colours against your living room décor. But concerns are already materializing as cyber criminals use this technology to sharpen their tools and practices.

As a truly consumer-first cyber security leader, F-Secure is no stranger to AI. In fact, we've spent the last two decades using this exciting technology to enrich our offering. In this whitepaper, we'll take you on the journey of how we're using AI to protect consumers' digital moments, and what we have in store for the future.



## AI has been around for years, what's changed now?

Since the early 2020s, advances in deep neural networks have enabled a number of generative AI systems to accept natural language prompts as input. Now, AI models no longer require thousands of hours of model building, training, or production to work. Consumers and companies can simply take a pre-built foundation, feed it with relevant data, and apply it for their own use. Further learning then happens by using the system itself.

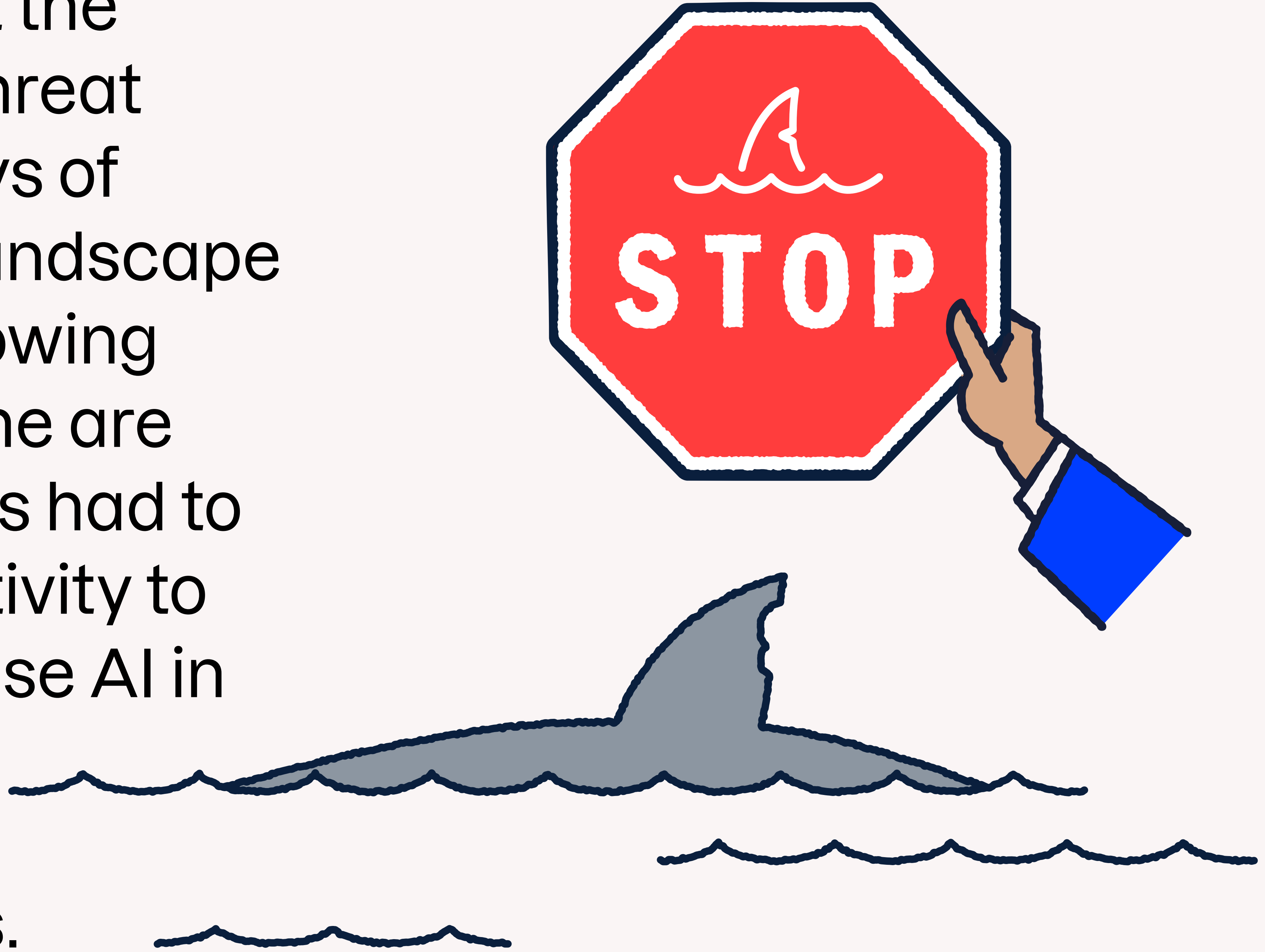
Laura Kankaala

Threat Intelligence Lead F-Secure

**"Cyber criminals will exploit AI the way they have the world wide web, email, mobile devices, and social media - that is in any way they can."**

# Sharks smell blood in the water - how cyber criminals are utilizing AI

We've spoken at length about the increasingly complex cyber threat landscape since the early days of computer viruses. Now, this landscape is expanding thanks to the growing use and capabilities of AI. Gone are the days when cyber criminals had to rely merely on their own creativity to craft attacks. Now, they can use AI in numerous ways to improve the effectiveness and sophistication of their exploits.

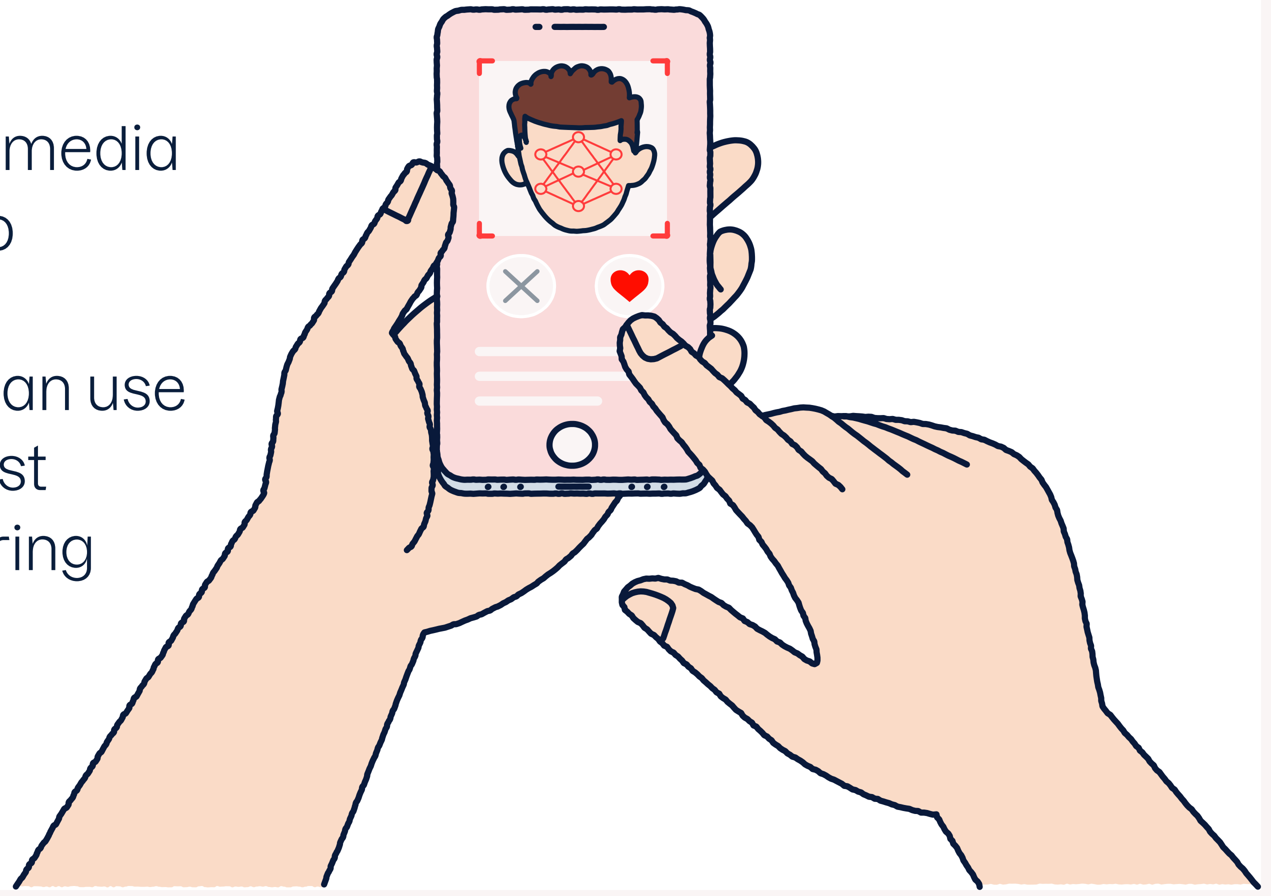


## Fraud and Scams

AI can be used to generate highly convincing fake identities, documents, and financial records to carry out fraud and scams. For example, criminals can use AI to craft convincing phishing emails or phone scams – and in more languages than ever before.

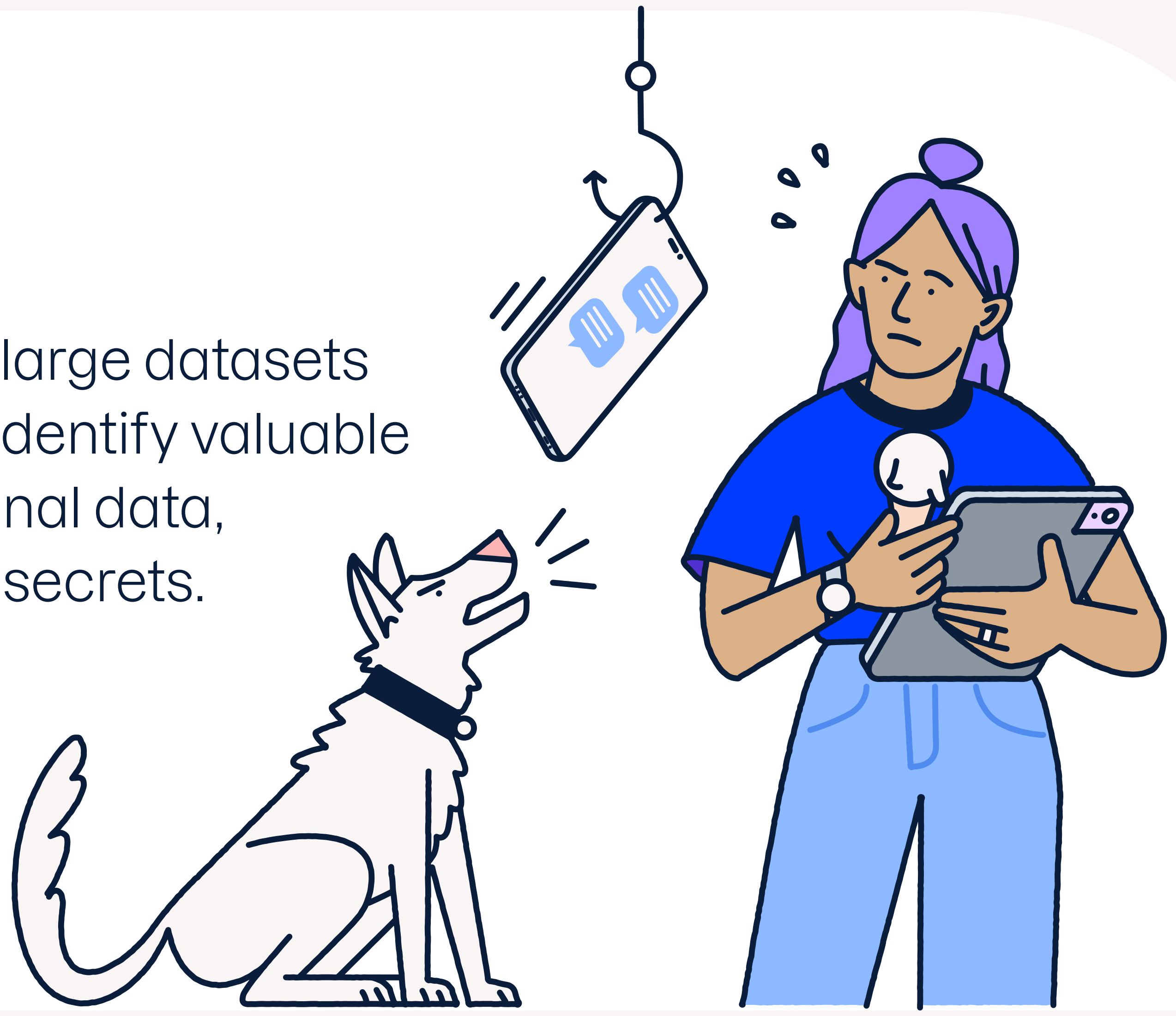
## Social Engineering

AI can be used to analyze social media profiles and public information to create more convincing social engineering attacks. Criminals can use AI-generated profiles to build trust and manipulate victims into sharing sensitive information.



## Data Theft

AI can be used to analyze large datasets quickly, helping criminals identify valuable information such as personal data, financial records, or trade secrets. This stolen data can then be sold on the dark web.



## Cyber Attacks and Hacking

Criminals can use AI to develop sophisticated malware that evades traditional cyber security measures. AI-powered tools can automate and optimize attacks, such as brute force attacks, phishing campaigns, and data breaches. AI is also used to enhance illegal activities on the dark web, optimizing drug distribution routes or evading law enforcement monitoring.

# AI is nothing new to the cyber security industry

Changes in both the threat landscape and consumer behavior are often a catalyst for wider technological advancement. And the rapid evolution of the threats we've faced over the past decade has meant the cyber security industry has had to remain at the forefront of this. Often, this has meant leveraging AI in various ways to enhance our ability to prevent, detect, and respond to these threats. Below are some key ways in which AI is utilized in cyber security:

## Malware Detection and Prevention

AI can analyze files and code to identify malware signatures and behaviors. This helps real-time detection and blocking of malicious software.

## Behavioral Analysis

AI can establish a baseline of normal behavior for users, systems, and networks. It can then detect deviations from this baseline, helping to identify potential insider threats, compromised accounts, or abnormal activities.

## Threat Detection and Analysis

AI-powered systems can analyze massive amounts of data to identify patterns and anomalies that might indicate a cyber attack. Machine Learning (ML) algorithms can learn from historical data and recognize new attack vectors, even those previously unseen.

# Why is AI so important to cyber security?

Cyber security is very data sensitive, and massive amounts of data samples need to be analyzed to identify malicious content from the non-malicious content. This goes far beyond what security analysts can handle manually, so this is where AI comes in.

## Anomaly Detection

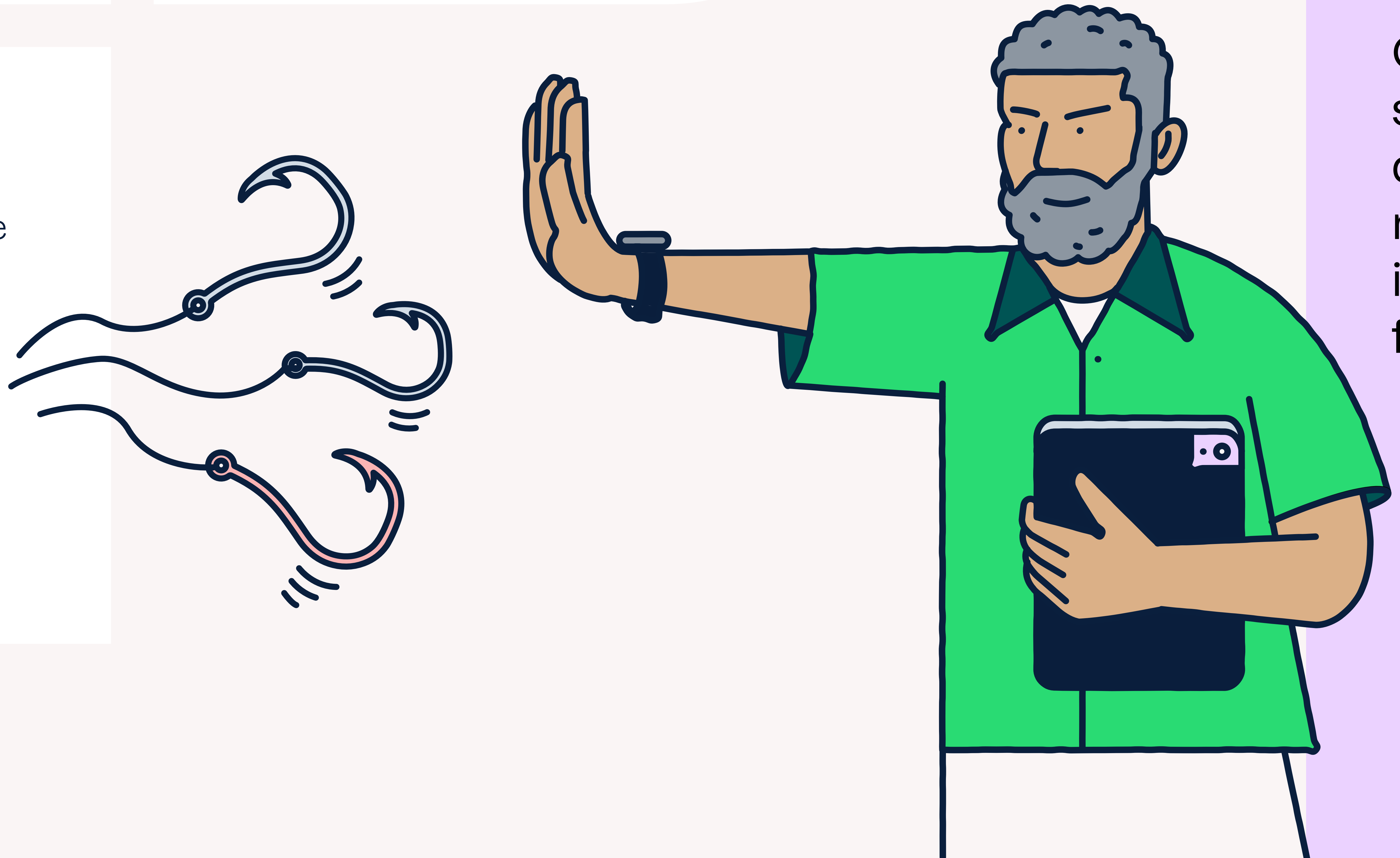
AI algorithms can identify unusual patterns or behaviors that might signify a breach or unauthorized access. This includes detecting abnormal network traffic, unusual login times, and unexpected file access.

## Predictive Analytics

AI can predict potential security breaches by analyzing historical data and identifying patterns that might lead to an attack. This allows organizations to proactively strengthen their defenses.

## Phishing Detection

AI-powered systems can analyze emails and messages to identify phishing attempts. They can do this by spotting patterns in content, sender behavior, and attachments that indicate malicious intent.



# How we use AI and Machine Learning at F-Secure

F-Secure has used AI and ML since the early 2000s. Initially these technologies were adopted to analyze massive amounts of files in our backend systems for better antivirus protection. Now, we use AI across the board to protect all areas of our customers' digital lives.

## Layered 'Kill-Chain' Protection

### What this is

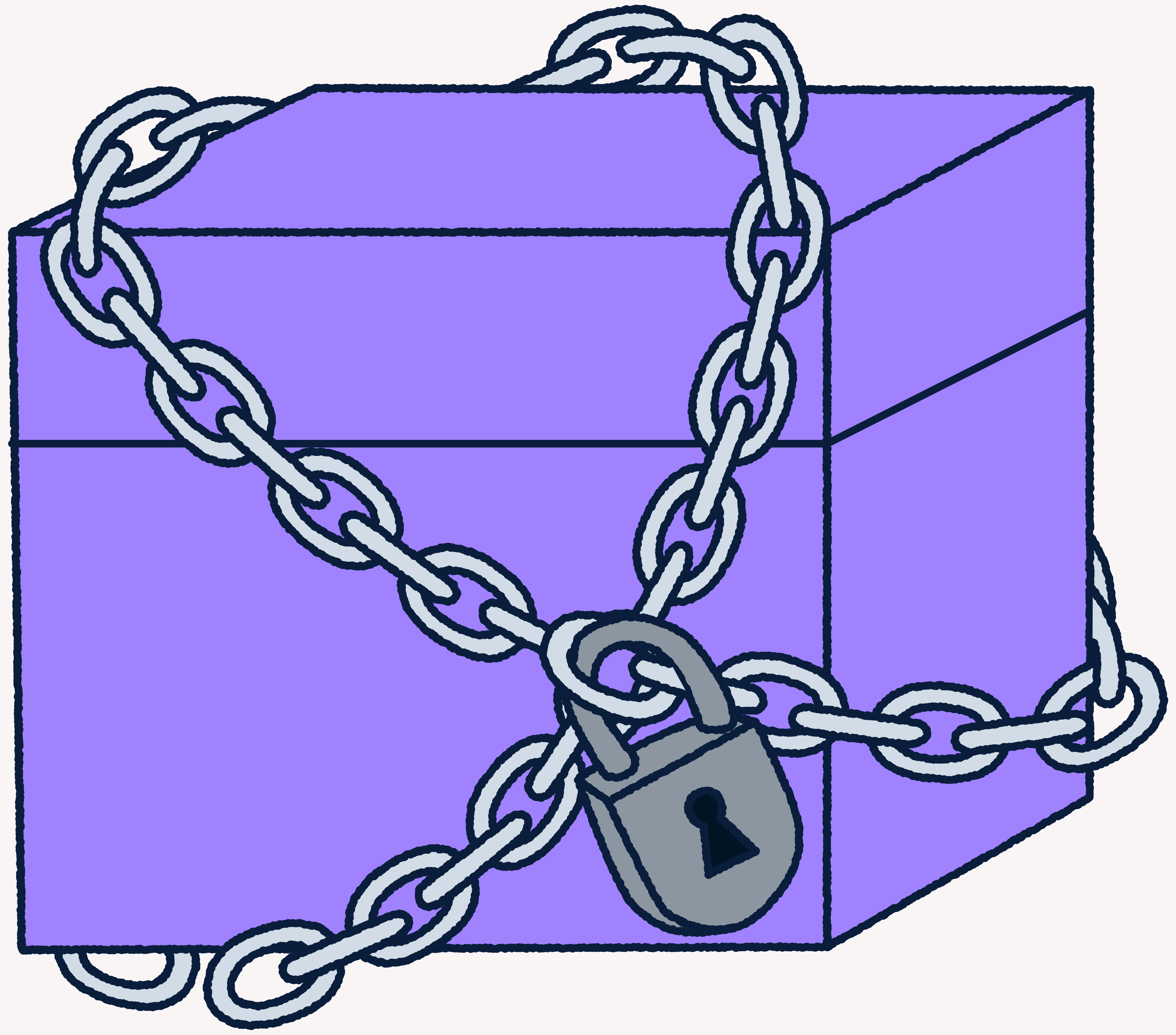
A combination of several protection technologies that communicate with each other and work in tandem to identify and block attacks. Kill-chain protection means multiple layers can block a threat or part of it, making it ineffective.

### How it works

Digital moments happen via devices and online services. However, these devices are not equal from a cyber security perspective. By using layered protection and kill-chain functionality, zero-day threats missed by traditional signature-based scans are blocked, because the best protection for our customers can only be reached by using multiple layers of protection. We also use data science techniques capable of selecting targets and would-be threats.

### The benefits

The benefits of each protection technology and each layer are cumulative. Ultimately, more layers mean more opportunities to identify and block the attacker.



| | | | |
|---|---|---|---|
| **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 behaviour |

- **Automated malware research**
- **Content classification**
- **Dataflow modelling**
- **Network behaviour research**
- **AI-built detection rules**
- **Machine learning models**

> **“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.”**
>
> **Mika Lehtinen, Director, Research collaboration, F-Secure**

# DeepGuard Behavioral Analysis

## What it is

F-Secure DeepGuard Behavioral Analysis is a host-based Intrusion Prevention System which performs file reputation analysis and behavioral analysis. It is responsible for the proactive, on-the-fly monitoring and interception of threats.

## How it works

This AI-enabled module has been embedded in F-Secure products since it was introduced in 2006. It bridges the gap between the time when a new malware is introduced in public and the moment when a dedicated malware detection has been added in the antivirus database. It also serves as the final and most critical line of defense against new threats in F-Secure products such as Total, even defending against those targeting previously unknown vulnerabilities.

## The benefits

By using DeepGuard, we significantly reduce time taken to analyze new and existing threats, keeping our customers protected and a step ahead of spotting and remediating emerging threats.

# Security Cloud Ecosystem

## What it is

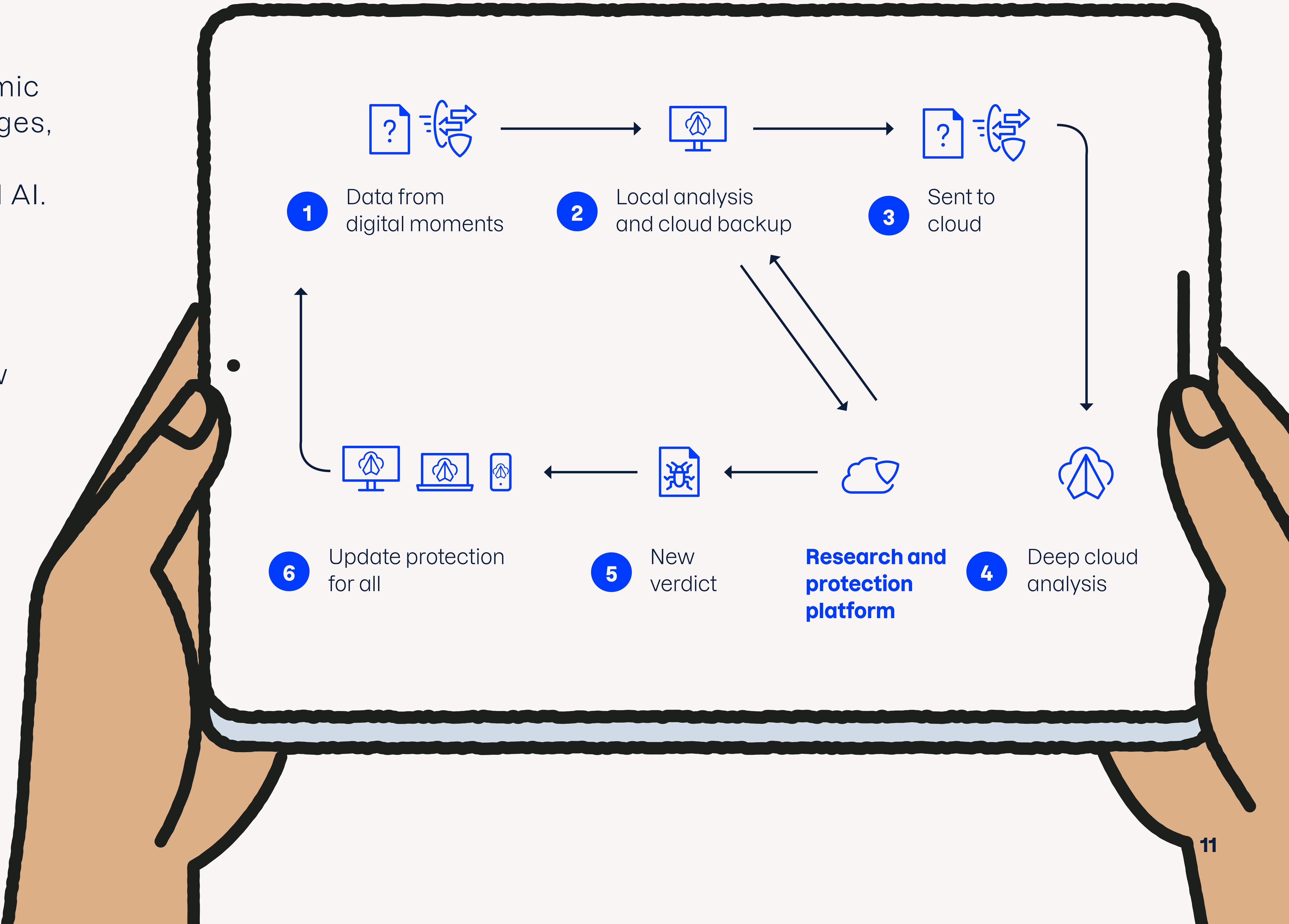
We analyze anonymous data from our users' digital moments using AI to improve our solutions long term.

## How it works

Our intelligence systems provide us with all kinds of threat-related objects. We analyze the objects individually and their relationships using many different techniques like reverse engineering, static and dynamic analysis around files, web pages, URLs, certificates, etc. This is executed both by experts and AI.

## The benefits

F-Secure can now create new verdicts based on the data at hand and share the updated protection among all users, improving the protection we offer consumers via our products overall.


1 Data from digital moments
2 Local analysis and cloud backup
3 Sent to cloud
4 Deep cloud analysis
Research and protection platform
5 New verdict
6 Update protection for all

5

# A new era for cyber security - how we plan to use AI going forward

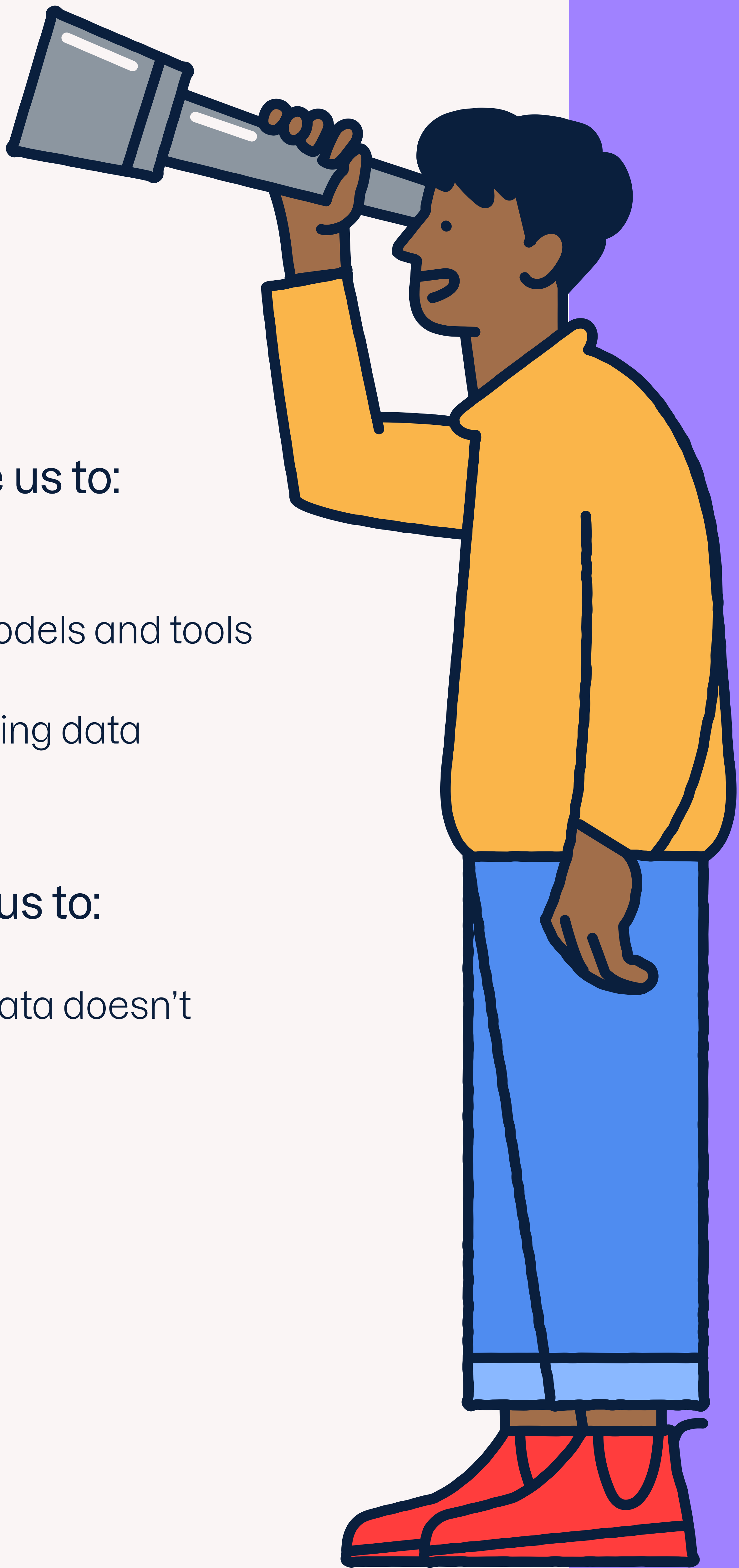
Like the rest of the world, we're excited about the recent development in AI technologies and generative AI tools. This enables us to improve how we protect our customers' digital lives, future-proofing the protection we offer. At F-Secure, we currently have many ongoing AI-related initiatives. Our short-term initiatives are either already under development or planned next development phases of existing features, while our long-term initiatives address AI more holistically.

In the short term, AI will enable us to:

- Improve our existing services
- Be faster to market with existing models and tools
- Process everything in the cloud
- Remain clear and strict on processing data privacy

In the long term, AI will enable us to:

- Ensure privacy-focused AI where data doesn't leave the device
- Explore generative AI solutions
- Combine device and cloud AI



## AI may not be the right tool for everything

At F-Secure we will always use AI with the goal of improving our customer and partner experience and protection. But it's important to remember that while AI is exciting, it may not be the right tool for everything, and we don't plan on using AI for AI's sake. Instead, we will always look to use the right resource for the task, whether that's AI, ML, or human expertise.

“The biggest advantage of AI is that it will make our products better and enable some completely new experiences that have not been discovered yet.”

Timo Salmi, Senior Product Marketing Manager, F-Secure

# Better overall protection

AI is already a great tool for analyzing security events and creating efficient protection measures. And its recent rapid development has opened new opportunities to protect customers more holistically with better accuracy by analyzing a wider variety of inputs and their relationships - even on the consumer’s device. In the short term, AI will enhance many protection capabilities, but it’s good to remember that the applications will be analyzed case-by-case.

# Better service experience

Today's consumer faces increasingly complex security threats, many of which they've never even heard of, and all the while the technological landscape develops around them at an alarming pace. At F-Secure, our ultimate vision is to become the #1 security experience company in the world. We understand that AI can be a fantastic tool for simplifying this complex world for our customers, helping them to protect their digital lives simply and effectively.

AI can help F-Secure customers to stay protected in the moment with context. For example, smart VPN will connect automatically when the customer needs protection, or when a malicious online service needs to be blocked. F-Secure will also be able to block harmful or malicious SMS messages using this context.

# Better online shopping protection

F-Secure Trusted Shopping feature (available as part of our Total solution) keeps consumer wallets safe by detecting the reliability of online stores while browsing the internet. This AI-enhanced feature uses real-time analysis of legitimate online shops, as well as fake and malicious sites. It automatically shows trust ratings for online stores in the internet search results list or when entering an online store page. Trusted Shopping is a reputation-based service similar to F-Secure Browsing Protection, enhanced with shopping threat intel.

# AI-powered smishing protection

According to F-Secure's consumer market research, SMS scam messages are the most prevalent form of cyber crime facing consumers. SMS Scam Protection is a new F-Secure Total feature that utilizes AI for analyzing received text messages. A new feature under the Scam Protection feature module, SMS Scam Protection safeguards consumer money and personal information against SMS-based fraud and scams. It also checks potentially risky incoming messages using AI to filter out dangerous messages.

# Protecting the entire connected home with F-Secure Sense

At F-Secure, we take a comprehensive approach to protecting consumer digital moments. So, F-Secure Total isn't the only product to utilize AI and ML. F-Secure Sense is an embedded software application for the consumer's Wi-Fi router/home gateway that protects every single connected device in the home against cyber threats. We are currently conducting research to harness the power of F-Secure Sense and the way it communicates with IoT devices. This will help us to form an understanding of what the 'normal behavior' of IoT devices is and gain an aggregate view of expected internet communications patterns of smart devices.

As well as AI, F-Secure Sense uses ML to detect anomalies. Instead of processing URLs, F-Secure Sense works by looking at communication patterns. Using these insights, we can observe and monitor behavior and patterns easily. If the device behaves significantly out of the 'normal range' we act quickly. While we're already utilizing AI and the recent advancements in the field to maximize the protection of the connected home through F-Secure Sense, we are excited for what the future brings in terms of product development and enhanced protection.

# Want to find out more about how F-Secure is using AI to protect digital moments?

Contact us now

# About us

F-Secure makes every digital moment more secure, for everyone. We deliver brilliantly simple, frictionless security experiences that make life easier for the tens of millions of people we protect and our 200 partners.

For more than 30 years, we've led the cyber security industry, inspired by a pioneering spirit born out of a shared commitment to do better by working together.

For more information visit F-Secure today.

F-Secure®