
EFFECTIVE DETECTION
AND RESPONSE
IN A CLOUD
SERVICE WORLD
F-Secure

WHY CLOUD?

200 years ago, every factory had its own power source: a steam engine or a waterwheel, yet few businesses today; generate their own power they buy electricity, instead. In the world of IT (Information Technology), cloud services are having a similarly disruptive effect.

The benefits of cloud computing are clear: more flexibility; no capex; and no need to attract and retain those scarce IT skills. Over 90% of organisations have a strategy using cloud services and most likely, the other 10% are using them without knowing it.

Many have also realized that they'll only see the full benefits of cloud computing if they fully immerse themselves – this is driving a shift towards cloud-native architectures rather than 'lift-and-shift' of infrastructure from on-premises data centers to the cloud.

HARNESSING CLOUD BENEFITS

In the commercial world, we tend to believe that generating profits is our principal mission, with survival and risk control something to perhaps consider, but are we missing the strong logical precedence of survival over success? To make profits and buy that jet ski, it would be a good idea to first, survive.

How can businesses embrace the benefits of cloud computing without taking excessive risk?

This document gives security leaders a summary of how cloud adoption is changing the challenge of defending against cyber-attacks.

CLOUD SECURITY CHALLENGES

Cloud adoption brings new security challenges because cloud services are:

- **New:** attackers and defenders are learning how to bend the cloud to meet their ends. How do you defend workloads when there's no Operating System to install a monitoring agent into? How do you detect attacks when you have to predict how attackers will evolve their methods?

- **Networked:** cloud-based computing is inherently networked, and those networks are larger, more complex and harder to defend. How do you secure an environment that's accessible over the public internet? How do you protect your cloud environment, on-premises environment and user endpoints all at the same time?

- **Shared:** responsibility for IT security in the cloud is shared between customers and cloud service providers (CSPs) giving rise to error. In the cloud, you need only get a few things right to have a proficient level of security. Conversely, you need to only misconfigure a few things to expose your network to the internet. A quarter of the largest cloud service incidents in the last decade have been due to user misconfigurations. Gartner claims that "Through 2025, at least 99% of cloud security failures will be the customer's fault".

Meeting these challenges

Legacy IT will be here for a long time and will need monitoring to detect direct attacks on on-premises IT with the aim of compromising either on-premises IT, or the cloud services consumed by users; and attacks on endpoints used to access either on-premises IT or cloud services.

Protecting on premises and cloud environments involves many of the same skills, but like freshwater and ocean sailing, there are differences. Ocean sailors need to think about tides, currents, waves, navigation, and salt water corrosion. Freshwater sailors need to think about paddle boarders, underwater obstacles and proximity to other vessels.

A mindset shift is needed for attack detection in the cloud: away from known malicious behavior, and towards finding abuse of legitimate functionality. Threat hunting will be especially important as attackers will be looking for new ways to attack. Organizations running multi-cloud environments also need a consolidated view of their risk.

Meeting these challenges requires a 24x7 solution that combines excellent cloud expertise and threat intelligence, with a deep understanding of how to detect and respond to attacks at enterprise scale. F-Secure Countercept is our solution.

Cloud service users will work with service providers for the reasons they do today: difficulty in attracting and retaining skills; and running a 24x7 operation. Gartner predicts that by 2025, 50% of companies will have adopted MDR services to avoid competency and resource development challenges.

F-Secure Countercept is a Managed Detection and Response (MDR) service built by attackers for defenders, delivered in partnership with clients' IT Security teams, by threat hunters who form a 'battle-fit' Detection and Response Team (DRT). Our vision is that no F-Secure customer should suffer a major business impact from a cyber-attack. Countercept has a proud history of fulfilling this vision and defending its customers from the most sophisticated on-premises attacks, but we recognize that we must continually evolve our MDR solution.

Countercept for cloud

Countercept's evolution is driven by four key insights about security when running so-called hybrid cloud environments, where on-premises and cloud IT are used at the same time:

1. **Cloud configuration -** The cloud's extreme flexibility and public nature mean that secure configuration is more important than ever – many cloud breaches today are the result of simple misconfiguration rather than attacker sophistication.

2. **Identity-based detection -** The adoption of cloud-native Platform-as-a-Service features and improving endpoint security are driving a shift towards identity-based attacks, so User and Entity Behavior Analytics (UEBA) – profiling user behavior and finding suspicious anomalies – is the foundation of a hybrid-cloud monitoring solution.

3. **Endpoint Detection and Response (EDR) -** Not only can workloads run in virtual machines, containers and serverless functions can be directly attacked, they can be attacked via endpoint devices, so EDR is needed on top of identity-based detection.

4. **Unified solution -** Attackers often target endpoints or on-premises systems to get to the cloud, so separate security solutions won't do – a unified solution to defend the whole organization is needed.

Countercept for cloud

Countercept's security platform defends hybrid cloud environments by combining proprietary F-Secure technology with key data sources and integration points, including:

- Operating system authentication logs
- Cloud control plane logs and management APIs (Application Programming Interfaces)
- Identity and Access Management (IAM)
- Cloud Access Security Brokers (CASB)
- Mobile Device Management (MDM)
- Software as a Service (SaaS) applications
- Continuous Integration / Continuous Deployment (CI/CD) systems.

COUNTERCEPT ROADMAP

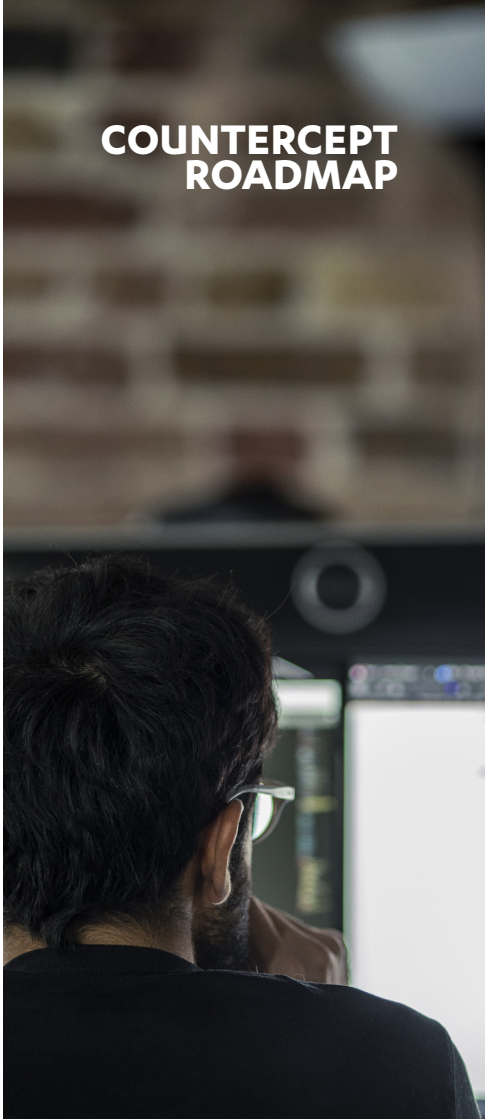
Existing capabilities are shown in bold and under-development capabilities in italics.

	Peacetime Value	UEBA	Attack Detection	Response
Cloud	**Cloud Security Posture Managements**	*Cloud Control Plane* *IAM, CASB and MDM* **SaaS Applications** *CI/CD Systems*	*Container Detection* *Container Orchestration* *Serverless Applications*	*Cloud API Integrations* *IAM Integrations* *CASB Integrations*
Endpoints / On-Premise	**Security Insights** **Threat Intelligence**	**OS Authentication Logs**	**EDR**	**EDR**

Peacetime value

Peacetime Value describes how Countercept delivers value even when there's no attack going on, by helping customers continuously improve their security posture.

- Security Insights uses data gathered for threat detection to also highlight elements of weak security posture such as insecure protocol usage, or excessive assignment of administrative privileges.
- Cloud Security Posture Management uses scanning technology developed by F-Secure to find cloud security risks introduced by misconfiguration, such as missing encryption or storage inadvertently exposed to the internet.



User and Entity Behavior Analytics

User and Entity Behavior Analytics (UEBA) highlights credential misuse through a unified risk score for users across all on-premises and cloud environments. The risk score is calculated from:

- Operating System Authentications (Active Directory).
- Cloud Control Plane activity (Amazon Web Services, CloudTrail and Azure Activity Logs).
- Logs from critical SaaS applications such as Microsoft 365.
- Logs from other key technologies that enable cloud usage, such as IAM and CASB.

Attack detection

Countercept uses F-Secure's market-leading Endpoint Detection and Response (EDR) for Attack Detection on user endpoints and servers on-premises or in the cloud, complemented by specialized detection capabilities for:

- Containerized applications and container orchestration systems such as Kubernetes that are running on self-managed hosts. This detection is provided through a combination of Linux EDR and proprietary analysis of Docker and Kubernetes logs.
- Containerized applications running in managed cloud services such as Amazon's Elastic Container Service (ECS). This detection is provided through proprietary analysis of Docker logs.
- Container orchestration systems running in managed cloud services such as Amazon's Elastic Kubernetes Services (EKS). This detection is provided through proprietary analysis of Kubernetes logs.

Response

Countercept's Response capabilities supply full remediation of cyber-attacks, rather than just giving customers unwelcome news. This includes:

- EDR-based response on Windows, Linux and macOS endpoints, covering termination, containment, blocking and removal of malicious activity and artefacts.
- Cloud API-based response to gather artefacts for investigation and revoke attackers' privileges in cloud environments.
- API (Application Programming Interface) integrations with key cloud technologies to disrupt attackers, for example using an IAM API to force a multi-factor authentication prompt for a user whose credentials are suspected to be compromised, based on UEBA.

THE RESULT

The combination of Countercept's purpose-built technology platform and hard-won expertise gives customers a solution to the security challenges that come with running a hybrid cloud environment.

Countercept drives continuous improvement of security posture, deterring attackers and minimizing their chances of success, combined with comprehensive monitoring and response capabilities which quickly detect and contain any attacks which do slip through the first line of defense. It doesn't matter whether attackers abuse leaked credentials, target the cloud directly or try to use the on-premises environment as an entry point – the Countercept team is watching.

WHY F-SECURE?

Cloud security is still an emerging field. Attackers are guaranteed to evolve and develop new approaches. Trying to predict exactly what will happen next is a fool's errand, but F-Secure has the platform and the expertise to keep pace with attackers and maintain our position as a provider of truly effective security solutions. We will always be at the forefront of threat intelligence and security research, and as a heavy user of cloud services ourselves, we understand the journey that many organisations are on and the challenges that come with this new way of working.

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

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

F-Secure