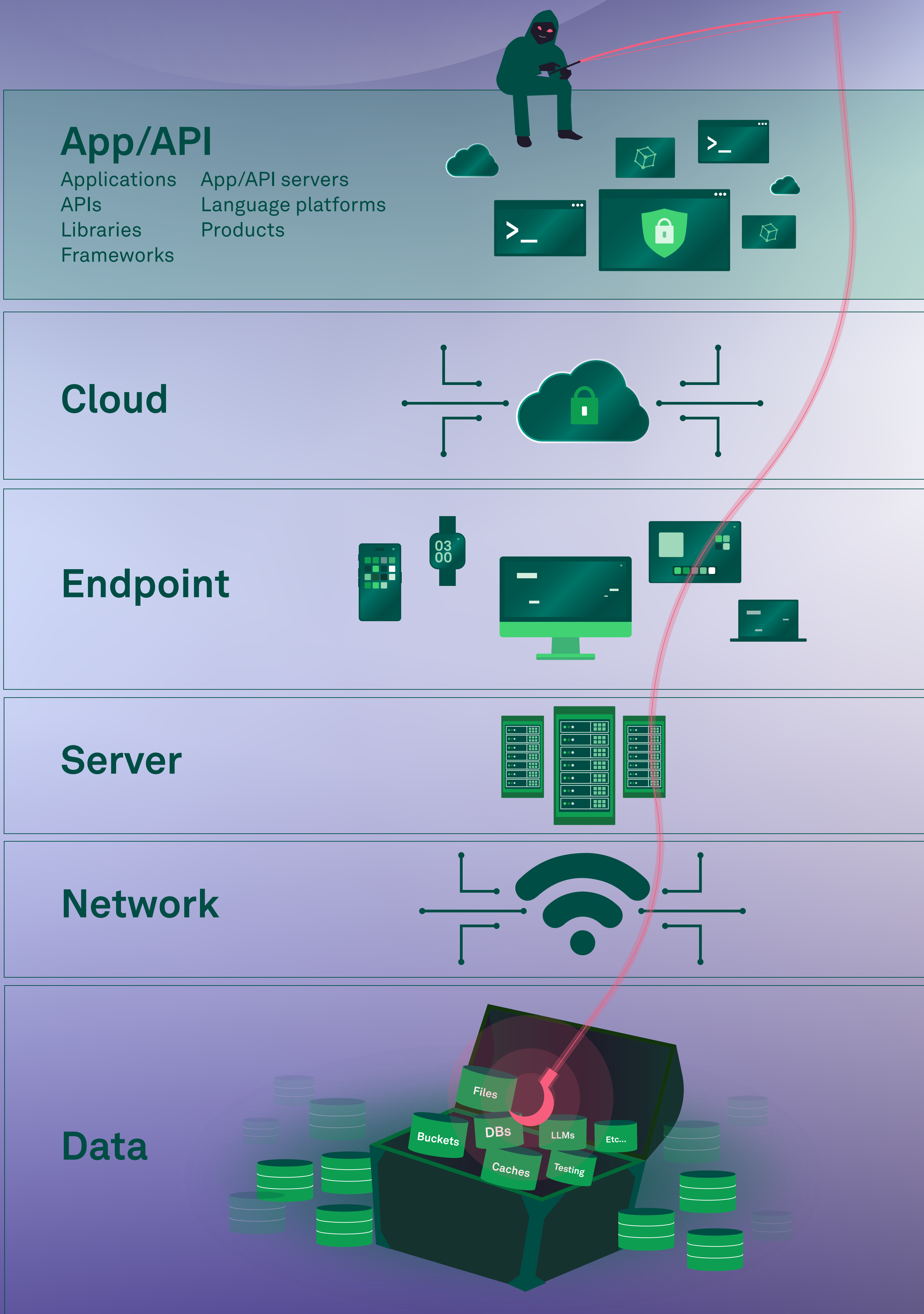# Application Detection and Response (ADR): Helping SecOps teams address NIST CSF

The security operations center (SOC) requires the right combination of people, processes and technology to protect the organization's assets.

Most SOCs lack visibility into the application and application programming interface (API) layer.

Threat actors inside the application and API layer can bypass other controls, get access to vulnerable data and launch devastating attacks.

App/API
Applications   App/API servers
APIs   Language platforms
Libraries   Products
Frameworks

Cloud

Endpoint

Server

Network

Data

Files   Buckets   DBs   LLMs   Etc.   Caches   Testing

How the SOC can stop application layer attacks

The Cybersecurity Framework (CSF) from the National Institute of Standards and Technology (NIST) is designed to help organizations better understand and more effectively manage their cybersecurity risk. As such, it's particularly useful to SecOps — especially at the application layer.

NIST CSF core function	Current SOC activities	How Application Detection and Response (ADR) can help
Govern	Compliance management, policy enforcement	ADR automatically generates detailed, real-time security blueprints of every application and API, including how they connect with each other. These blueprints help teams ensure compliance with regulatory requirements and enable effective security governance across the organization.
Identify	Threat and vulnerability management and Red Team activities	ADR extends visibility to the application and API layer, providing detailed context of anomalous behavior throughout the entire software stack.
Protect	Security tooling validations	Identifies anomalies that indicate security incidents.
Detect	Security monitoring, shadow IT monitoring, data loss prevention	With ADR, analysts can track lateral movement from its point of origin — in applications and APIs — and stop the incursion before it becomes persistent.
Respond	Incident response and investigation, digital forensics	Automatically takes action to mitigate threat and/or provides information so the incident response team can do it.

Learn more about Contrast Security