

# CLOUD SECURITY TOOLING STARTER PACK

v1.0 2023.11.08.

## AV to EDR/CNEP

Traditional AV used signatures; EDR uses behavior detection; CNEP adapts EDR for cloud environments

## WAF to CNAPP

WAFs protect web apps at the HTTP level; CNAPP evolved to provide a holistic security posture in the entire cloud-native application lifecycle, including development, deployment, and runtime

**Firewalls to SASE** Firewalls manage network traffic rules; Network Security in SASE provides comprehensive network control and security in the cloud

## SIEM to XDR

SIEM aggregates logs for analysis; XDR extends this by integrating more data sources for threat detection and response across systems

## Rise of SOAR

SOAR automates and orchestrates responses to security alerts, integrating with other tools

