The Evolution of **Modern Cloud Security**

sysdig SECURE EVERY SECOND.

Remember asking your teachers why you needed to know history? They probably said that learning history is important in understanding how society has changed and progressed over time, and that we can learn from past experiences and mistakes.

That's all equally true when it comes to the history of security. How did we evolve to the modern state of cybersecurity, and what does that tell us about the best path to take going forward?

Before Cloud Computing

To understand what's happening in the cloud, we first need a refresher on the evolution of endpoint security.

late 1900s - early 2000s

The first computer viruses

As internet use skyrocketed in the late 90s and early 2000s, viruses like the ILOVEYOU worm and the Anna Kournikova virus began spreading across the globe.

late 1900s - early 2000s

Antivirus software

The first antivirus software (e.g., Anti-Virus eXpert, ClamAV) sprang up, using signature-based methods to shield systems against a database of known viruses.

late 1900s - early 2000s

Polymorphic malware

The rise of polymorphic malware, which could change its code to evade detection, rendered signature-based protection increasingly ineffective.

Mid 2000s - 2010s

Next-generation antivirus (NGAV)

To combat polymorphic threats, NGAV solutions moved beyond simple signatures, incorporating advanced techniques like machine learning and behavior analysis.

⚠ Too many threats

Attacks continued to succeed, and once inside a network, there was no way to detect them.

2013

Endpoint detection and response (EDR)

EDR introduced capabilities for monitoring, detecting, and responding to threats in real time, complementing the NGAV protective measures.

•••

For a time, it seemed all we would have to do was continue improving our EDR and endpoint solutions, and we'd all be safe from cyber attacks.

Along Came the **Cloud**

The cloud is an entirely different type of attack surface — one that is orders of magnitude larger and faster-moving. As business migrated to the cloud, it became clear that traditional security wasn't going to cut it. So we started replacing our on-prem security tools with cloud equivalents

2010

Cloud workload protection platforms (CWPP)

Tools to secure workloads and containers in the cloud

2014

Cloud security posture management (CSPM)

A set of tools that help detect and remediate misconfigurations and posture drift

2020

Cloud infrastructure entitlement management (CIEM)

Software that helps find and fix over-permissioned or unused accounts, roles, and permissions

⚠ But there's still too many threats

Just like we needed EDR to protect our systems against attacks that breached preventative controls of on-prem systems, we now need software purpose-built to do the same for the cloud.

Let's learn from the past, and use CDR to make our future more secure.

Find out more in the full Evolution of Cloud Security ebook

READ NOW →

2017

Cloud Detection and Response (CDR)

Where legacy EDR and XDR tools are fundamentally unsuited for the cloud, a good CDR solution can detect known and unknown threats across your cloud estate in real time, accelerate investigations, and automate threat response.

sysdig

INFOGRAPHIC

ING-012 REV. A 12/24

About Sysdig

In the cloud, every second counts. Sysdig stops cloud attacks in real time by instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across workloads, identities, and services to uncover hidden attack paths and prioritize the risks that matter most.

REQUEST A DEMO →