VECTRA®
SECURITY THAT THINKS

EDUCATION GUIDE

Cloud Security Challenges

VECTRA
SECURITY THAT THINKS

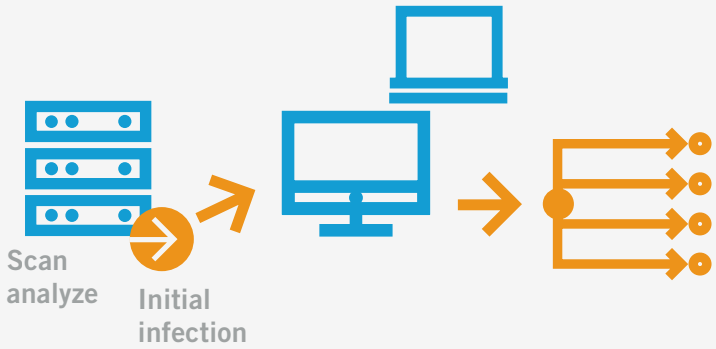
Adapting to changes in securing the cloud

The need for speed and agility in today's always-on, always-connected digital business has led IT teams to transform the traditional on-premises infrastructure to cloud-native architectures. The rise of DevOps and the use of Platform as a Service (PaaS) & Infrastructure as a Service (IaaS) have been foundational to this change and is now the norm. But where security traditionally fell on dedicated teams, it now often falls on the developers themselves, and as a result, when speed and agility increase, so does the risk of introducing security issues.

Cyberattack lifecycle

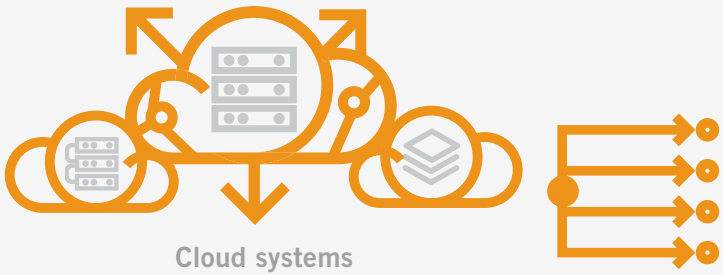
At first glance, the attack lifecycle in cloud seems similar to the traditional network; however, as we examine them closer, there are some key differences that change the way security needs to be considered.

Network



- Initial infection
- Command and control
- Internal reconnaissance
- Lateral movement
- Data exfiltration

Cloud



- Compromise user credentials
- Account creation/ manipulation
- Privilege escalation
- Lateral movement
- Data exfiltration

VECTRA
SECURITY THAT THINKS

What are the different types of cloud deployments and their security challenges?

IaaS
Infrastructure as a Service

Moving existing applications from private data centers to Cloud Service Providers (CSPs) (i.e. Amazon Web Services, Microsoft Azure, and Google Cloud) is commonly referred to as lift-and-shift or infrastructure as a service (IaaS).

IaaS security challenges:

You lose your security perimeter when you migrate to the cloud. Where you traditionally would have servers behind firewalls and network access control, in the cloud the IaaS instances have to be configured and secured independently.

PaaS
Platform as a Service

Completely restructuring the way applications are built to make heavier use of prepackaged services available on these cloud service platforms – often referred to as lift-and-reshape, serverless or platform as a service (PaaS).

PaaS security challenges:

PaaS forgoes operating systems and in a lot of cases operate as services. This means that traditional security approaches like installing agents or monitoring traffic flows will be unavailable. You need new tools to maintain visibility and control.

SaaS
Software as a Service

Choosing to forgo running copies of standard applications and instead having the application vendor host them – sometimes referred to as drop-and-shop or software as a service (SaaS).

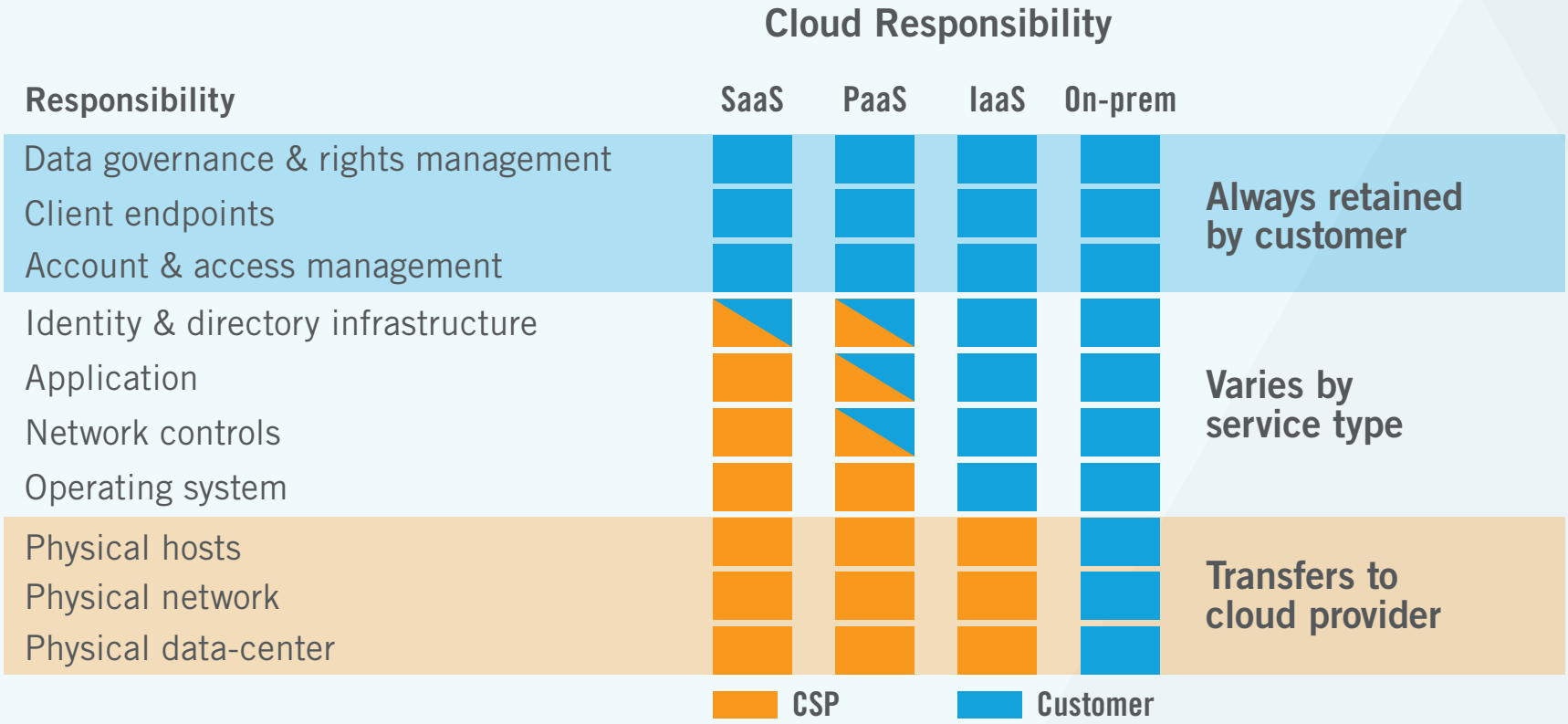
SaaS security challenges:

In a SaaS deployment model, you rely entirely on the provider to keep your data secure. However, you are still responsible for account-based attacks. This means you need to monitor and secure identities and privileges.

VECTRA
SECURITY THAT THINKS

Shared responsibility in the cloud

When adopting cloud services, security inherently becomes a shared responsibility model. In this model it falls to the Cloud Service Provider (CSP) customers to constantly adapt and deliver their half of the security operation that readjusts perfectly to the changing threat surface exposed by the CSP architecture.



VECTRA
SECURITY THAT THINKS

What are the biggest cloud security challenges?

Infrastructure as a service

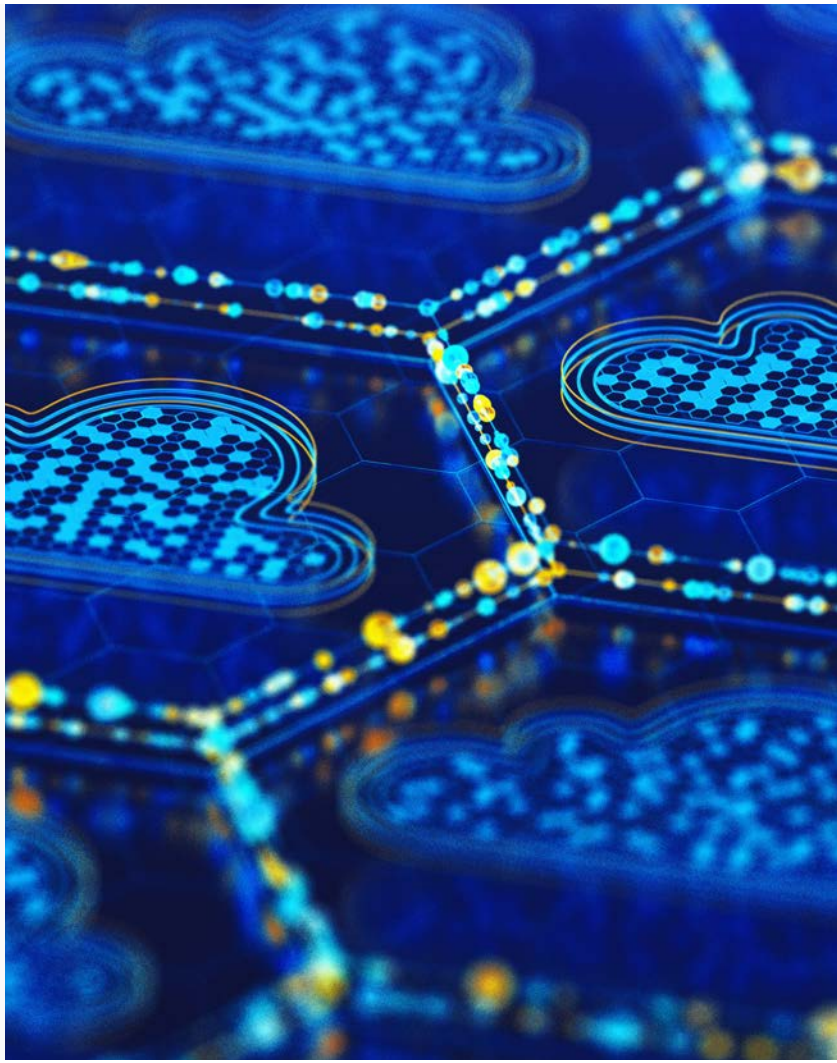
Initially, IaaS security appears to have the least change from your on-premises environment. After all, the cloud is just your application running on someone else's computer.

But Cloud Security Providers (CSPs) supply you with that computer, along with an entirely new and unfamiliar management and control plane, new identity and access paradigms, and new forms of storage.

The first generation of cloud-related breaches stemmed from organizations not understanding this new paradigm and placing confidential information in cloud storage while leaving access open to the internet.

This never happened to them in the enterprise, where their network firewalls and segmentation provided a backstop to this type of misconfiguration. What changed? There is no way to physically surround all your assets in the cloud with a network and place firewalls at the edge of that network.

The crux of the issue is simple: CSPs provide incredibly complex ecosystems that are constantly in flux as new features are added.



VECTRA
SECURITY THAT THINKS

Platform as a service

The security implications of adopting PaaS are not well-understood by many organizations. The services in question range from simple (e.g. storage) to complex (e.g. analytics stacks). And each of these services has their own security nuances.

There is a broader challenge with all services delivered via PaaS: Security teams generally have no pre-existing models of how to secure a service embedded in an application without surrounding it with a secure network. There is no way to apply that model to PaaS-delivered services.

Also note that the goal of CSPs is different from that of their customers. In rolling out new services, CSPs who develop those services are judged by the adoption of the service.

In making decisions on the default security posture of a new service, CSPs will generally remove barriers to make customer deployments easier, rather than add security controls which might also slow down its adoption by customers.

VECTRA
SECURITY THAT THINKS

Software as a service

With SaaS, there are no illusions that everything is the same, as the only thing you have access to is accounts and identities. However, SaaS has been broadly adopted as organizations realize that it allows them to introduce new applications literally overnight and without having to worry about software upgrades, backups and other mundane support tasks.

These SaaS applications can be accessed from anywhere and elements of endpoint detection and response (EDR) on the device that accesses them if you are lucky, and maybe a cloud access security broker (CASB) are expected to recreate the safety of old.

Furthermore, SaaS applications have become incredibly complex. And keep in mind this is just part of a much bigger job for IT organizations tasked with provisioning and deprovisioning access and overseeing security issues for applications.

When an end user is successfully phished or a mistake is made in configuring some part of the cloud application, attackers quickly have access to your data, and a great entry point to other services.

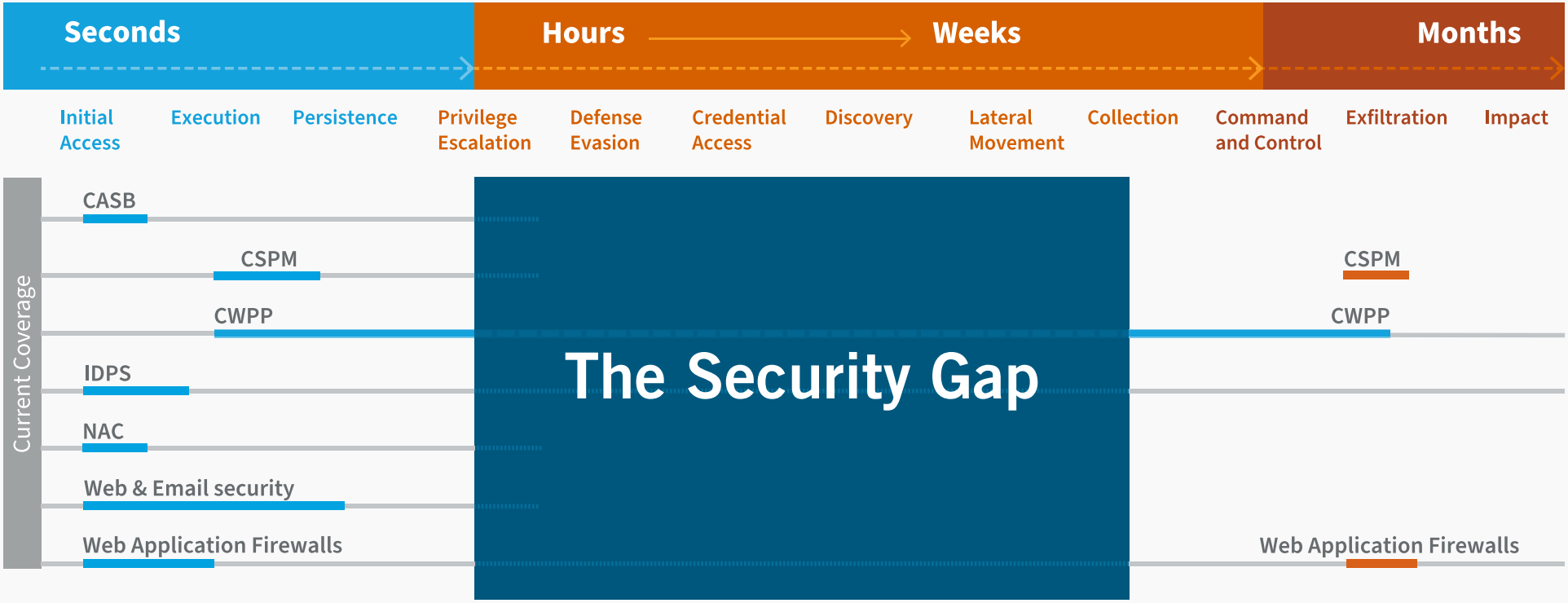
Cloud security failures in the customer's portion of the responsibility model

of enterprises are running workloads on AWS in 2021

VECTRA
SECURITY THAT THINKS

Mapping different cloud security solutions to the attack lifecycle

Your cloud security coverage will vary based on which cloud security solution you choose. See how different tools provide different breadths and depths of coverage below.



* CWPP has wide coverage, but only where agents can be deployed, which is lacking in cloud

VECTRA
SECURITY THAT THINKS

Definitions

CASB
Cloud access security broker
Sits between cloud service consumers and cloud service providers to enforce security, compliance, and governance policies for cloud applications.

CWPP
Cloud workload protection platform
Primarily used to secure server workloads in public cloud Infrastructure as a Service (IaaS) environments leveraging an agent.

CSPM
Cloud security posture management
Helps organizations discover, assess and solve cloud misconfigurations by monitoring policies.

IDPS
Intrusion detection and prevention system
A device or software application that monitors a network or systems for malicious activity or policy violations, which are typically signature-based.

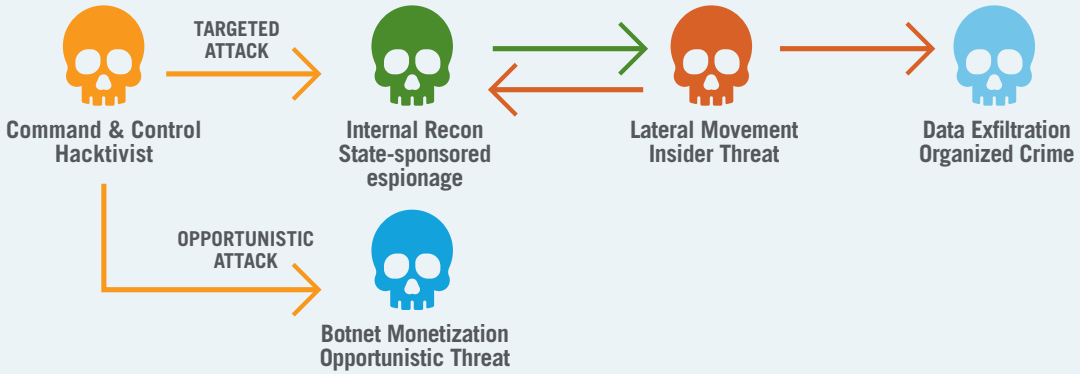
Web Application Firewalls
A web application firewall filters, monitors, and blocks HTTP traffic to and from a web application.

Web & Email security
Miscellaneous security tools targeted at protecting a specific service, such as email.

NAC
Network access control
Attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication, and network security enforcement.

VECTRA
SECURITY THAT THINKS

Preventing a compromise is increasingly difficult but detecting the behaviors that occur – from command and control to data exfiltration – is not.



VECTRA
SECURITY THAT THINKS

Detect and respond

While the move to the cloud has immediate benefits in costs and agility, there is a clear and tangible increase in risk due to poor visibility. The siloed approached to detecting threats in the hybrid cloud world provides you blind to compromised users, accounts, roles, and misconfigurations.

The traditional hardware-based method allowed security to be added after deployment in the form of firewalls and virtual patching, something that is no longer possible in cloud deployment. Once a deployment is live in the cloud, it is already too late to think about preventative security.

According to Gartner, 99% of cloud security failures will be the customer's fault. The reality is the cloud will never be configured securely due to the sheer size and scale coupled with continuous change. Ideally, you want to have visibility into the creation and changes to accounts as well as how services are being used without relying on agents or static policy rules.

Legacy operations and security practices don't translate well to the public cloud, and the cloud surface area that needs to be protected and audited is constantly changing.

Watch the video

For more information please contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai