Securing Container and Cloud Workloads

Shain Singh, Principal Security Architect, F5

@shainsingh

Our Speaker

Shain Singh

Principal Security Architect @F5

25+ years in security, network and IT

Worked in Telco/ISPs, Education, Government sectors

- DevSecOps (Continuous security in operations)
- MLSec, MLOps
- 5G Security (IIoT, Smart Cities, Edge Networks)
- API/Application Security
- Government/Industry Standards and Compliance

Social

https://linkedin.com/in/shsingh

shain.singh@owasp.org

https://twitter.com/shainsingh

https://github.com/shsingh

Professional Memberships

Research into Public Breaches

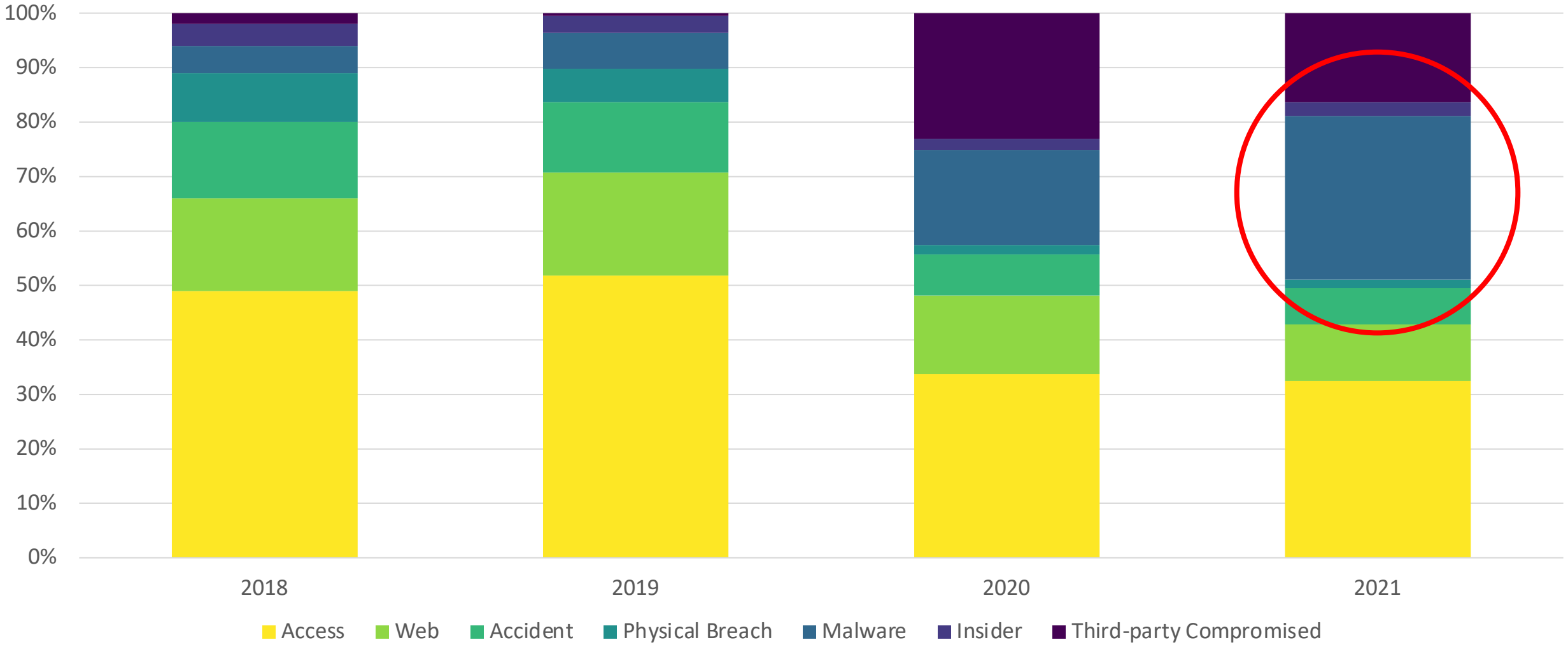
Application Protection Report

Using data to unite tactics and strategy in risk-based security

Analysing Breaches: A Prevalence of Malware

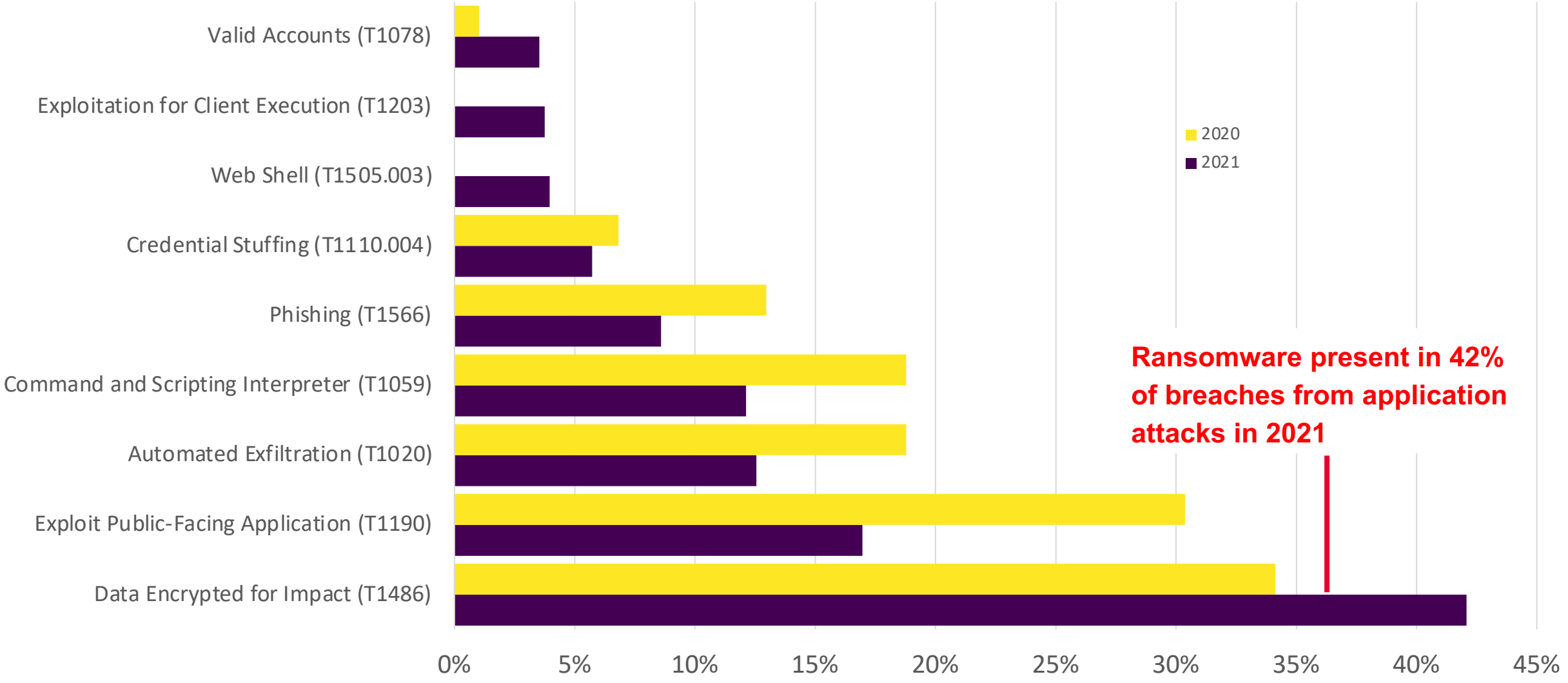
DATA BREACH DISTRIBUTION

Malware climbed to 30% of breaches in 2021

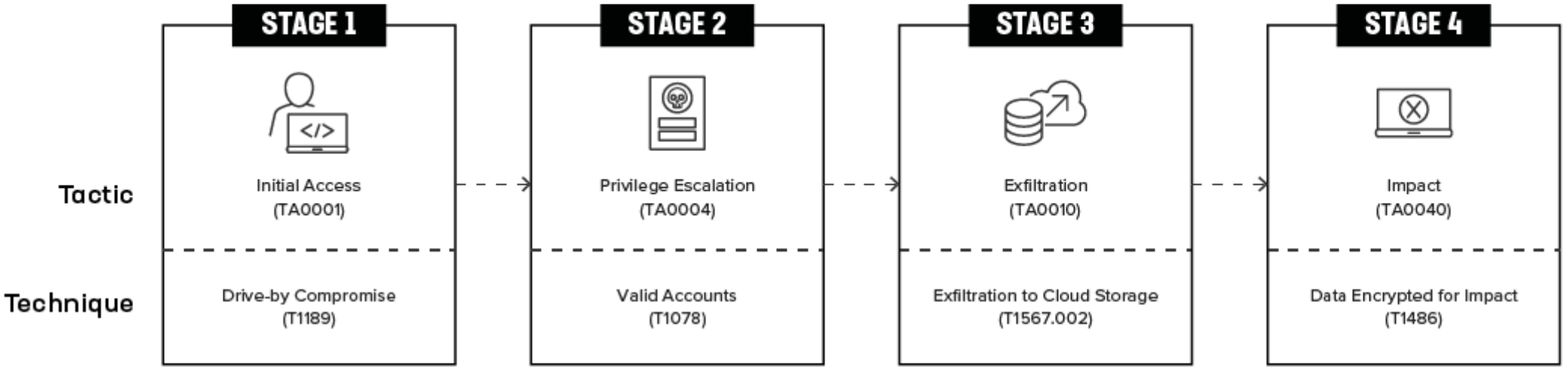


Analysing Breaches: A Prevalence of Malware

MITRE ATT&CK TECHNIQUES USED IN DATA BREACHES



Ransomware: Tactics, Techniques & Procedures



- Drive-by compromise masquerading as browser update
- Attacker obtained credentials with ***elevated privileges through unspecified activity***
- ***Lateral movement*** for reconnaissance and persistence *using legitimate tools* and credentials
- Disabled monitoring and security tools, ***destroyed backups***.
- ***Copied***, ***compressed***, and staged data from hosts for exfiltration
- Cloud storage used for ***exfiltration***
- ***Encrypted*** data using unspecified ransomware

Ransomware: Tactics, Techniques & Procedures

EVOLUTION OF RANSOMWARE SINCE 2019

1

- Long dwell times to:
  - Disable security tools
  - Compromise backups
  - Synchronise encryption

2

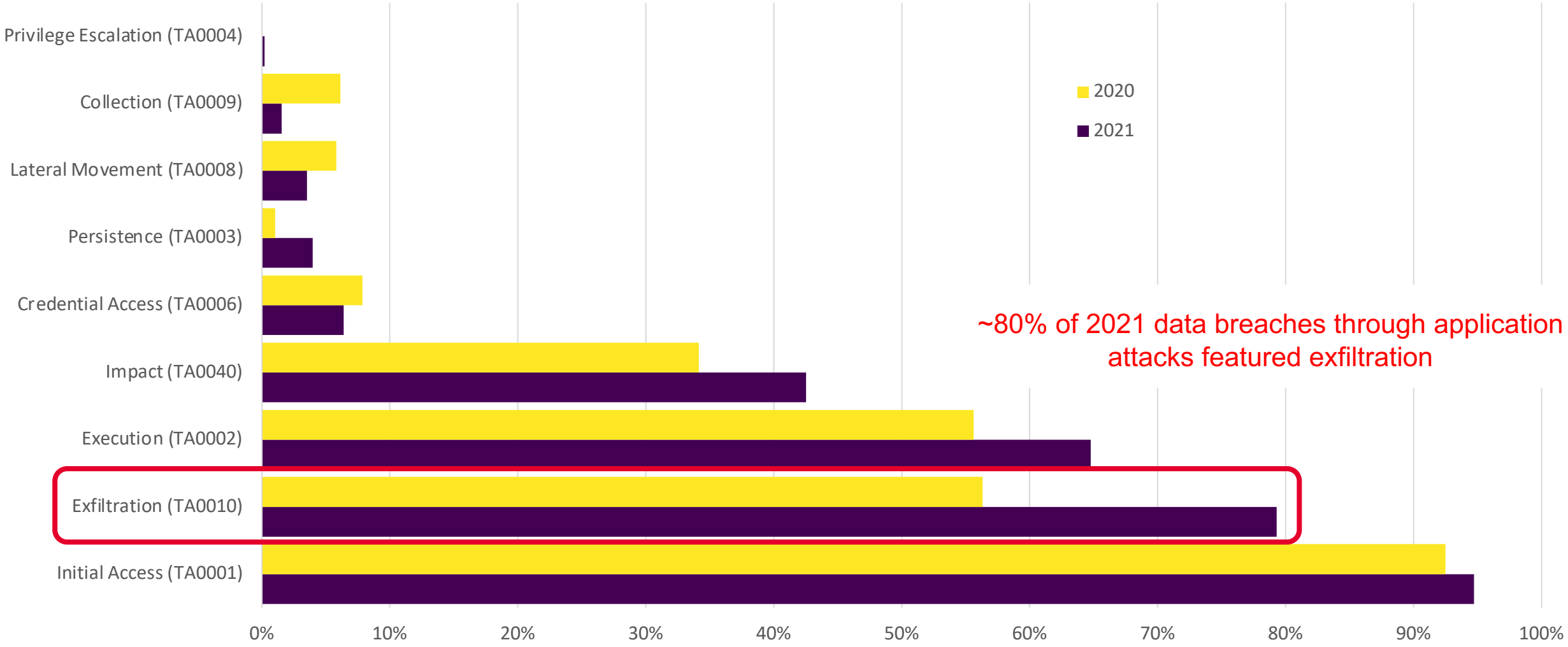
- Exfiltration of data prior to encryption
  - Double ransom approach raises likelihood of payment

3

- Ransomware-as-a-Service (RaaS)
- Affiliate model (e.g. Gandcrab)
- These practices raise frequency and impact of ransomware attacks

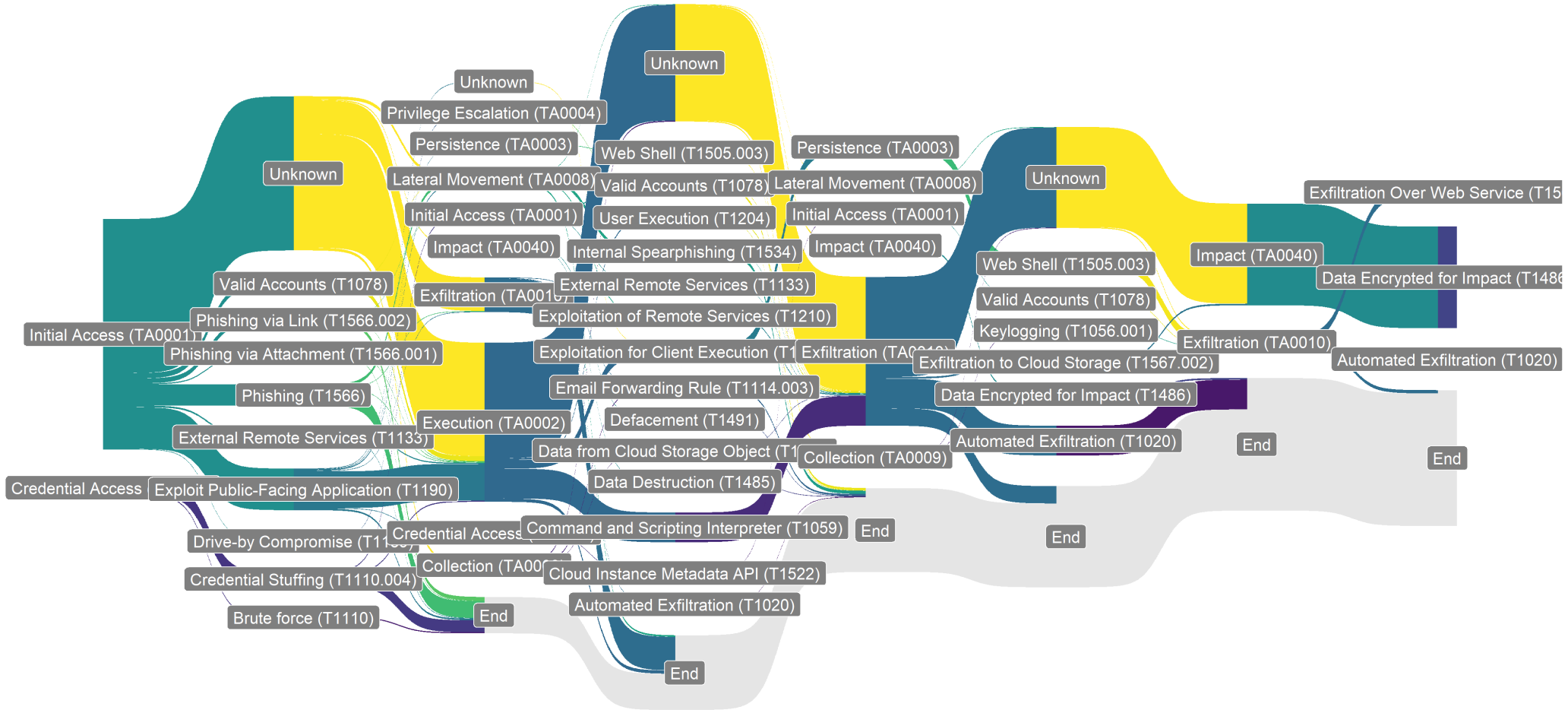
Analysing Breaches: Exfiltration

MITRE ATT&CK TACTICS USED IN DATA BREACHES



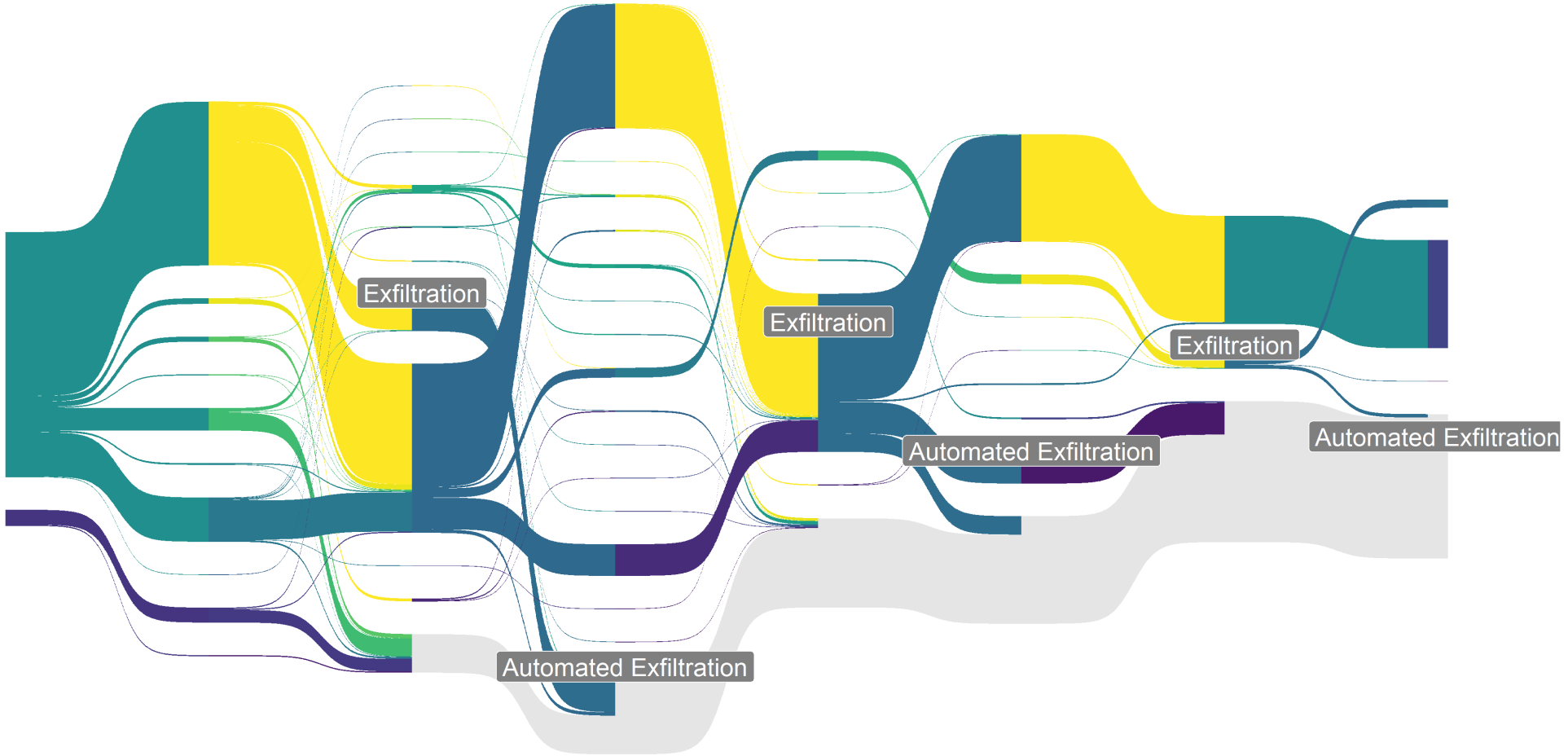
Analysing Breaches: Exfiltration Targeting

2021 MITRE ATT&CK CHAINS, *n* = 454



Analysing Breaches: Exfiltration Targeting

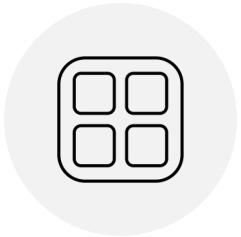
2021 MITRE ATT&CK CHAINS, *n* = 454



Challenges with Application Sprawl

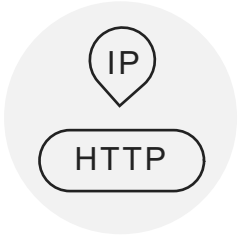
Fundamental shift in how apps are designed & deployed

Monolithic Apps



One Cloud Provider

Network-based Communication



Microservices-based Apps

Multi-cloud and Edge Computing

API-based Communication

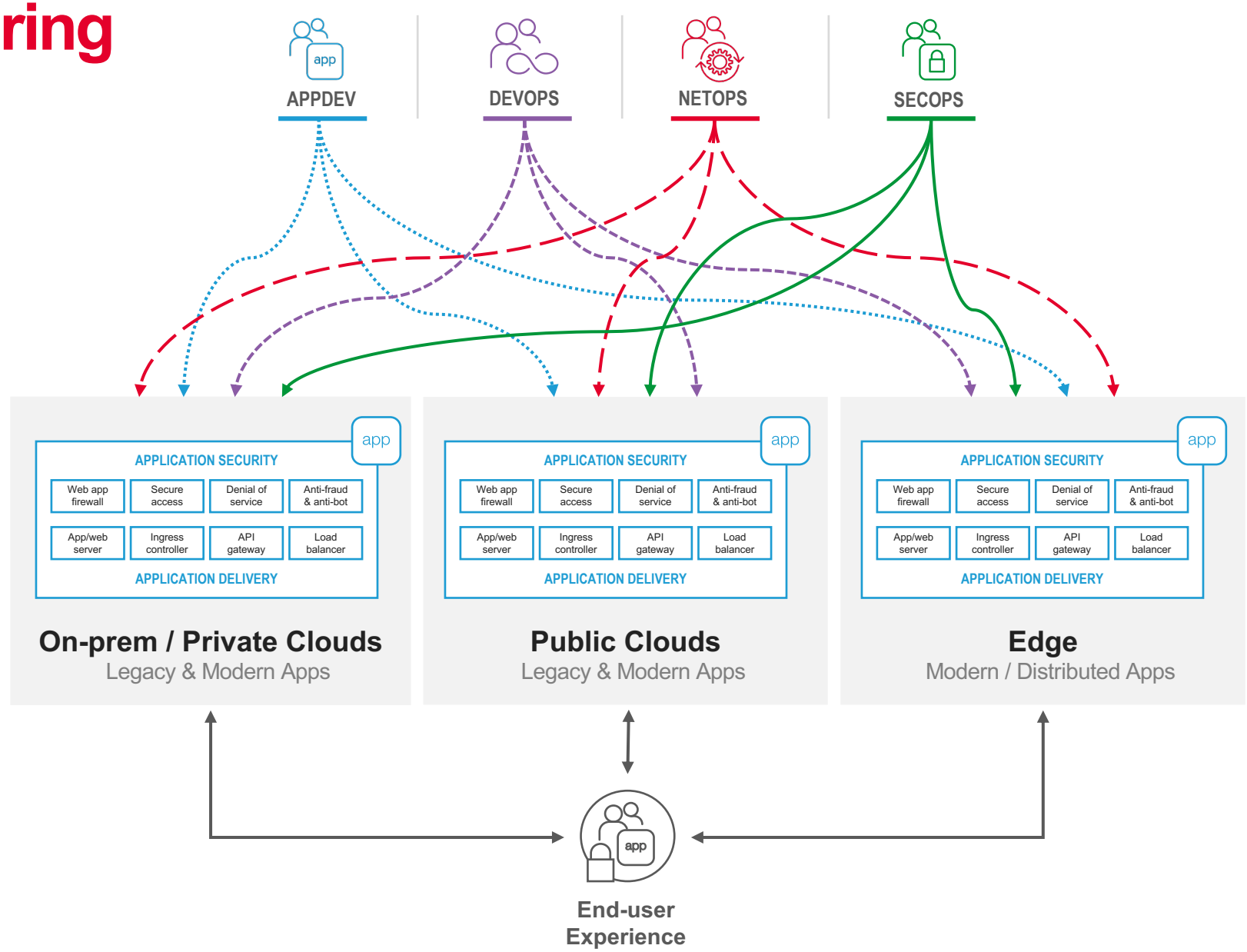
Challenges in delivering and securing apps

#1 Complex coordination because of technology inconsistencies between teams and across environments

#2 Automation challenge ”stitching” multiple environments, layering net, security, and apps, at scale

#3 Security difficulties due to multiple different attack surfaces and sophistication of bad actors

#4 Limited observability of siloed telemetry trapped in disjointed systems & environments

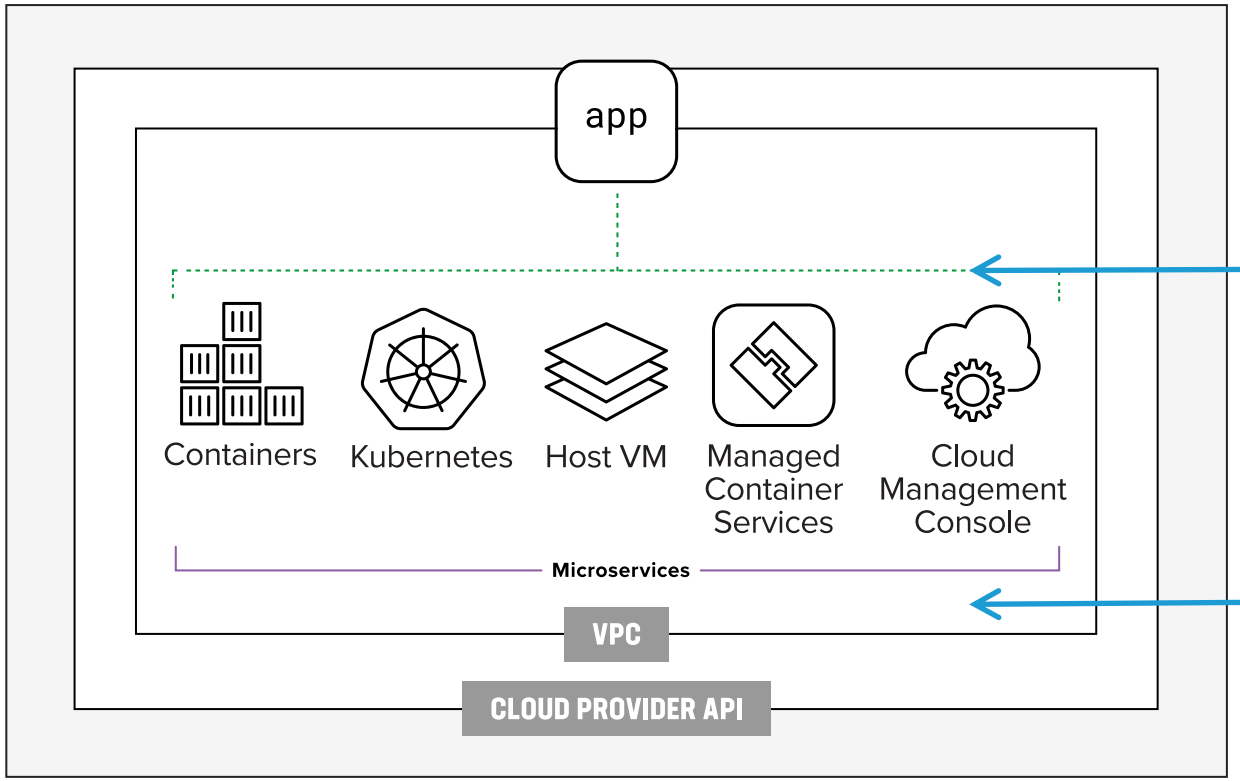


Digital Transformation and Application Modernisation

LARGE-SCALE INVESTMENT IN MICROSERVICES AND CLOUD-NATIVE INFRASTRUCTURE

Modern applications enable:

- Speed of new application deployments
- Improved TCO with operational efficiency



1. Applications delivered as microservices in containers, enables rapid delivery of new features

2. Infrastructure-as-code delivers virtualised compute and storage for rapid creation of infrastructure

Benefits of cloud-native infrastructure have inherent trade-offs

Modernisation Increases the Threat Surface for Attack

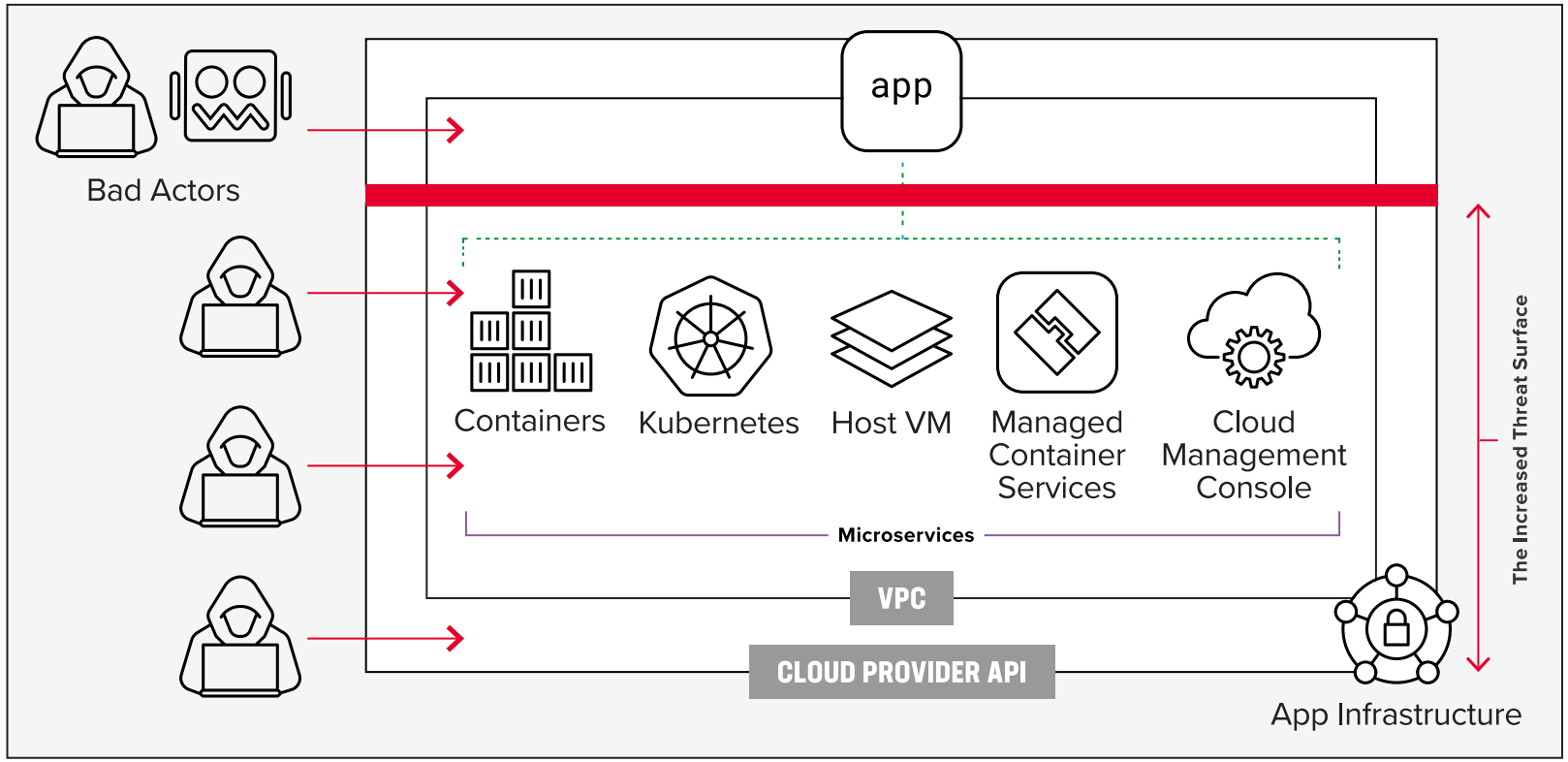
INTRODUCING MORE SECURITY RISK FOR CUSTOMERS TO CONSIDER

1 The Application

Applications and APIs are susceptible to L7 attacks, 0-day attacks, and OWASP Top 10 that can exploit vulnerabilities in code, software, or business logic.

2 Cloud-native Infrastructure

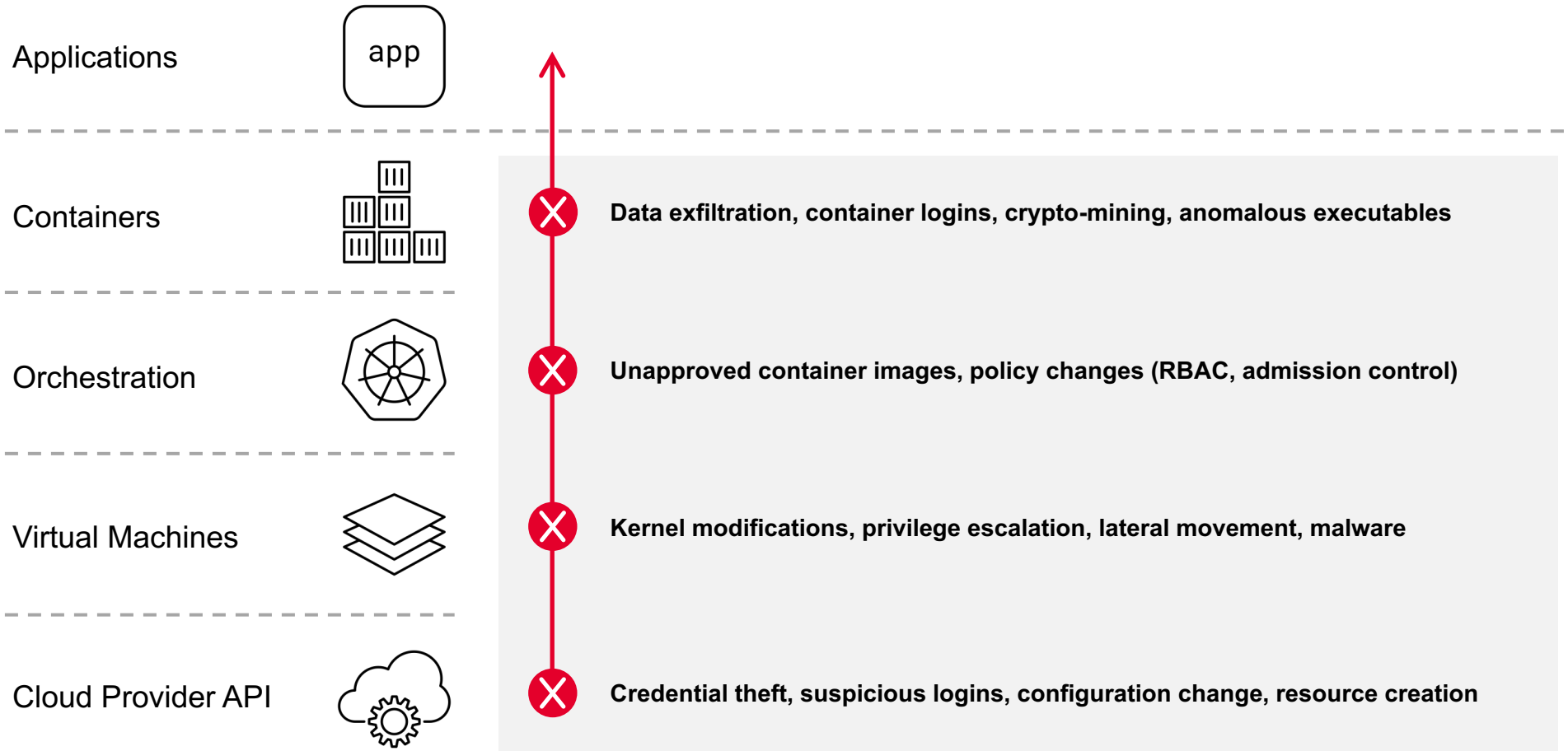
Cloud infrastructure like containers, orchestration tools, virtual machines, and cloud provider APIs can be misconfigured and vulnerable to data exfiltration, container logins, crypto-mining, and credential theft from bad actors.



Applications are only as secure as the infrastructure the run on

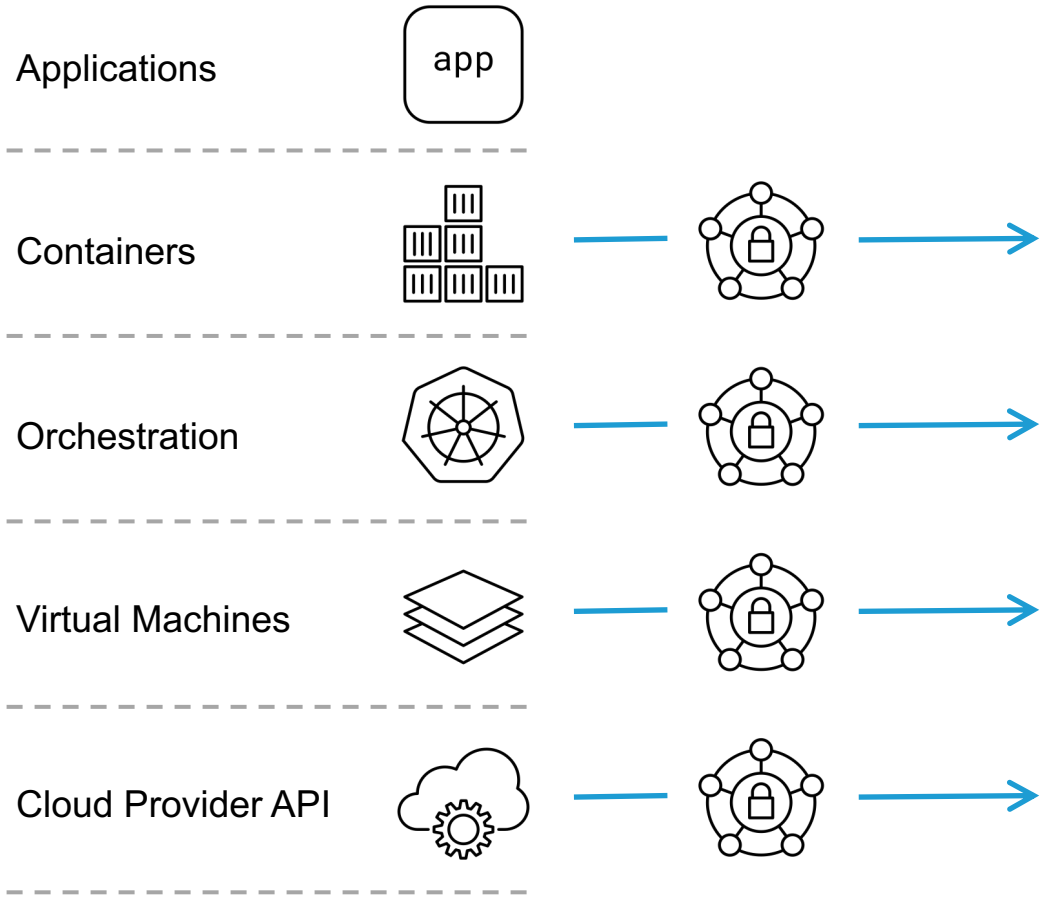
The Increased Threat Surface

ATTACKS LEVERAGE MULTIPLE ACCESS POINTS IN CLOUD NATIVE INFRASTRUCTURE



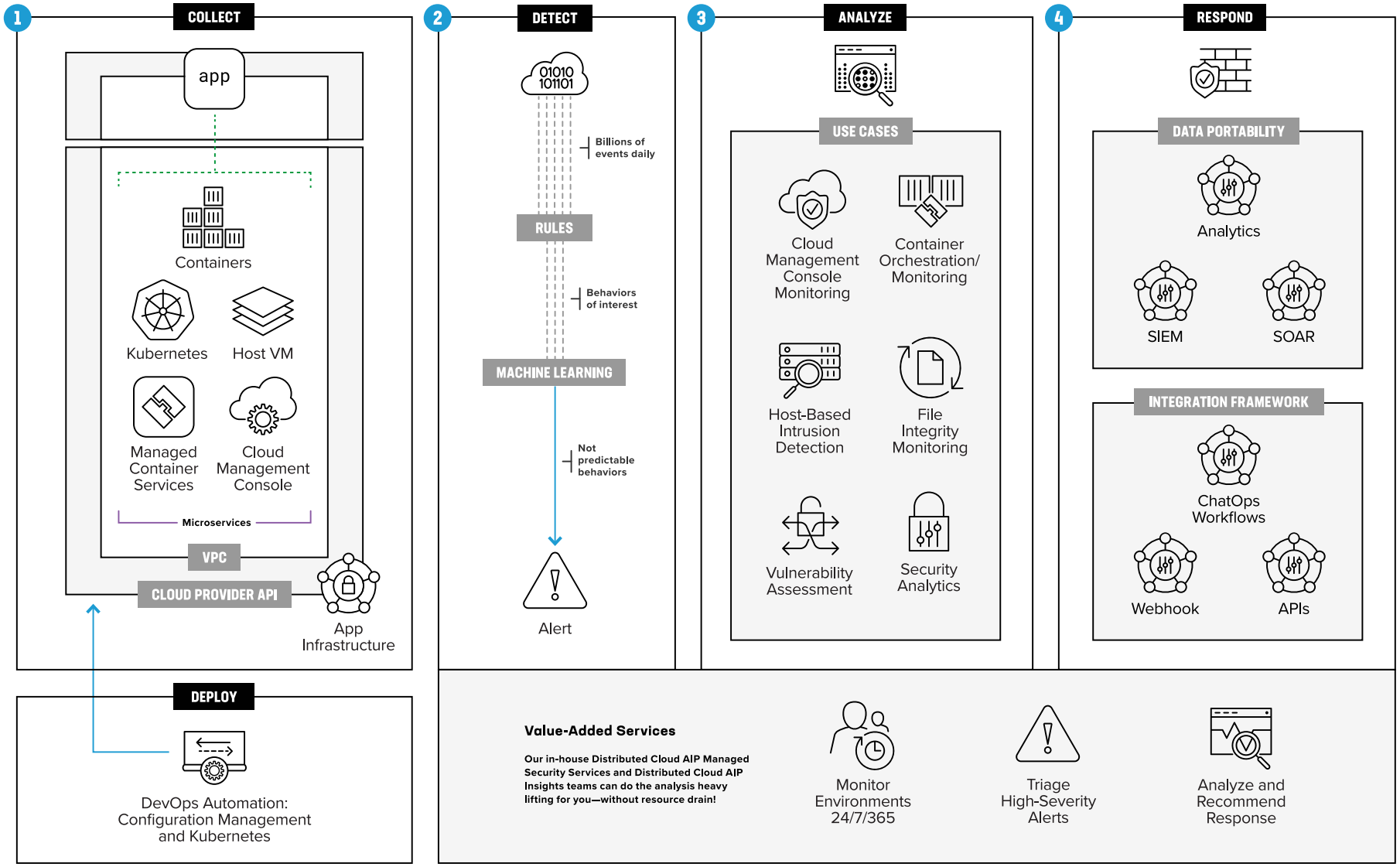
Application Infrastructure Protection (AIP)

F5 Distributed Cloud AIP - Full-stack Observability



1. **Delivered as a SaaS**
2. **Collects telemetry from each layer of the stack:** process, network, user, and file behaviors
3. **Analyzes trillions of events for threats and indicators of compromise**
4. **Integrates with incident response workflows for rapid remediation**

F5 Distributed Cloud AIP - Solution Overview



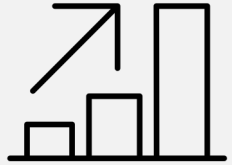
F5 Distributed Cloud AIP - Key Use Cases

Threat Detection

Behavioral analysis that leverages rules and machine learning to detect internal/external threats and IOCs

Compliance

Reports that demonstrate adherence to common compliance frameworks like PCI-DSS, SOC2 Type II, and ISO27001

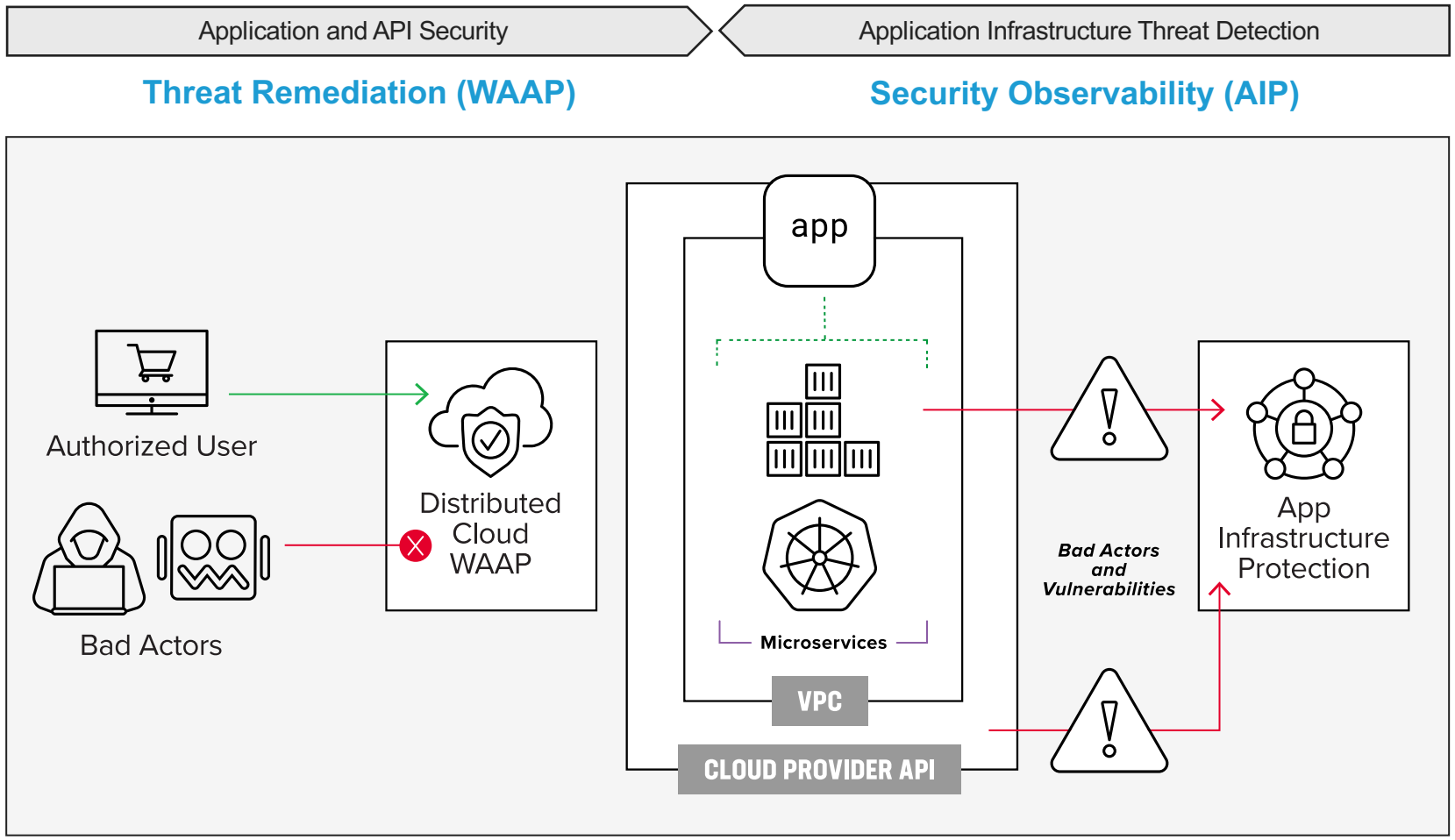


Security Posture

Analytics that highlight security posture and proactively identify areas of risk in cloud security hygiene

F5 Distributed Cloud – Combining WAAP and AIP

- Protection from L7 attacks, 0-day attacks, and OWASP Top 10
- Bot mitigation based on inferences from the client
- API auto-discovery and security



- Intrusion detection for cloud-native workloads: public, private, and hybrid cloud environments
- Real-time analysis of telemetry to detect internal threat, external threat, and risk of data loss
- Support for virtual machines, containers, Kubernetes

Detect and act on threats in real-time

Thanks for listening!