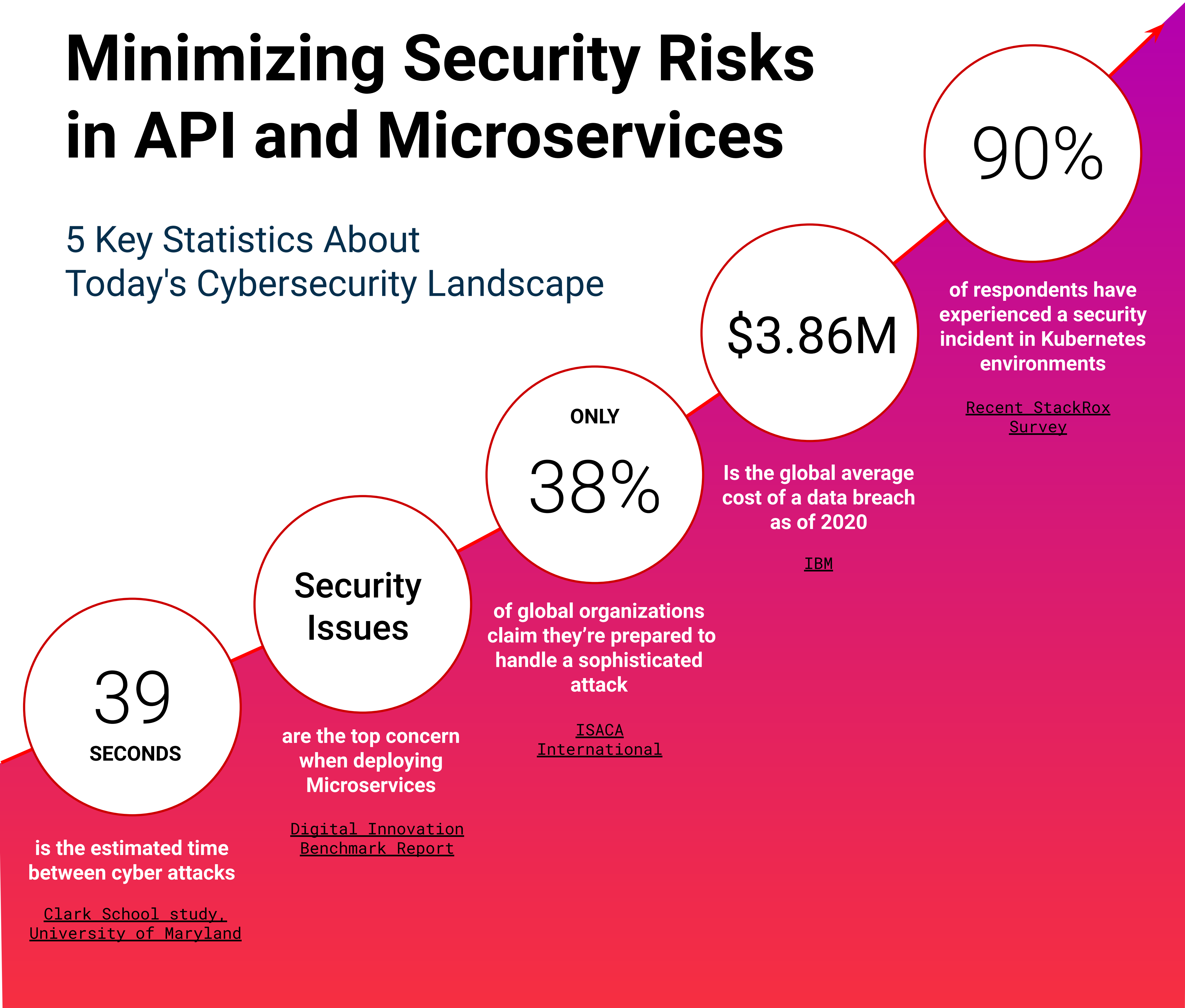
Kong

Minimizing Security Risks in API and Microservices

5 Key Statistics About Today's Cybersecurity Landscape



39 SECONDS

is the estimated time between cyber attacks

Clark School study, University of Maryland

Security Issues

are the top concern when deploying Microservices

Digital Innovation Benchmark Report

ONLY 38%

of global organizations claim they're prepared to handle a sophisticated attack

ISACA International

$3.86M

Is the global average cost of a data breach as of 2020

IBM

90%

of respondents have experienced a security incident in Kubernetes environments

Recent StackRox Survey

Security Complexities in Multi-cloud and Hybrid Cloud World

We are increasingly living in a multi-cloud/hybrid cloud world. Maintaining application and data security in a multi-cloud environment is complex at best –

- Policy configurations may be awkward or difficult to apply universally across on-premises and cloud environments
- As per the shared responsibility model, the pressure is on the Architects and CISOs to protect customer data, apply access control policies, configure firewalls and set encryption policies
- There are myriad challenges around managing and aligning your cloud provider's capabilities to the ever-evolving compliance requirements for regulations

Download the ebook to learn more.

Security Challenges in Microservices Architecture

Implementing microservices holds many promises but also introduces a unique set of security challenges. A microservices application –

- Has many small services – For each service, developers need to consider all the vulnerabilities they might expose
- Communicates via APIs – By design, APIs give access to your data. Exposing APIs via the network without proper security makes your application vulnerable to a diverse number of attacks including DDoS, API abuse and more
- Can be built by different teams – Each team may have ownership of one or more services and may require a different technology stack. Maintaining a consistent security posture across all teams and technologies is difficult

Download the ebook to learn more.

Diverse Security Approaches for Containerized and VM-based Applications

Nowadays, companies are moving from virtual machine(VM) to container-based infrastructure. Both VMs and containers are vulnerable to an array of attacks. However, it is also true that containers present more nuanced security challenges as they don't provide the same OS-level isolations as VMs.

- Containers share hosts with each other which requires a different approach and additional consideration for security
- The number and ephemeral nature of containers make it difficult to implement consistent networking and security policies that adhere to the least privilege principle

Organizations run the risk of

Losing Customer Trust and Confidence

Compliance Violations and Fines

Slowing Speed of Application Development

Questions that Help You Assess Your Microservices Security Posture

PEOPLE

- **Organizational Maturity**: Does our organization have the maturity and alignment between workforce, budget, and strategic initiatives around security?
- **Awareness:** Does our team have a clear picture of our security posture and how it relates to industry best practices with respect to APIs and microservices?
- **Skills:** Does our team have the right security skills to devise and implement a security plan that truly addresses an ever-changing threat landscape?

PROCESS

- **Secure Connectivity:** Are we making our microservices application and the traffic flowing through it secure at the edge and within the application?
- **Consistent Security across any Infrastructure:** Are we establishing consistent security across our containerized and VM-based applications deployed across clouds and data centers?
- **Mitigation Plan**: Do we have an established process to respond to security breaches?
- **Compliance:** Do we have the operational checks and policies in place to ensure compliance with industry, government and organizational standards?

TECHNOLOGY

- **Encryption**: Is our data encrypted during transit and at rest?
- **Centralized Management**: Are we able to centrally apply and enforce security policies across all our services and APIs?
- **Resiliency**: How are we creating application resiliency while prioritizing security between services?
- **Multi-tenancy Security**: How are we ensuring data safety or privacy of tenants' data in a multi-tenant environment?
- **Observability**: Do we have the right tools to proactively detect and mitigate potential threats?

Address Your Security Gaps by Putting Zero-Trust Principles To Work

LEVERAGE

Mutual Transport Layer Security (mTLS)

to encrypt service-to-service communication

SET

Traffic Permission

policies to allow or disallow traffic between services in an environment

ENABLE

Open Policy Agent (OPA)

to provide fine-grained, policy-based control by default across a cloud native stack

aws | Azure | Google Cloud | OPENSHIFT

Consider across all Infrastructure:
Clouds/Regions/Kubernetes and VMs

Kong

To learn more, schedule a demo today.