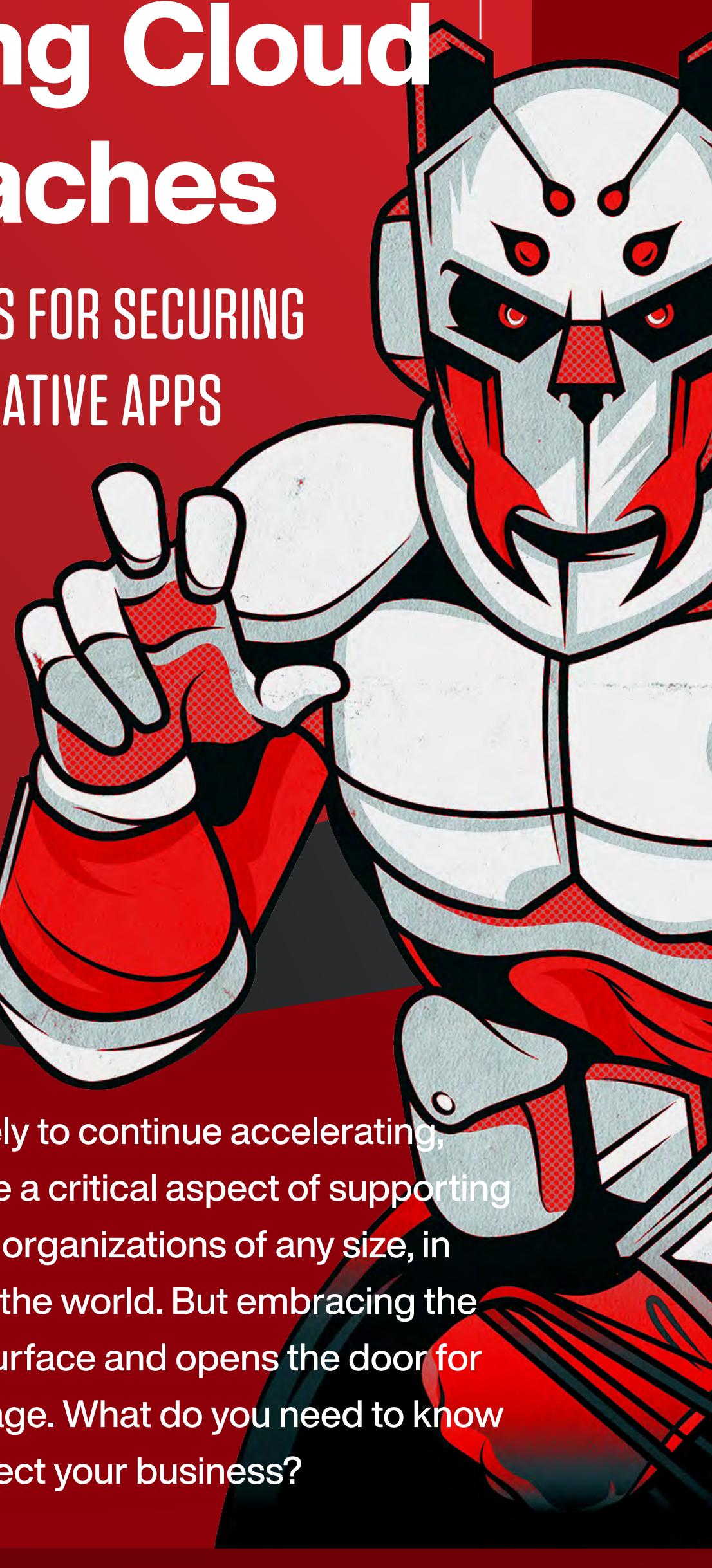
CROWDSTRIKE

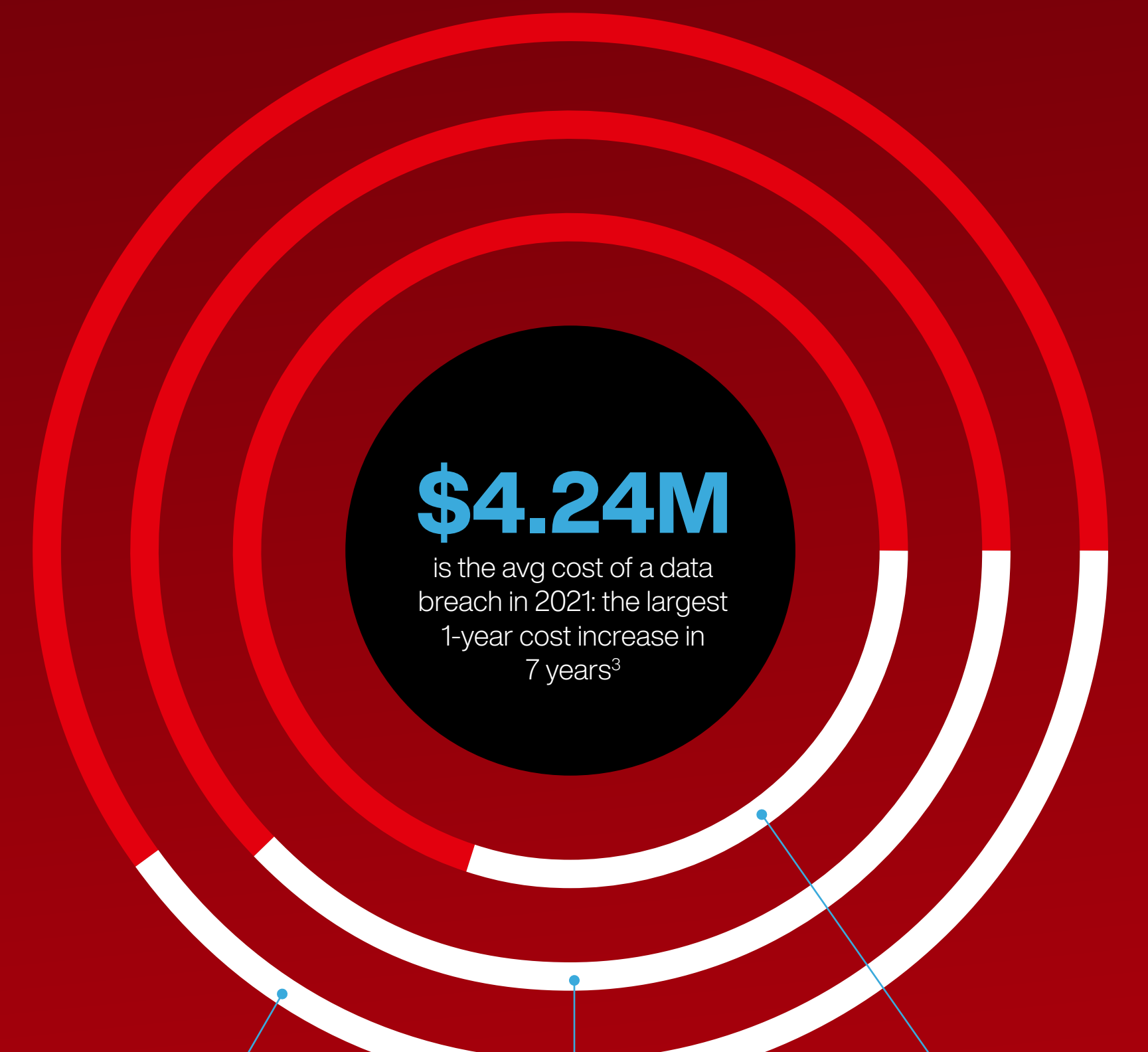
Stopping Cloud Breaches

6 ESSENTIALS FOR SECURING CLOUD-NATIVE APPS



With cloud adoption likely to continue accelerating, securing cloud assets will be a critical aspect of supporting digital transformation at organizations of any size, in any industry, anywhere in the world. But embracing the cloud widens the attack surface and opens the door for adversaries to take advantage. What do you need to know in order to protect your business?

What Are the Consequences?
"Data Out, Malware In"



40% of companies reported unauthorized access to apps and data due to cloud misconfigurations[2]

38% of companies reported the introduction of malware due to cloud misconfigurations[2]

30% of companies reported the introduction of ransomware due to cloud misconfigurations[2]

Why Is This Happening?

Shadow IT
- Lack of visibility
- Unauthorized usage
- Unsecured assets

Cloud Complexity
- Misconfigurations
- Security consistency
- Use of insecure APIs

Runtime Threats
- Adversaries
- APTs/zero-day exploits
- Vulnerabilities

Skills Shortage
- IAM, key management
- Cloud/security
- Shared responsibility

Today's Reality: A Diverse Range of Cyberattacks

Malware that has moved laterally to cloud workloads	27%
Targeted penetration attacks	25%
Exposed or lost data from an object store	25%
"Zero day" exploit(s) that took advantage of new and previously unknown vulnerabilities	24%
The misuse of a privileged account, secrets, or access keys via stolen credentials	23%

Despite all of this, only **1 in 5 organizations** regularly assesses its overall cloud security posture[4]

4 Top Priorities for DevSecOps

#1 Creating security consistency across data center and public and private cloud environments

#2 Automating the introduction of controls and processes via integration with the software development lifecycle and CI/CD tools

#3 Improving knowledge and understanding of the threat model and adversaries for cloud-native apps and infrastructure

#4 Consolidating to an integrated cloud-native cloud workload protection platform

6 Essentials for Securing Cloud-native Apps

1 Make it your mission to eradicate vulnerabilities
Know your images. Understand how they're built and what code is used — including both software and configuration.

2 Enforce container immutability
Harden your images, containers and hosts. Embrace automation to continuously scan and implement checks as you manage and align with regulations.

3 Reduce the attack surface before runtime
Take a "shift left" approach to security to identify and fix vulnerabilities earlier. Integrate with your CI/CD tools like Jenkins or Azure DevOps.

4 Enforce access control
Ensure role segregation of your container environment, and integrate access control tools with enterprise directories for detailed access management and better visibility.

5 Automate runtime protection
Immutability of containers enables faster, more accurate threat identification. Scale runtime protection through the automation of threat defense and anomaly detection by baselining container behavior.

6 Audit, audit and audit again
Take steps to minimize container sprawl, and eliminate risky containers and images.

Sources:
1. State of Cloud Security 2021 (Ermetic/IDC)
2. The Maturation of Cloud-native Security: Securing Modern Apps and Infrastructure (ESG, March 2021)
3. https://www.foley.com/en/insights/publications/2021/07/4-24m-now-the-average-cost-per-data-breach
4. Implementing Cloud Security Best Practices — August 2020 (Tripwire)

About CrowdStrike

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.