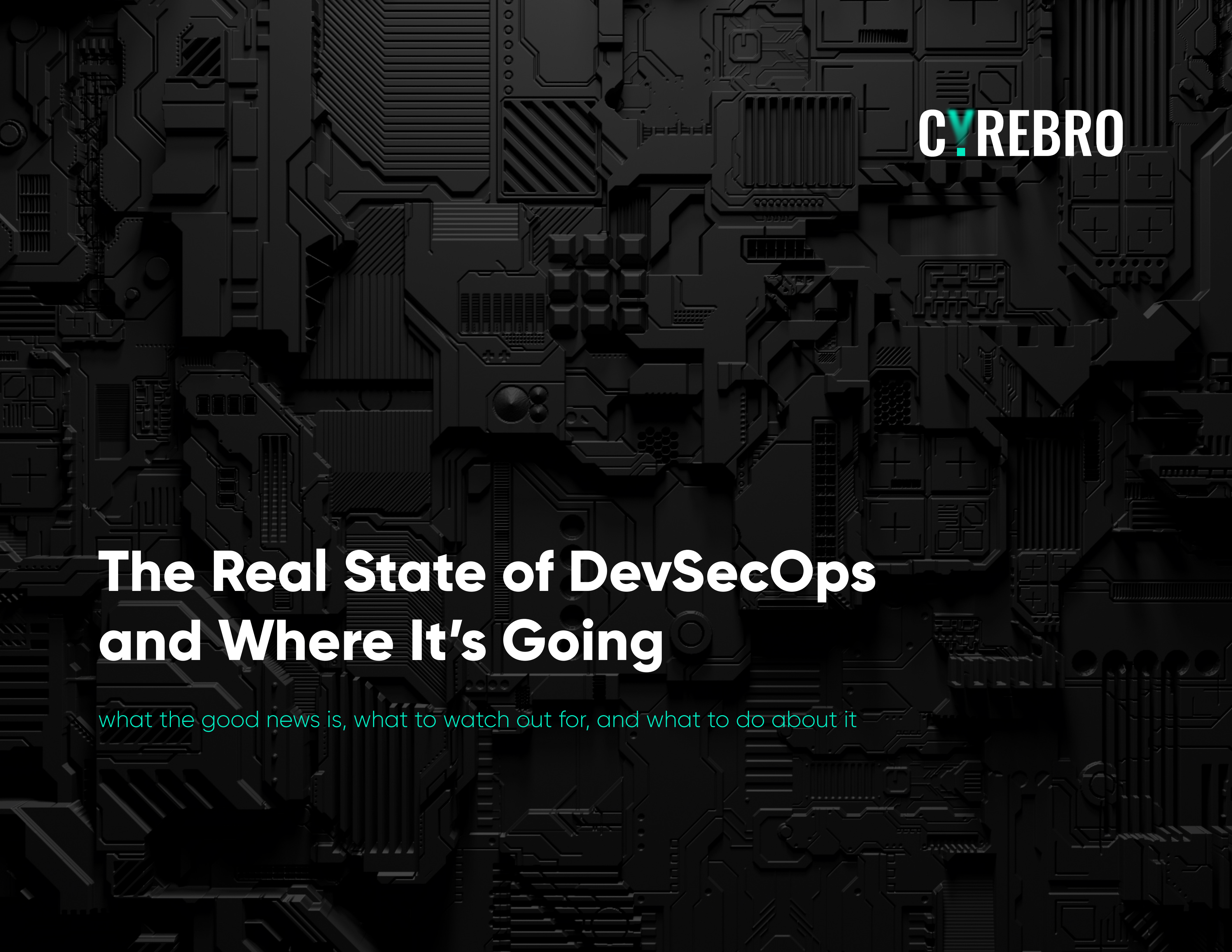


CYREBRO

The Real State of DevSecOps and Where It's Going

what the good news is, what to watch out for, and what to do about it

Contents

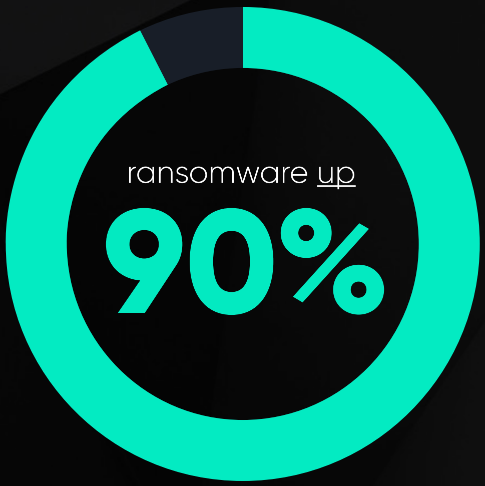
The state of security

The DevSecOps challenge

In our current state of ongoing uncertainty, there is one thing that we can be sure of – cybercriminals are only getting more and more sophisticated, and – implementing security decisions and actions that don't slow down development nor impact operations is only going to get more challenging.

destructive attacks on data and networks are up

102%



ransomware up

90%

2021 cost of cybercrime to reach

$6.1 trillion

Overcoming the challenge

Shifting security even further to the left to achieve scale and speed requires a carefully weighed understanding of the state of security.

In this paper we present the **trends** that will help **bolster** the capabilities of DevSecOps teams in assuring the security of data, applications, and systems.

We will also present those that could **hinder** their efforts as well as **key takeaways** for security prioritization and decisioning as we move ahead in the new normal.

The good news for boosting protection

The focus on DevSecOps is on

With over **1,000 DevSecOps projects** on GitHub, of which over 800 are from just the past couple of years, we see that the focus on and importance of DevSecOps-driven security is increasing all the time.

And here's the good news – the tools that no DevSecOps toolset can be left without are serving users and addressing needs better than ever, i.e. **monitoring** and **zero-trust**.

CYREBRO INSIGHTS

730%

increase in 2020 among clients using DevSecOps-related products

884%

more tickets related to infrastructure & tools security investigated in 2020

CYREBRO INSIGHTS

UPLIFT

in monitoring-centric projects

INCREASE

in client requests for connecting to a monitoring platform

24/7

monitoring of the full security stack in high demand

Eyes on monitoring

Observing and detecting security threats during each phase of the DevSecOps pipeline is critical.

As we all know, code that may be perfectly safe today, might be vulnerable tomorrow. Therefore, it must be monitored – both the code that is being developed as it is being developed, as well as that which is already running.

In fact, the trend to more and more monitoring is far-reaching with IDG noting that together with authentication and cloud data protection, **monitoring** will **top the list of security budgets and priorities** in the year ahead.

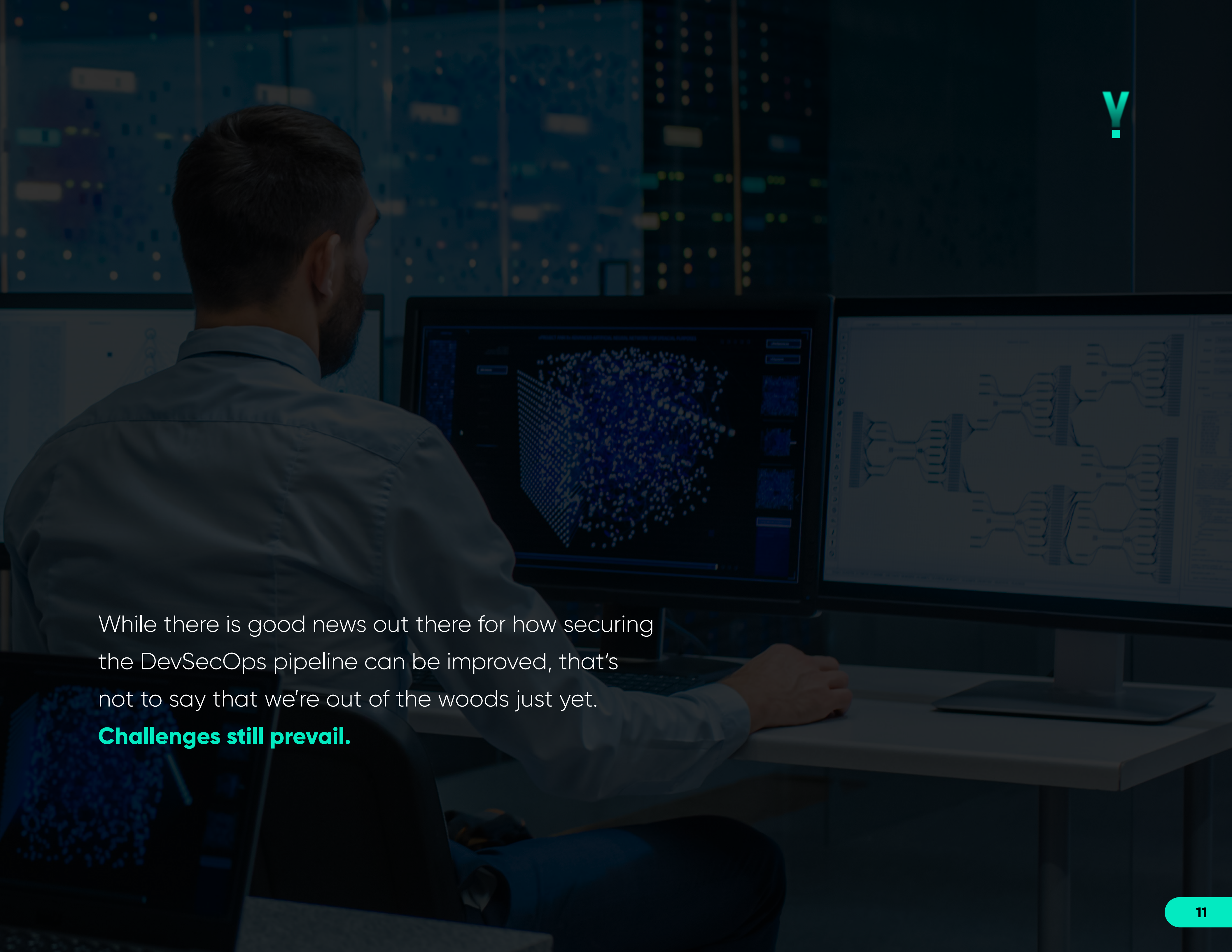
Trust in zero-trust

With traditional network security solutions no longer capable of protecting our perimeterl-ess world, zero-trust technologies introduce a more robust approach to the task.

The zero-trust approach enables DevSecOps with more rapid and more secure development, greater interoperability, and enhanced threat mitigation.

There are new tool sets and open-source SDKs available today that are helping DevSecOps drive zero-trust security through features such as mutual TLS, secure service discovery, network authentication, and access control for clients, services, and data.

What to watch out for



While there is good news out there for how securing the DevSecOps pipeline can be improved, that’s not to say that we’re out of the woods just yet. **Challenges still prevail.**

Beware of Docker images

There is no doubt that Docker is today's go-to for automating the development, deployment, and running of applications inside isolated containers. It delivers multiple benefits including agility, scalability, and portability.

In fact, Docker has seen a **70% increase in activity** from 11.3 million monthly active users who are sharing 7.9 million apps that are pulled 13.6 billion times every month.

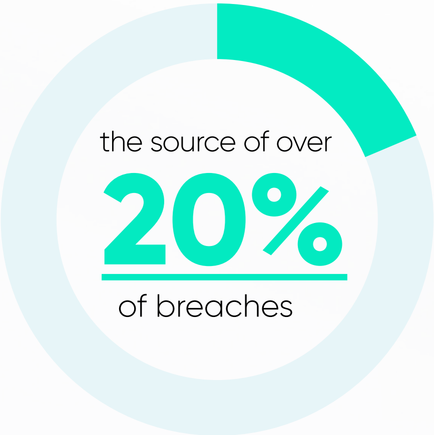
Though alongside its popularity, Docker does present some significant security challenges.

Namely, while Docker images make downloading and using containers easier by leveraging open source libraries, **51% of these images have exploitable vulnerabilities**.

To reduce the risk, **code repository scanning** is often used in the hopes of detecting such vulnerabilities, as well as misconfigurations and information disclosure. But this often leaves users on an endless chase after vulnerabilities and misconfigurations.

The misconception of misconfigurations

When it comes to assuring security in the DevSecOps pipeline, it is also critical to take heed of misconfigurations, which are:



the source of over **20%** of breaches

among the **top 3** cloud security threats

one of the **most common** ways for penetrating IaaS environments

And cybercriminals have taken note, having become quite adept at scanning code repositories for such misconfigurations to leak sensitive data.

Just one of the many examples comes from late 2020 when nine GitHub repositories were found to be leaking health data from over 150,000 patients.

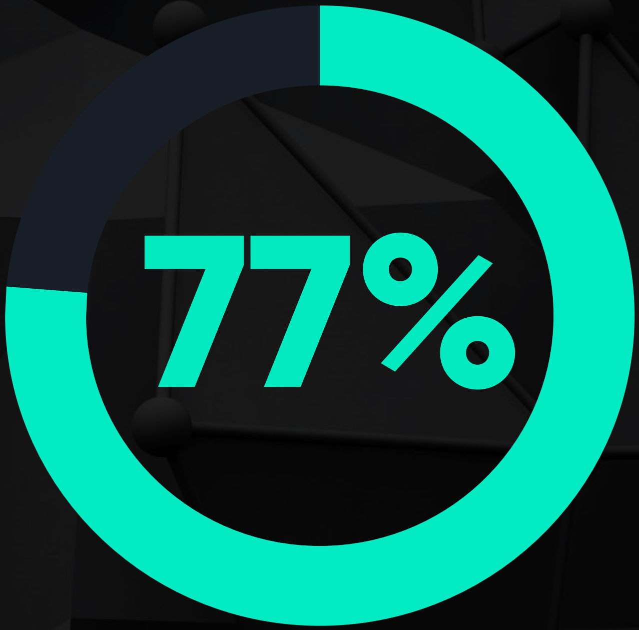
Who are you?

The third challenge we'd like to focus on is **user identity**, which – together with **privilege management**, is becoming more complex for DevSecOps, and now represents one of the top security concerns worldwide.

Even with many organizations having identity and access management (IAM) and privileged account management solutions in place, they are often insufficient for protecting cloud environments.

Among the reasons behind this is the accumulation of unnecessarily **excessive permissions** granted to users and applications for public cloud infrastructure deployments, a **lack of standardization**, and continual **shifts in privileges** and roles.

CYREBRO INSIGHTS



of user identity related incidents had user behaviour anomalies as the root cause.

The user behavior hurdle

Often, choosing which solution to opt for can be no less of a challenge, where the choice is often driven by the type of environment, whether mostly on-prem, cloud, or hybrid.

But regardless of which solution is selected, it is important to note that what lies at the heart of IAM and privilege management-driven security incidents is **user behavior**.

And, one of the most effective ways to prevent these incidents is to leverage **artificial intelligence** for detecting anomalous activities.

There is no such thing as trusted software

By now, we are all woefully familiar with the infamous case of the **SolarWinds** cyberattack, where hackers inserted malicious code into a software update that caused **18,000 customers** to inadvertently infect their systems.

This incident, regarded as one of the most massive breaches in recent US history, bears a lot of important lessons for DevSecOps.

The first and clearest lesson is that **software updates are no longer reliable** for preventing attacks.

And what may be perceived as a trusted piece of software, can no longer be trusted.

SolarWinds Hits

Microsoft
US Depart. of Homeland Security
US Depart. of Defense
US Depart. of State
US Depart. of Commerce
and many more

CYREBRO INSIGHTS

630%

increase in cloud data attacks since January 2020

79%

of companies reporting at least one cloud data breach

33%

of cyberbreaches investigated occurred in multi-cloud or hybrid-cloud environments

With cloud comes the storm

The move to cloud is continually accelerating, with the global SaaS market expected to reach **$138 billion** by 2022.

The benefits are clear – agility, scalability, and cost efficiency, among others.

But the risk is also clear, with cybercriminals being all too familiar with the vulnerabilities inherent to cloud computing and having refined their techniques for attacking cloud systems and web applications in their aim to penetrate the corporate network.

Key takeaways

The challenges are big

As we have seen, there is always progress in the innovation that is made available to DevSecOps for improving security throughout the application development lifecycle.

For example, we have great new capabilities for monitoring and the proliferation of zero-trust methodologies and architectures.

Though, there are still some very formidable challenges, including:

User identity & privilege management

Software updates

Docker images

Cloudification

Misconfigurations

What can DevSecOps do about it?

- **Consolidation**
- **Compartmentalization**
- **Accountability**

Consolidation

Consolidating security management solutions and enabling cross-platform automation is a key enabler for improving security.

This is because “tool sprawl” and a lack of cross-vendor integration often serve as obstacles to effective cyber protection.

Clearly, managing the security operation through a **single pane of glass** serves as a strategic boon to profoundly improving security.

Example #1

Even if different systems are used, such as identity management from different sources - whether cloud, AD, SAAS, or other, a single and unified zero-trust solution should be used for managing the organization’s identities.

Example #2

Developers can run many different types of containers and write code across different environments.

But the version management and vulnerability scanning should be executed from one place.

Compartmentalization

To avoid the risk of falling victim to risky software updates, permissions should be compartmentalized and distributed, and settings should be set as accurately as possible.

Accountability

The final takeaway takes us back to the fact that cybersecurity is not just about the technology. It is no less, if not more – about people. And here is where accountability comes into play.

For, we have seen that those who launch cyberattacks are continually increasing their ability to execute successful attacks. This means that we, as the defenders, must also improve our ability to defend.

CYREBRO TIP

The most powerful tools that can support the strategic effort of accountability are big data analytics and artificial intelligence, which are optimal for eliminating vulnerabilities, policy violations, data leaks, as well as for detecting, preventing, and responding to breaches and attacks.

Want to learn more?

To learn more about how your DevSecOps team can accelerate security in the new normal, we invite you to go to **www.cyrebro.io**.

About CYREBRO

At CYREBRO we are on a mission to revolutionize the way organizations manage their cybersecurity operations by putting the power of a full-fledged SOC in the hands of any user in any organization.

Our team of **cybersecurity experts** who come from the most **elite intelligence units** in the Israeli army and include seasoned white hat and red hackers, defenders, and state-level investigators, have developed the industry's first cloud-based technology-agnostic platform for SOC as a Service.

With the platform, both Fortune 500 and SMBs can address the **full scope of cybersecurity** needs including monitoring, threat hunting, response, and compliance, in the most **effective**, **powerful**, and **cost-efficient** way.