

GET THE CONTEXT
YOU NEED
TO PLAN YOUR
CYBER DEFENSE

- 3 Intro
- 4 Cybersecurity lifecycle management across typical enterprise organizations
- 7 The 3 challenges to reach best practices in policy management

CONTENTS

- 10 What to look for in a context-aware change management solution
- 14 Best practice business goals for policy management
- 19 Benefits of moving to context-aware policy management with Skybox
- 22 Your pathway to achieve comprehensive context-aware change management
- 25 Contact us

SEE

As the scale of your operations increases, so do potential vulnerabilities caused by the disappearance of traditional network perimeters. It's time to approach management of these vulnerabilities in a new, intelligent way to gain greater visibility across your operations.



77%

of CISOs report that cybersecurity issues are on their board's agenda at least quarterly¹

KNOW

Remote business operations and distributed workforce has triggered an urgency for deploying new technologies, applications and cloud-native solutions. There is a lack of cohesion between threat response and implementing new security policies and configurations, and a resulting lack of essential context that shapes long-term security strategies.



60%

of an organization's ecosystem, on average, is protected by cybersecurity programs²

ACT

The reality of siloed vulnerability and policy management technologies is exposing companies everywhere to systemic risk. These silos need to be removed, and the two management technologies united.



46%


of organizations had an incident caused by an unpatched vulnerability³

¹ Deloitte, The Future of Cyber Security, 2019

² Accenture, State of Cybersecurity Report, 2020

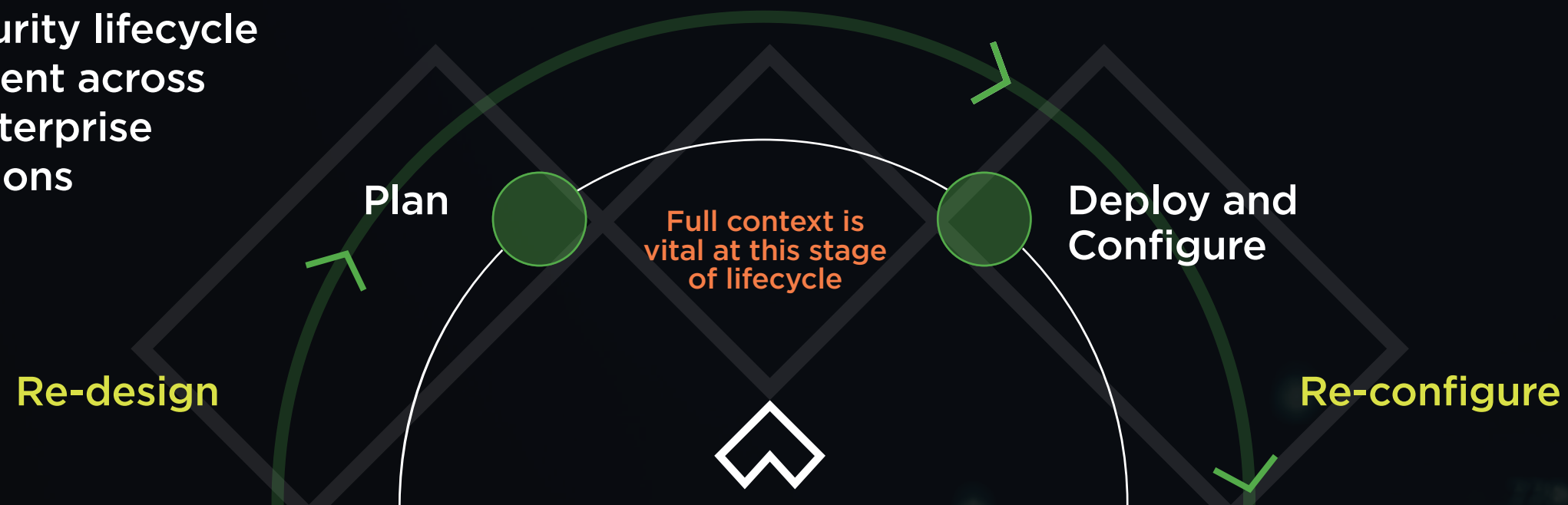
³ Cisco, UK CISO Benchmark Report, 2020

Cybersecurity lifecycle management across typical enterprise organizations

A circular diagram with five green nodes connected by a white line. The nodes are positioned at the top-left, top-right, bottom-right, bottom, and bottom-left. A thick white horizontal line passes through the center of the circle. The background features a dark blue grid with diamond shapes and faint network icons.

If the two halves of policy management and vulnerability management aren't coordinated properly, crucial **context** will be lacking across the enterprise cybersecurity lifecycle.

Cybersecurity lifecycle management across typical enterprise organizations



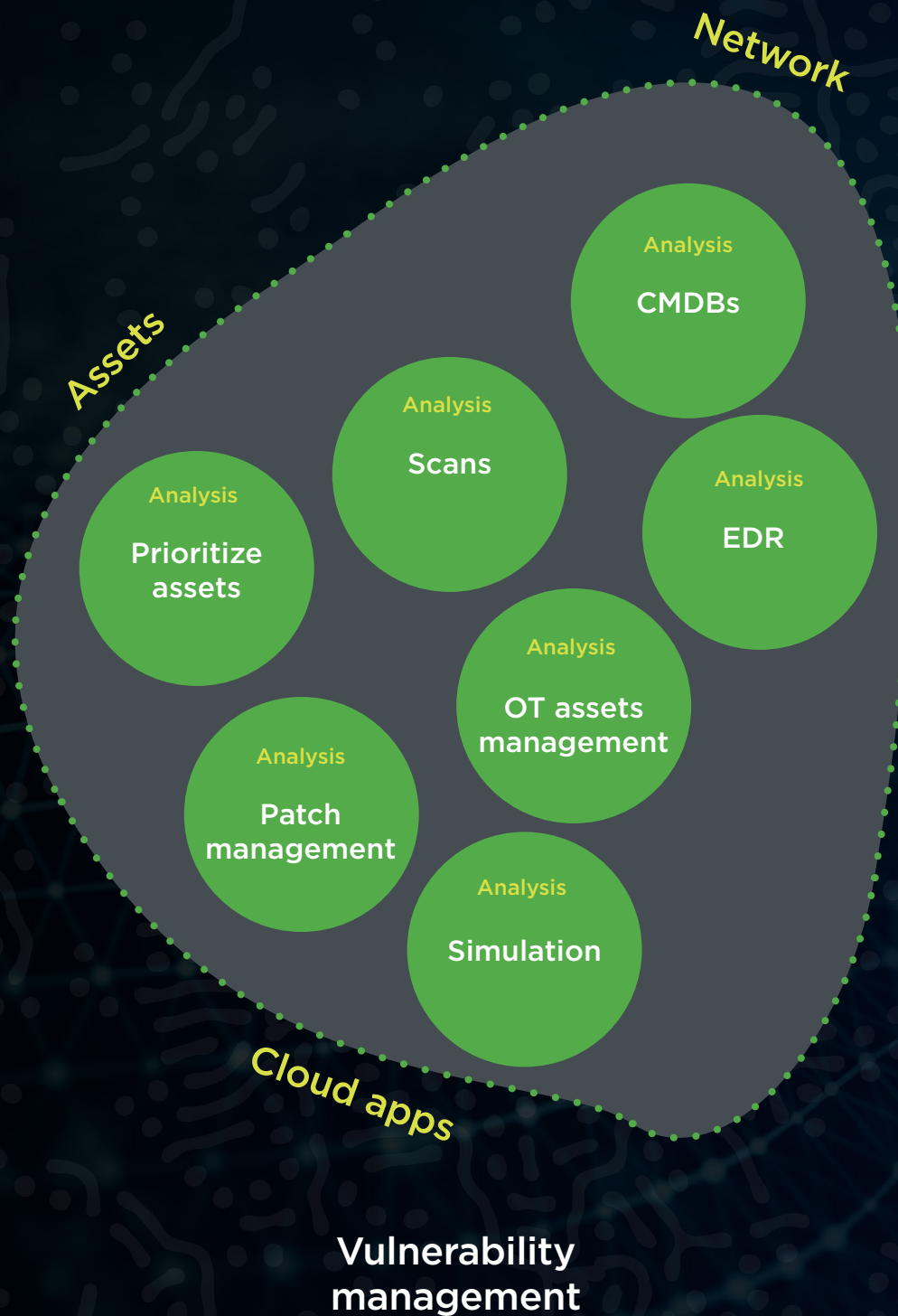
Cybersecurity lifecycle
management across
typical enterprise
organizations



Firewalls, IPS, Sandboxing, EDR, XDR, SIEM, SOAR, etc.

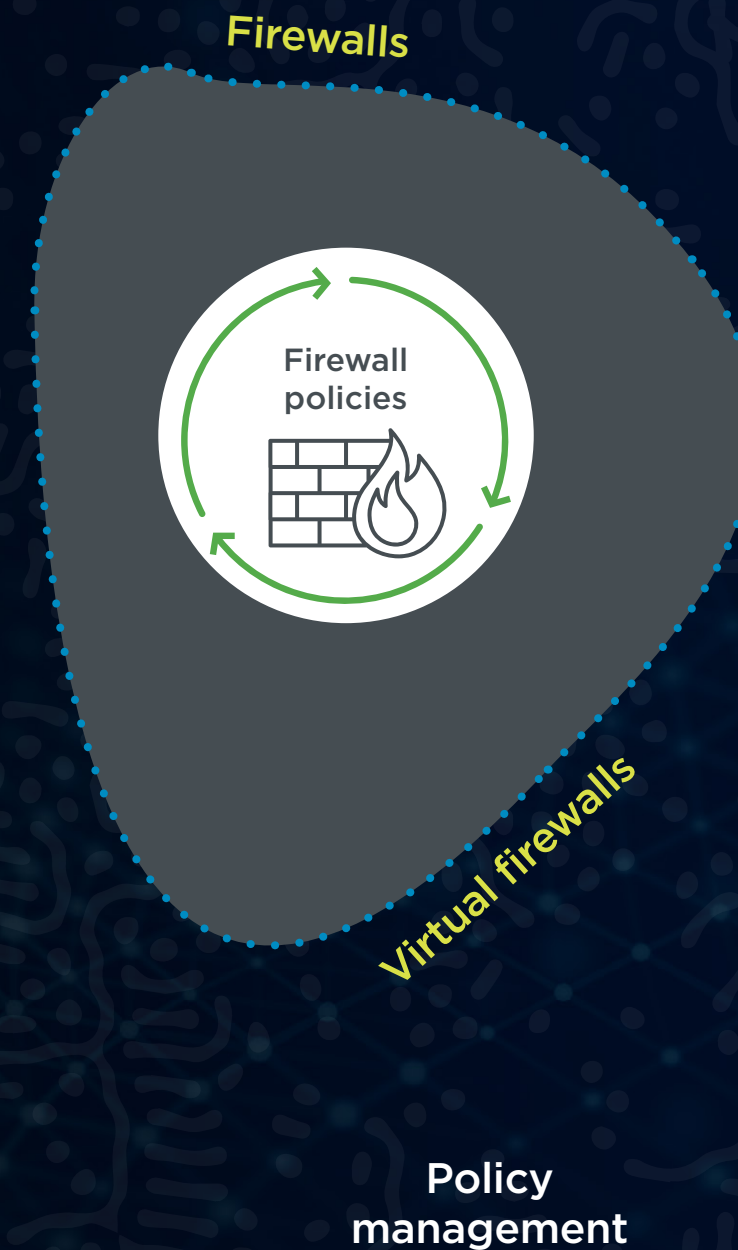
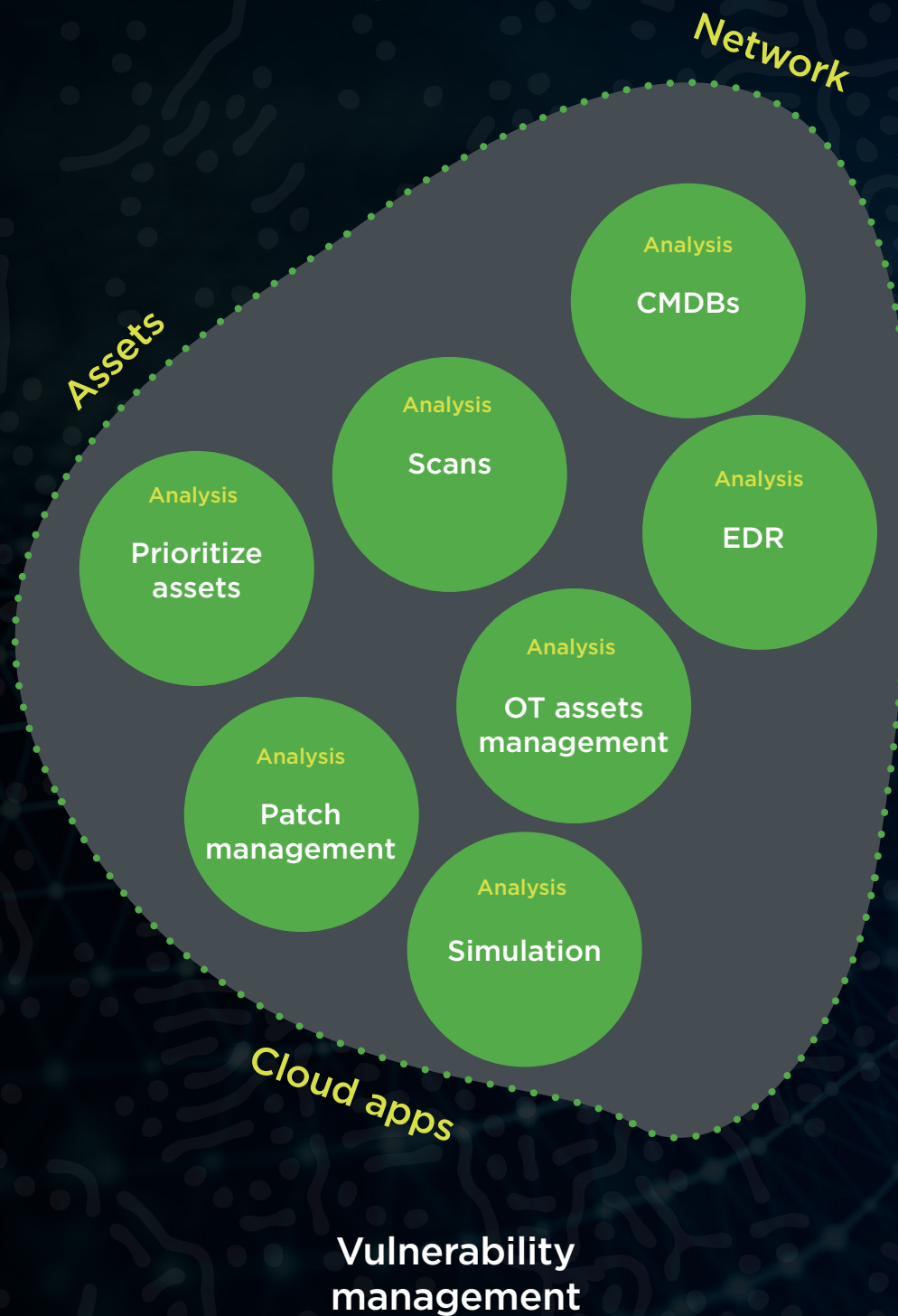
The 3 challenges to reach best practices in policy management

When security and network data are restricted in silos, companies are denied the collaboration and context needed to safely automate necessary changes to their cybersecurity landscapes. The result is blind change management.



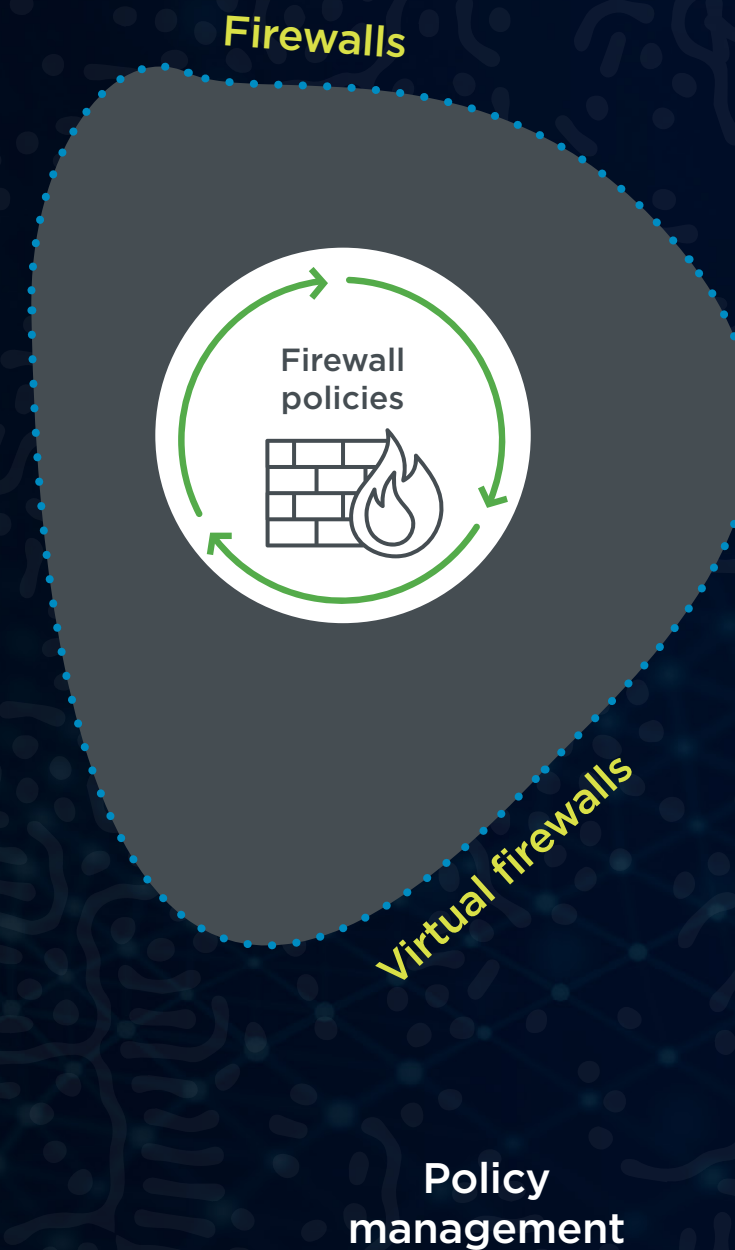
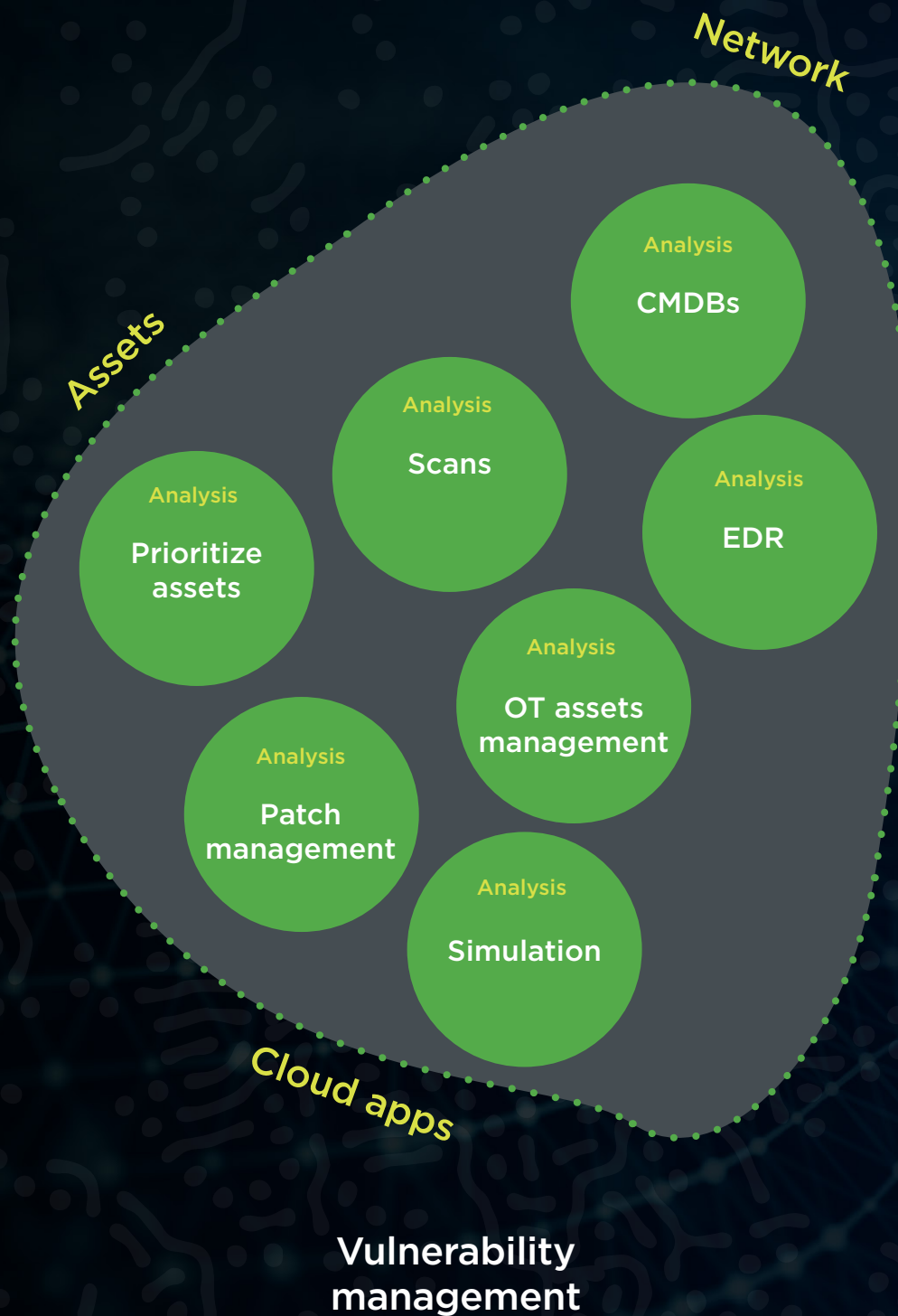
The 3 challenges to reach best practices in policy management

In the absence of a complete understanding of an enterprise's attack surface, security teams may have to deal with an over-reliance on reactive security measures.



The 3 challenges to reach best practices in policy management

Accurately validating new policies is essential. The lack of context necessary to do this can result in the unintentional introduction of new vulnerabilities with each new policy and rule deployment.





What to look for in a context-aware change management solution



Look to break down
organizational silos so that teams
can share data and analytics



What to look for in a context-aware change management solution



Verify the integrity of your
ongoing policy changes before
they are put into action



What to look for in a context-aware change management solution



Get a complete view of the
current state of the entire
infrastructure across physical IT,
multi-cloud and OT networks



What to look for in a context-aware change management solution

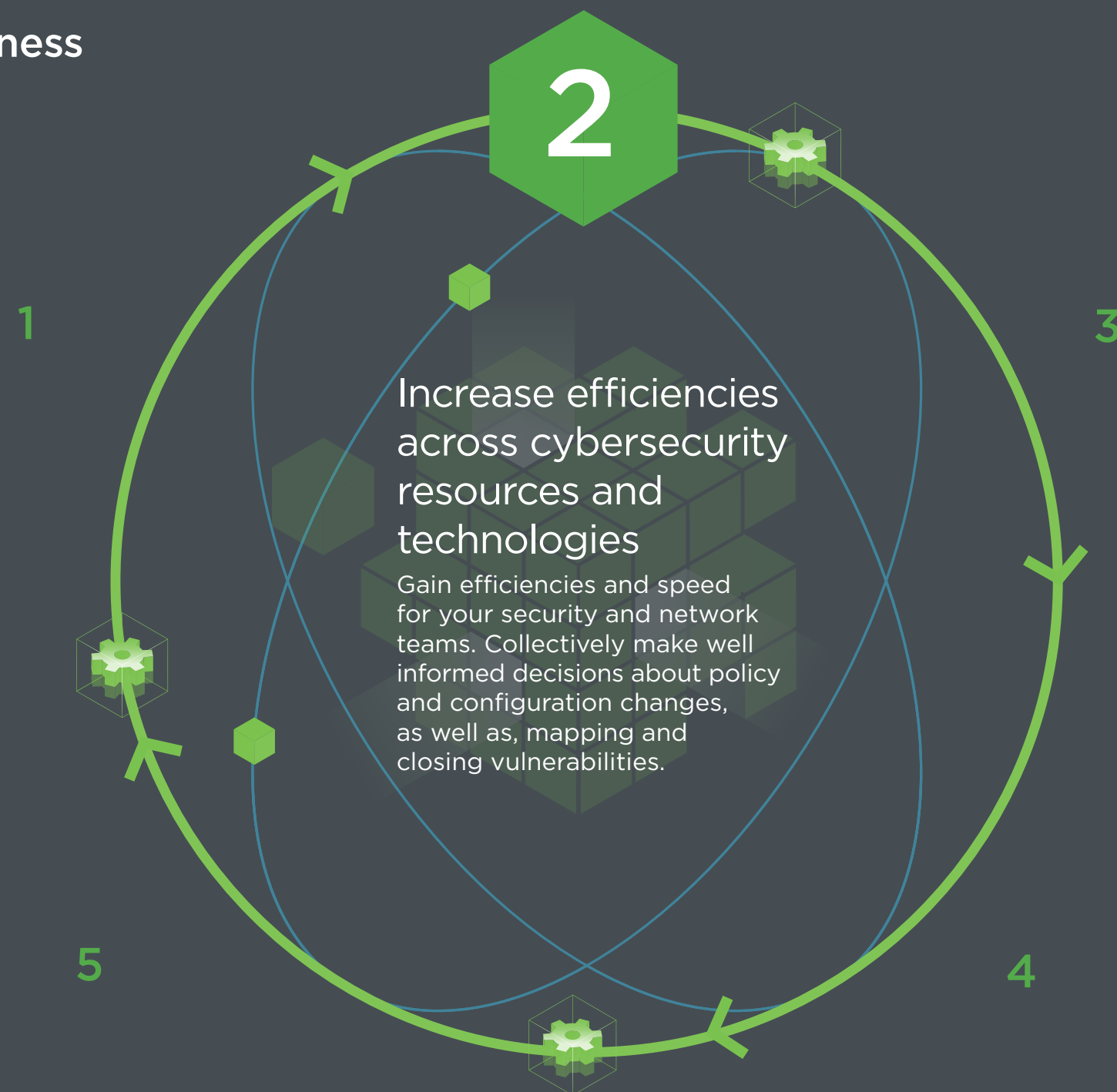


Analyze the potential for new
policy releases to expose
unforeseen vulnerabilities across
your network

Best practice business goals for policy management



Best practice business goals for policy management



Best practice business goals for policy management



Best practice business goals for policy management



Best practice business goals for policy management





Benefits of moving to context-aware policy management with Skybox

Gain a full understanding of attack surface before making policy changes



Context-aware policy management enables the merging and analyzing of data sets across the security, network, and cloud technologies. This allows for security and network teams to collaborate in order to gain an end-to-end understanding of the attack surface.



Benefits of moving to context-aware policy management with Skybox

Gain a full understanding of attack surface before making policy changes

Validate policies and rules with full network context prior to implementation

Proactively simulate policy changes to mitigate vulnerability exposure



By testing policy changes and new configurations before deployment, teams can get visibility on security issues that these changes may cause.



Benefits of moving to context-aware policy management with Skybox

Gain a full understanding of attack surface before making policy changes

Validate policies and rules with full network context prior to implementation

Proactively simulate policy changes to mitigate vulnerability exposure



Don't expose your network to unanticipated vulnerabilities with every policy change. Instead, establish a strong security lifecycle management approach that utilizes network context and wide-ranging remediation options. This gives security teams insights and tools to recognize policies quickly and effectively.



Your pathway to achieve comprehensive context-aware change management

Step 1:

Closed-loop
security lifecycle
management

STEP 2

STEP 3



Implement automated closed-loop workflows for firewall rule creation, recertification, and deprovisioning that help close security gaps, limit vulnerability exposures, and maintain continuous compliance.



Your pathway to achieve
comprehensive context-aware
change management

STEP 1

Step 2:

Unified security
and network
modeling

STEP 3



Ensure newly created policies
and controls enable connectivity
with the appropriate network
context to avoid exposing the
organization to attack vectors
or compliance violations.



Your pathway to achieve
comprehensive context-aware
change management

STEP 1

STEP 2

Step 3:

Exposure
analysis
and attack
simulation



Leverage insights from network topology and security controls that either protect or expose vulnerability assets, and prioritize exposed vulnerabilities that require immediate remediation.

Let's work together

The ongoing evolution of your enterprise infrastructure is fast-paced, and it demands a dynamic approach to its security to match it. As policies change, technology landscapes evolve and integrate with cloud-native solutions, and agile development is adopted; you need to have full visibility and context across your frameworks and areas that need safeguarding the most.

Skybox provides a collaborative environment necessary for your teams to efficiently manage the unpredictable challenges of enterprise security.

See around corners and intelligently plan your response.