Securing User to Application and Everything in Between

Tom Gillis, SVP/GM Cisco Security

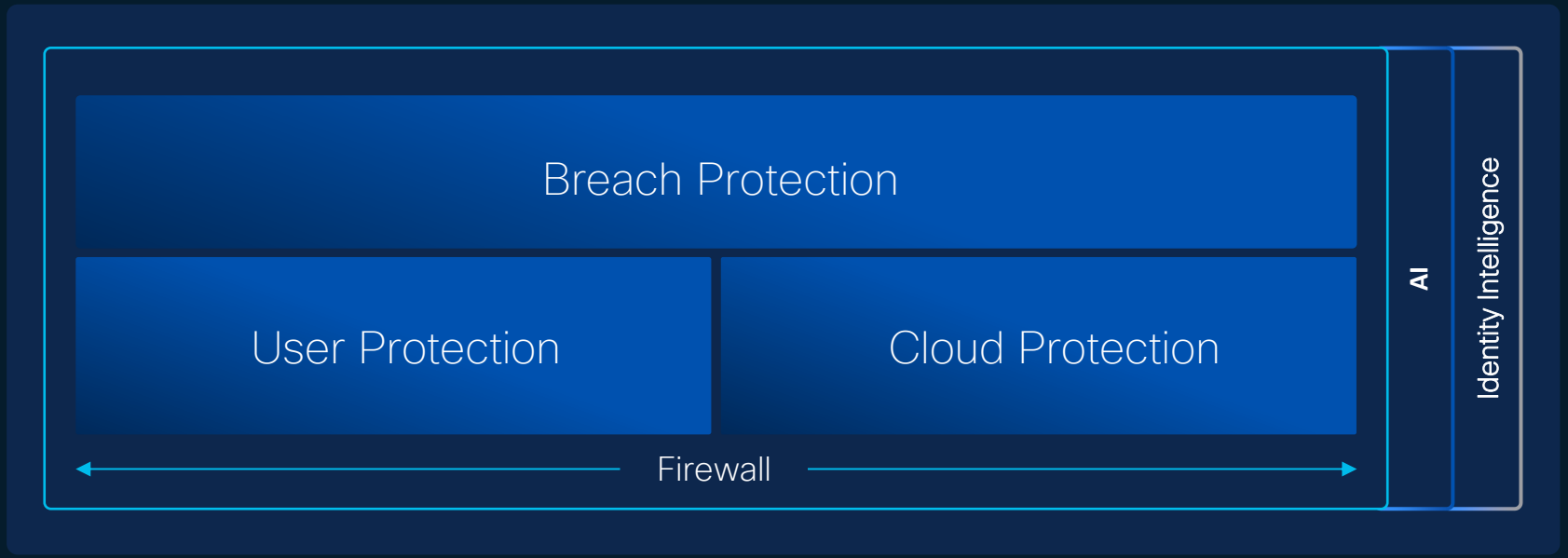
KDDSEC-1000

cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Security Cloud



Supercharged by **Splunk**

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

You've heard this story before.
We just rewrote it.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

One client, multiple functions

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Seamless Access

We handle the plumbing

Go to work

Private Apps

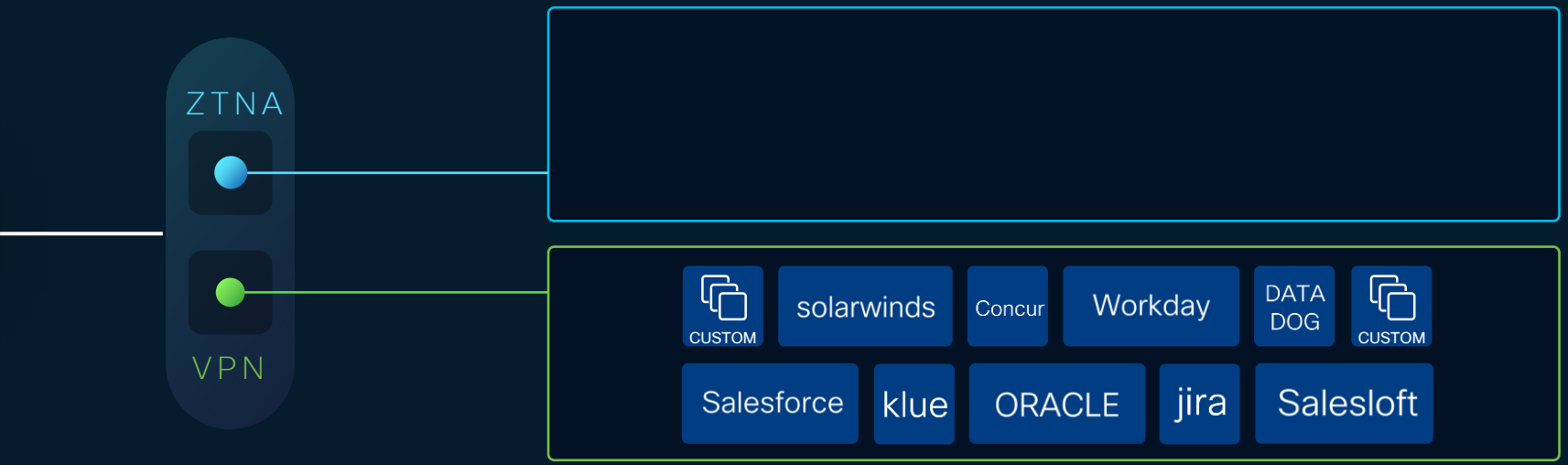
Internet Apps

Traditional Apps

SaaS Apps

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

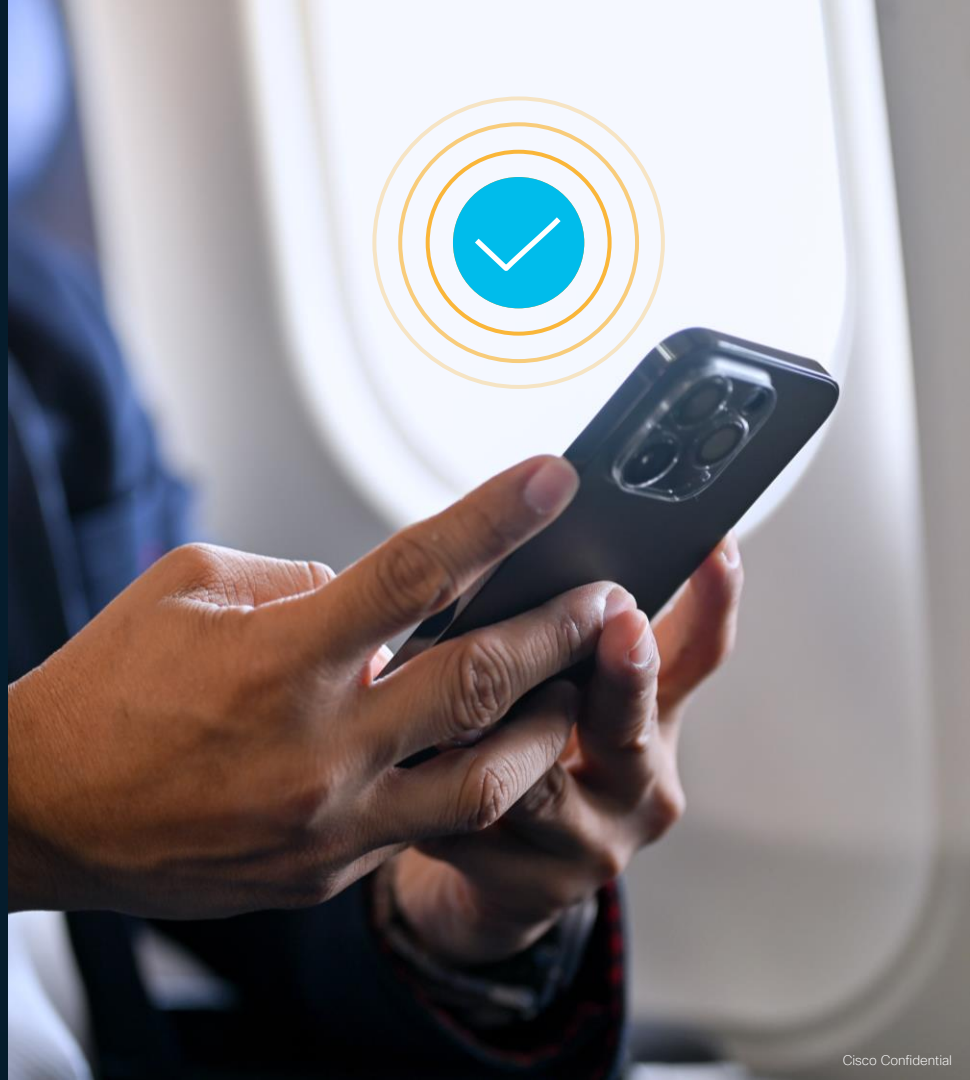
Seamless Experience



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Performance for low latency applications wherever you need it

3X faster than VPN



Cisco Confidential

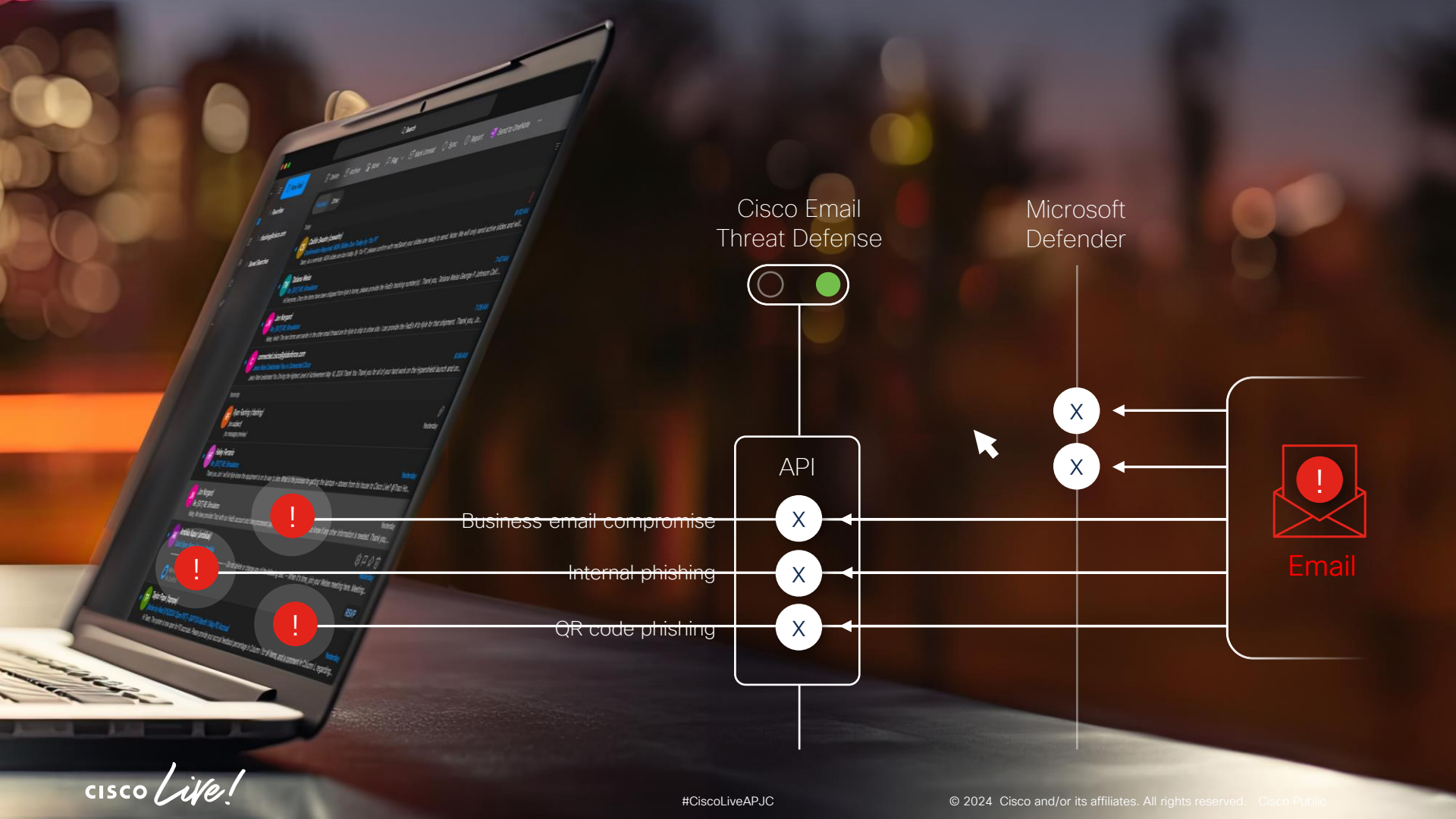
CISCO

Secure Access

REPLACES

Security Service Edge

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

MICROSOFT

Defender

CISCO

Email Threat Defense

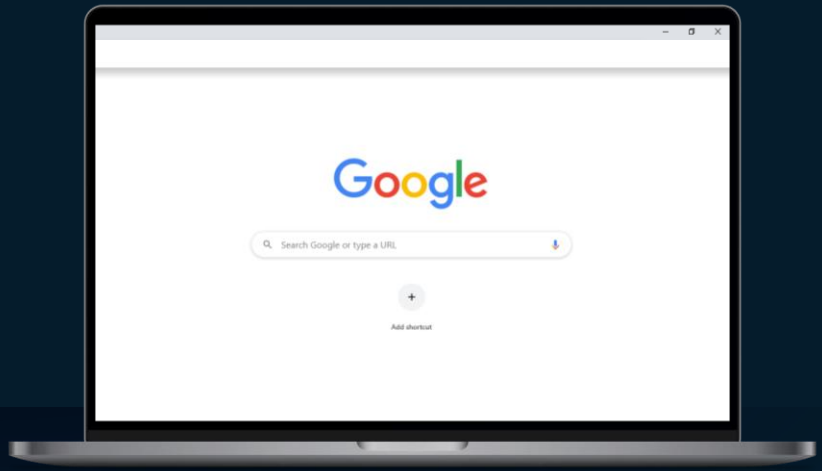
REPLACES

Secure Email Gateways

Point BEC Products

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



Enterprise Browser

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

GOOGLE

Chrome Enterprise

CISCO

Secure Access

REPLACES

Enterprise Browser

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity is the new spam.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity Intelligence

Authentication

Access

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SailPoint

Dragos

Crowdstrike

Salesforce

Cisco ISE

Okta

PingIdentity

Auth0

Microsoft

Google

Cyberark

Amazon

cisco Live!

and/or its affiliates. All rights reserved. Cisco Public

“Things are people too…”
USERS
MACHINES
SERVICES
HRIS
DATA
APPS
PLATFORMS
Cisco Identity Intelligence

Frustrate attackers, not users.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

MICROSOFT

Active Directory

CISCO

MFA & Posture

REPLACES

Point ITDR Products

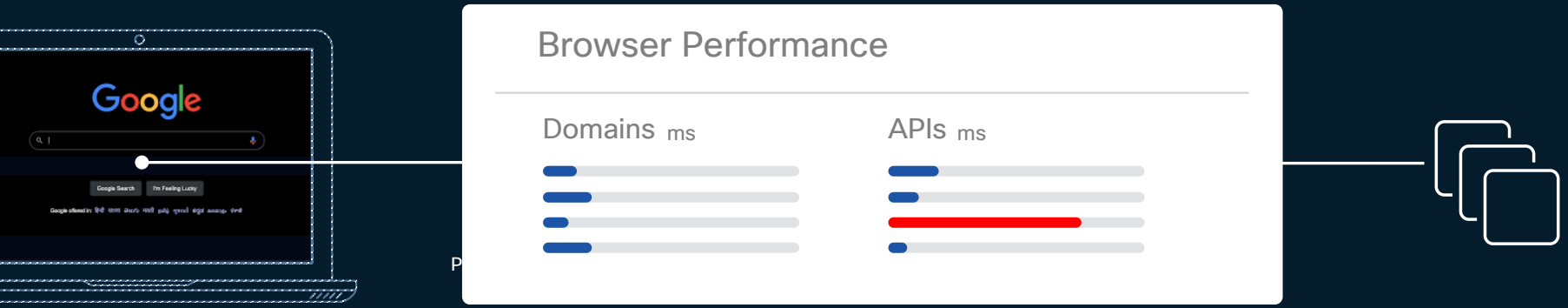
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

We deliver a great end user experience. And we measure it.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

End-to-end Visibility



Depictions are examples only.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

CISCO

ThousandEyes Client

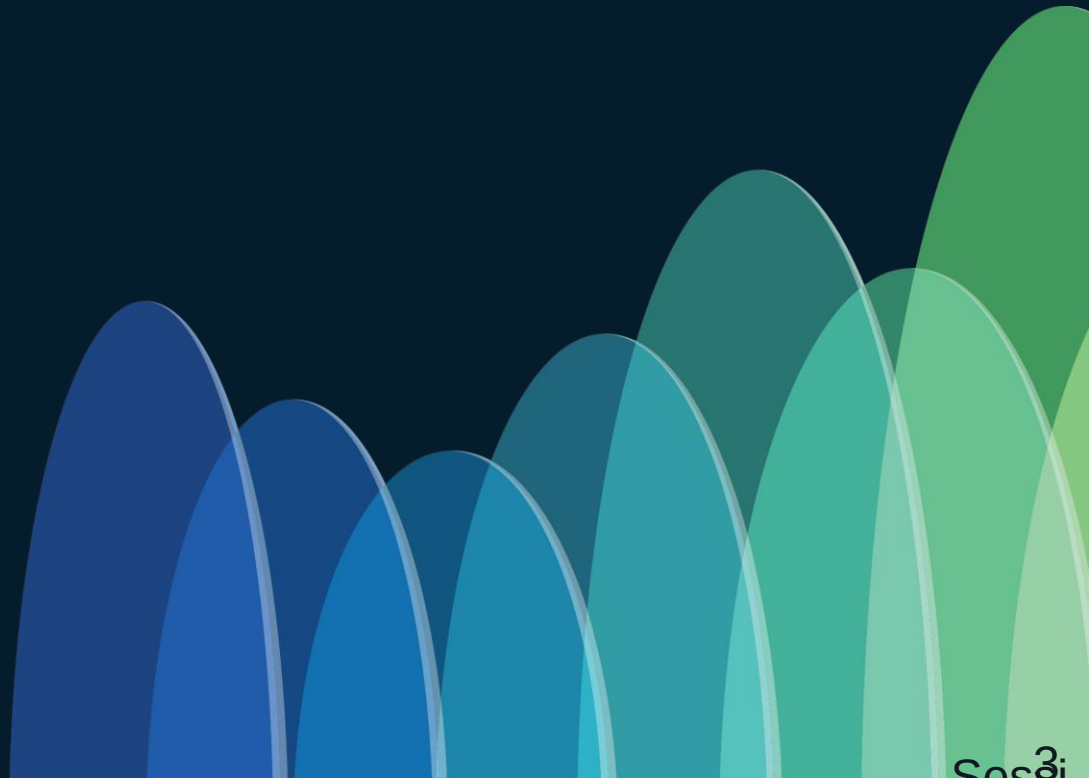
REPLACES

Service assurance tools

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Customer perspectives



Changing the fundamentals of data center security.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SOFTWARE DEFINED
INFRASTRUCTURE

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Not the next gen of anything.

The incumbent network fabric

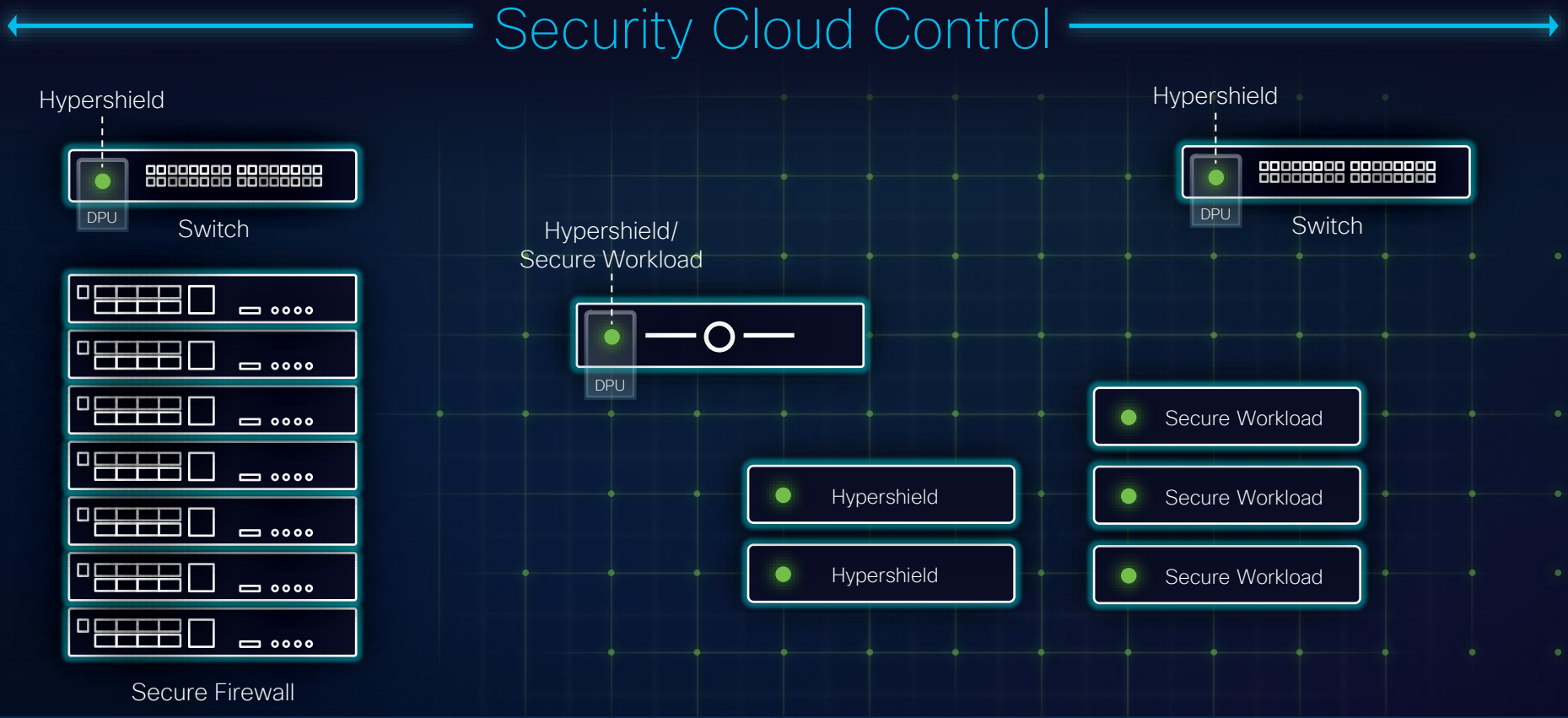
It's the first generation of something new.

Agentless

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

No rip and replace

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



Enforcement points change, rules don't

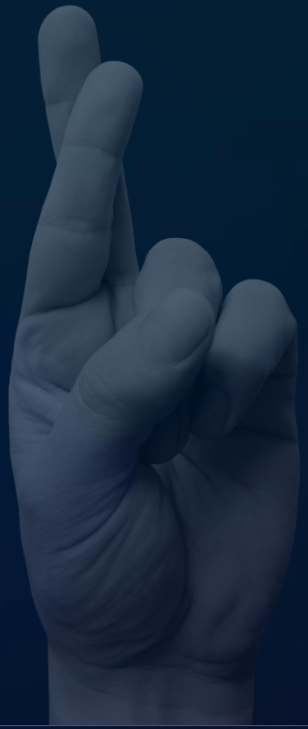
Stopping lateral movement
Segmentation That Works

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

40+

days to segment
an application

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

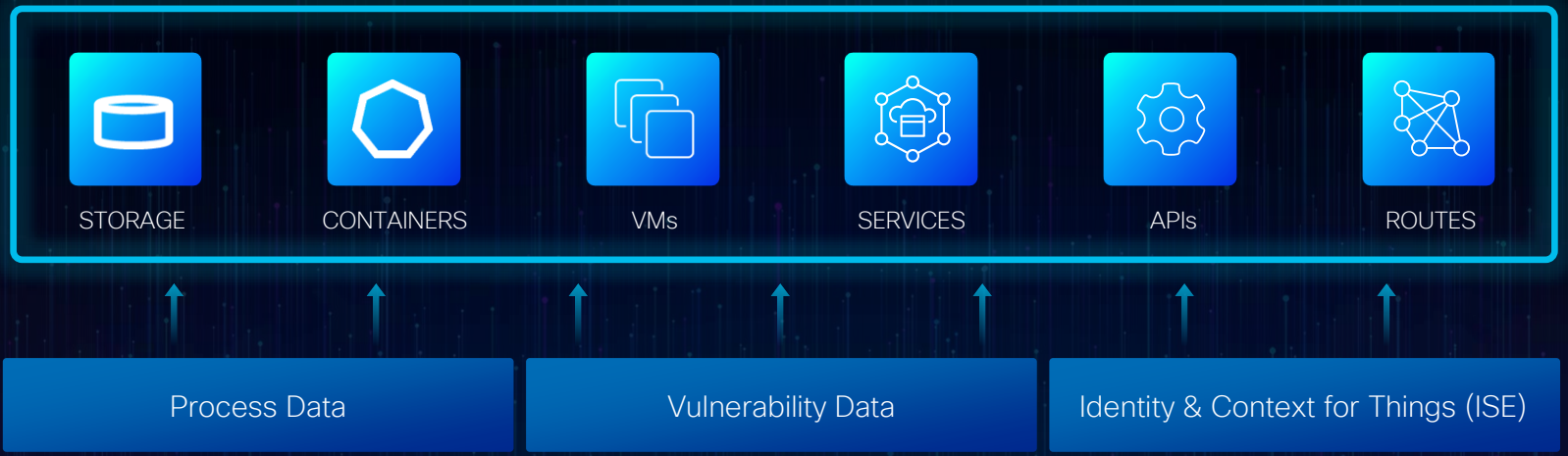


ACCURACY

TIME

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

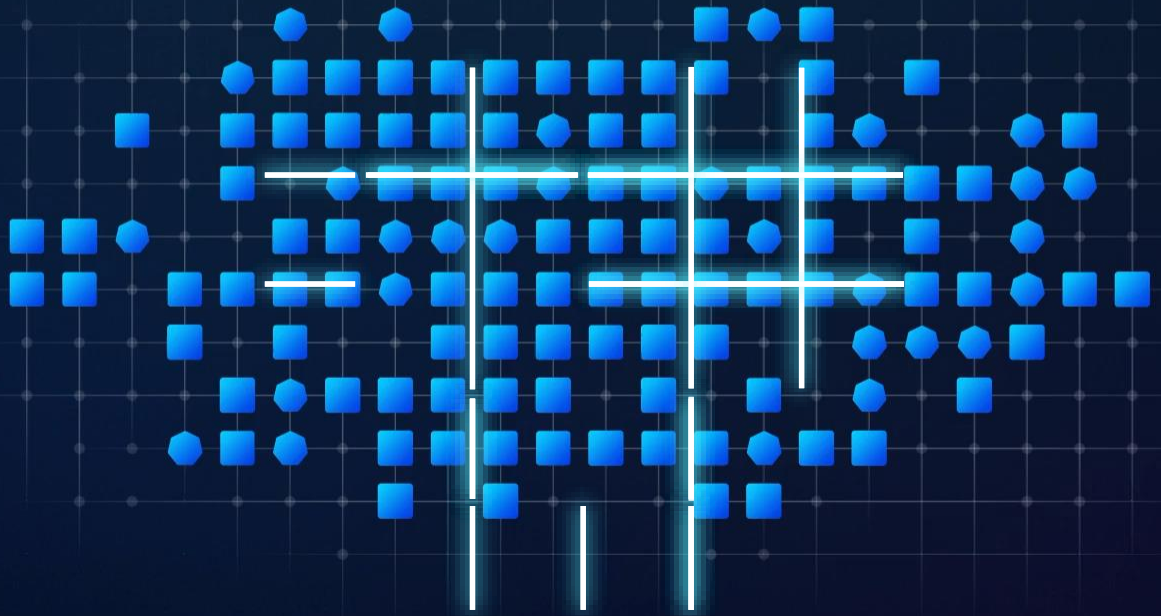
Unprecedented Visibility



APIs | Posture | Assets | Users | Devices | Hosts | Connections | Real-time app changes

2 million flows/second, near real-time

CONFIDENCE



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

CISCO

Segmentation

REPLACES

Microsegmentation point products

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

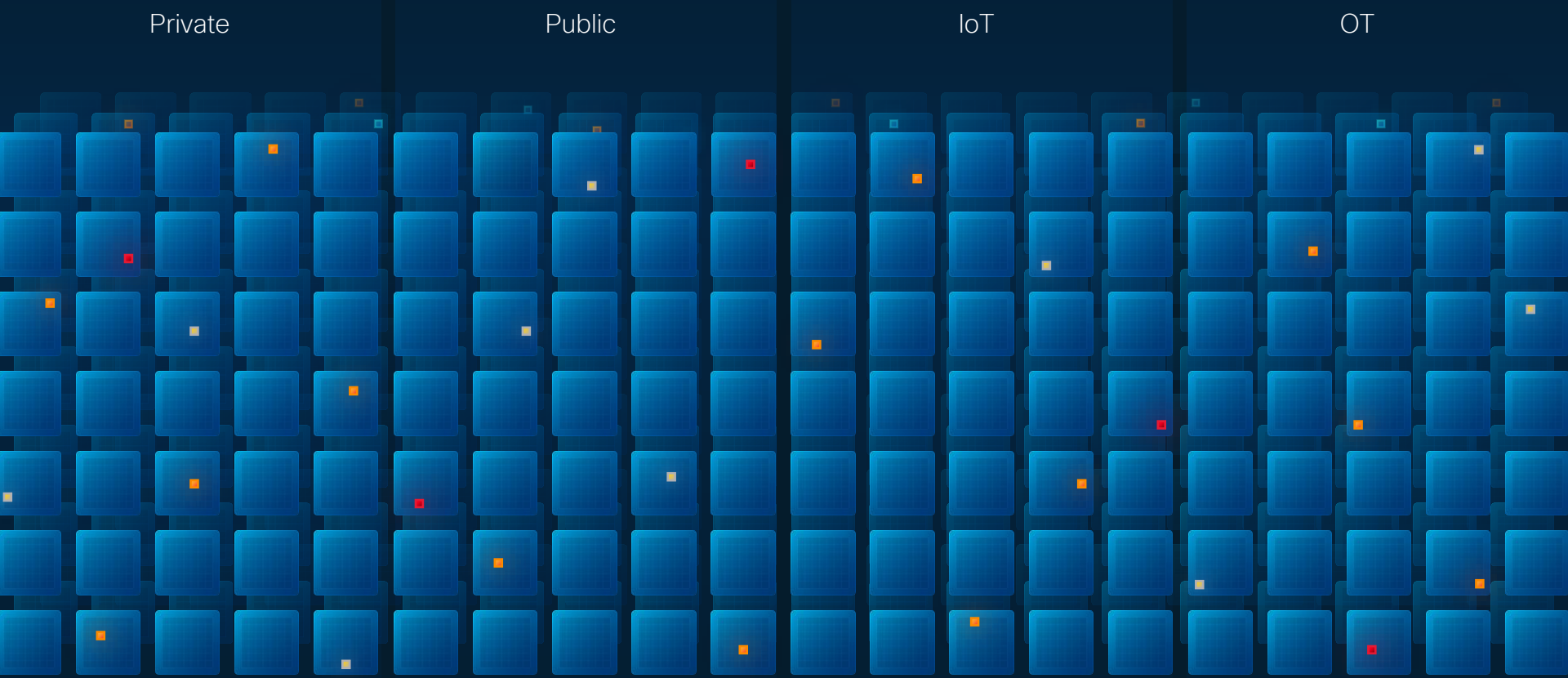
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Compensating controls
Distributed Exploit Protection

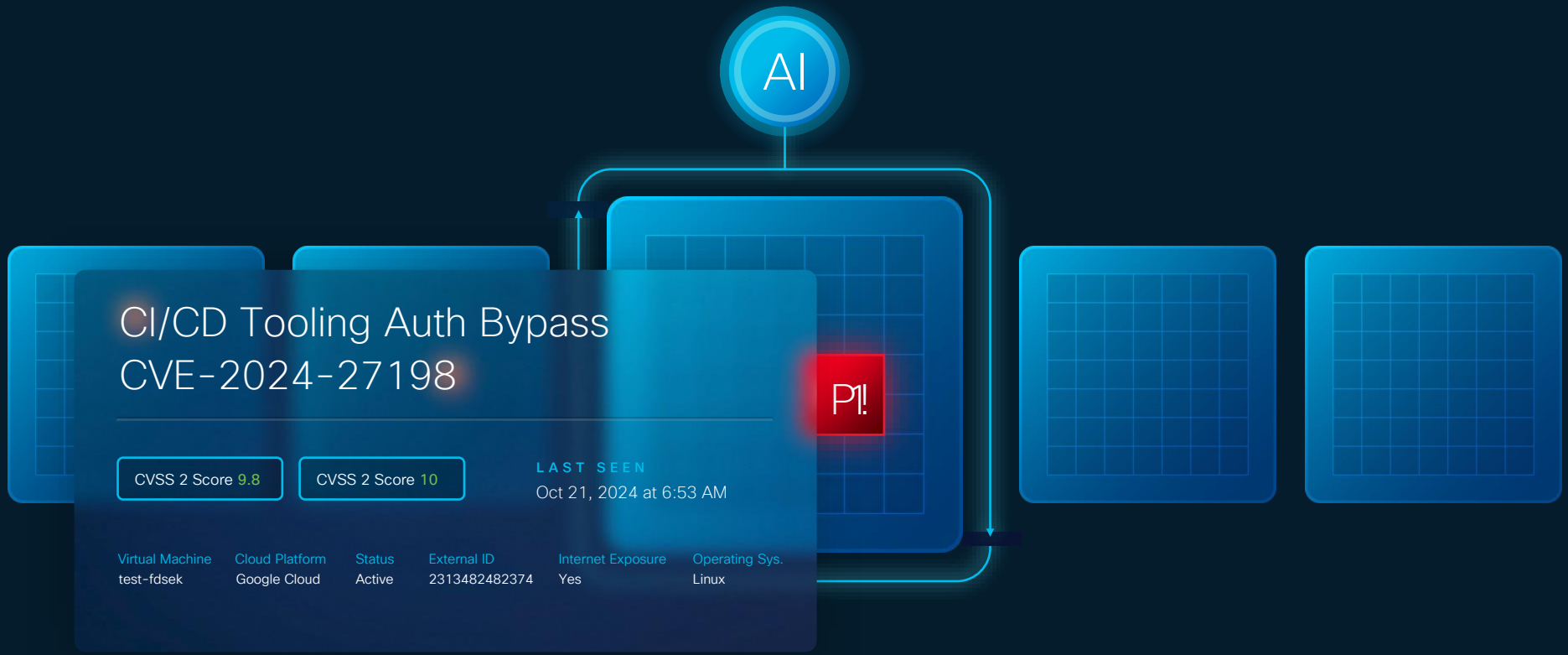
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Is it running in memory? | Is it being exploited in the wild? | Is it a high value asset?

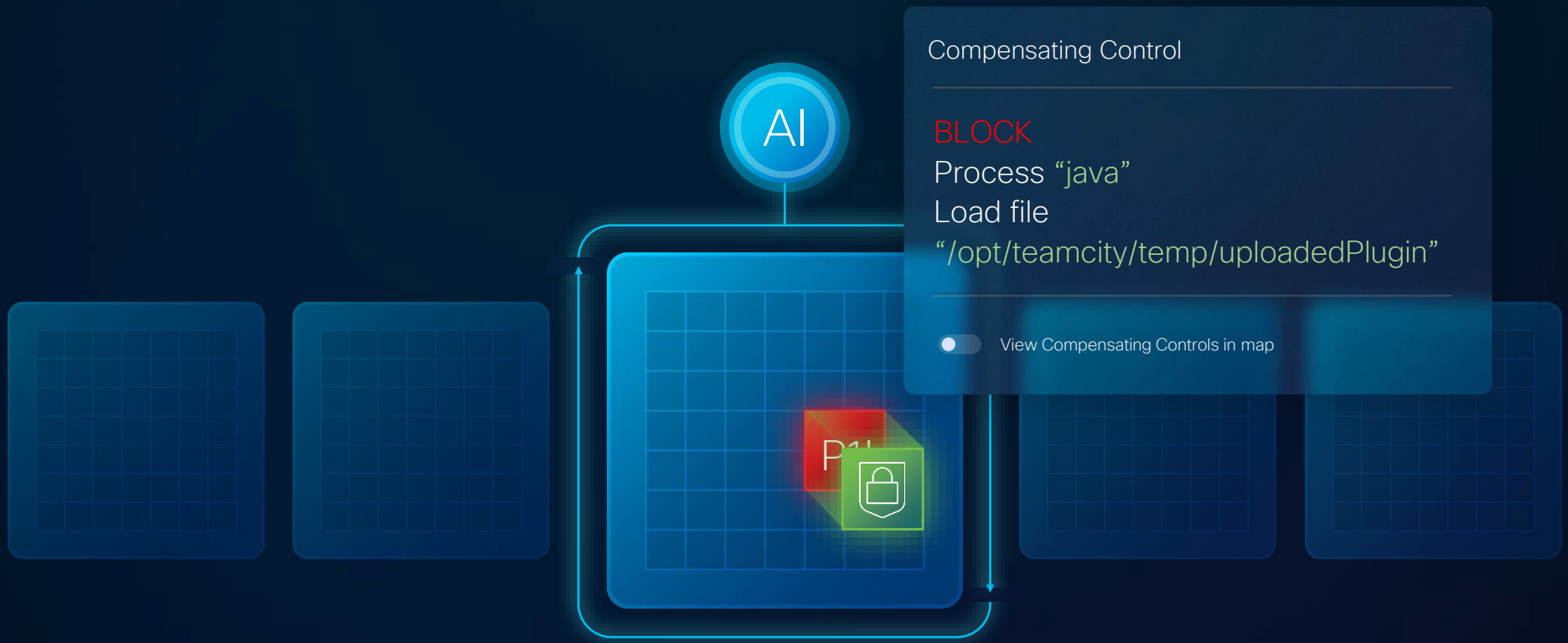
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

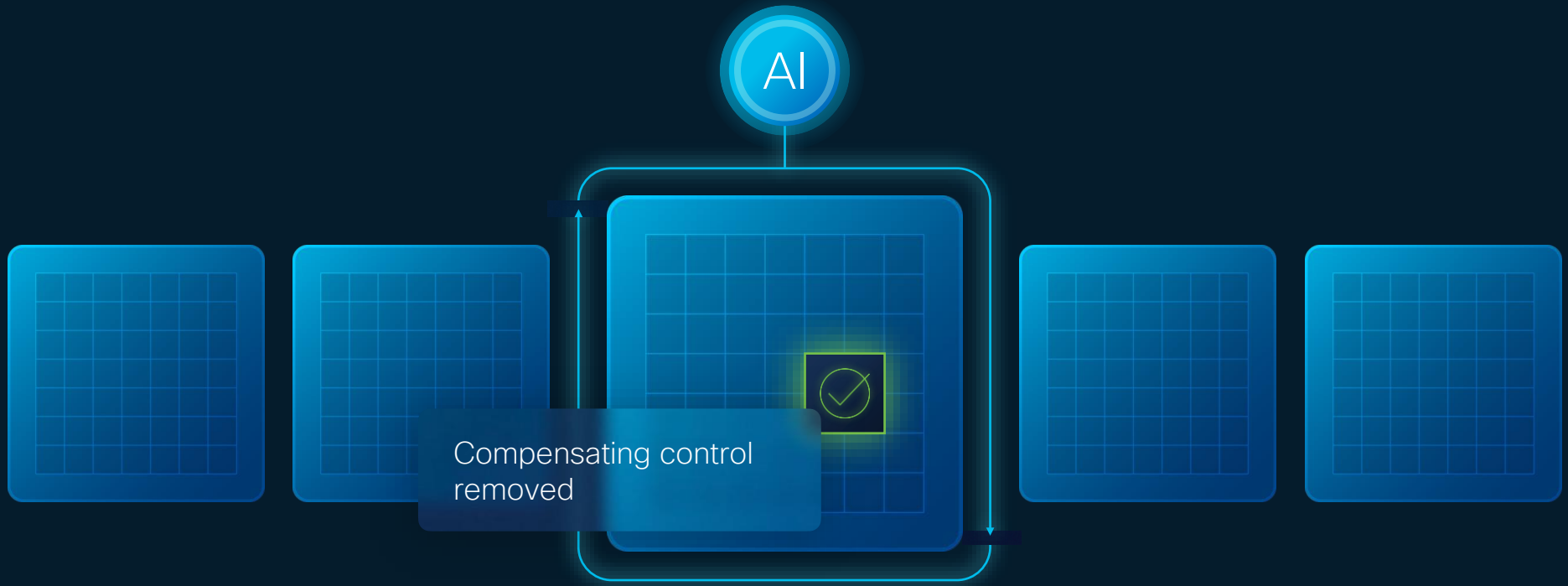


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



Perfect fit | Tested against real world traffic | Optimal placement

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

CISCO

Distributed Exploit Protection

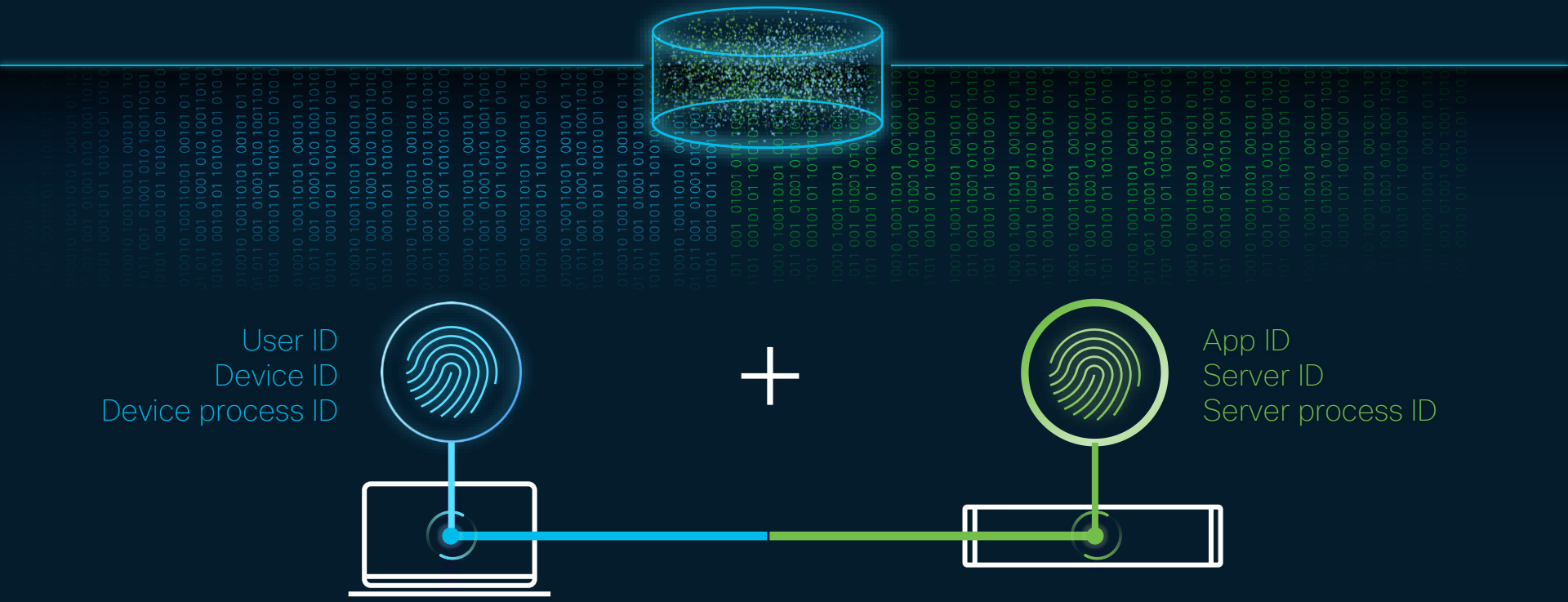
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Powering the SOC of the future.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SIEM / SOAR / ANALYTICS

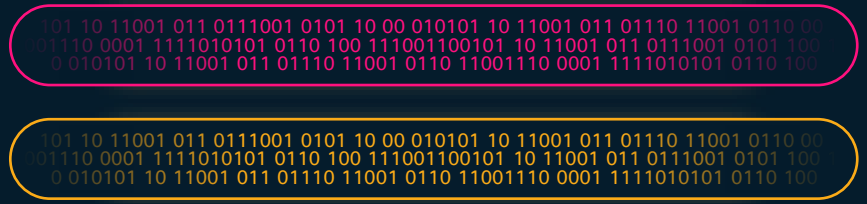


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

splunk>

SIEM / SOAR



ANALYTICS

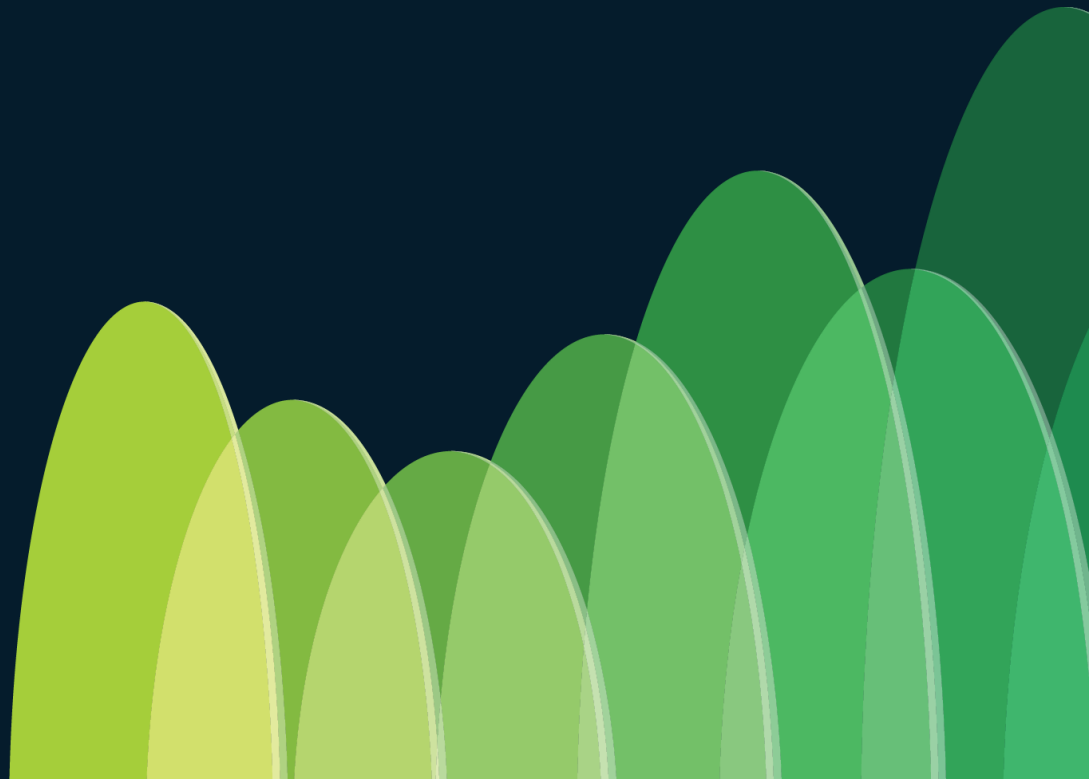
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

splunk>
SIEM / SOAR
ANALYTICS
FUTURE
User
Device
IoT / OT / Edge
Private
Public

Robert Pizzari

Group Vice President

Splunk



cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Innovations to Transform Security Operations

Power the SOC of the future

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk Recognized as a Leader

2024 Gartner® Magic Quadrant™ for Security Information and Event Management (SIEM)

Splunk named a **Leader** for the **10th consecutive time**

GARTNER is a registered trademark and service mark of Gartner and Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Splunk.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk powers the **SOC of the future**

Enterprise Security

SOAR

Attack Analyzer

Asset and Risk Intelligence

Embedded AI

Content and threat research

User/Cloud/ Breach/XDR

Networking

Third-party tools

Talos

Clouds

Devices

Data centers

Applications

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

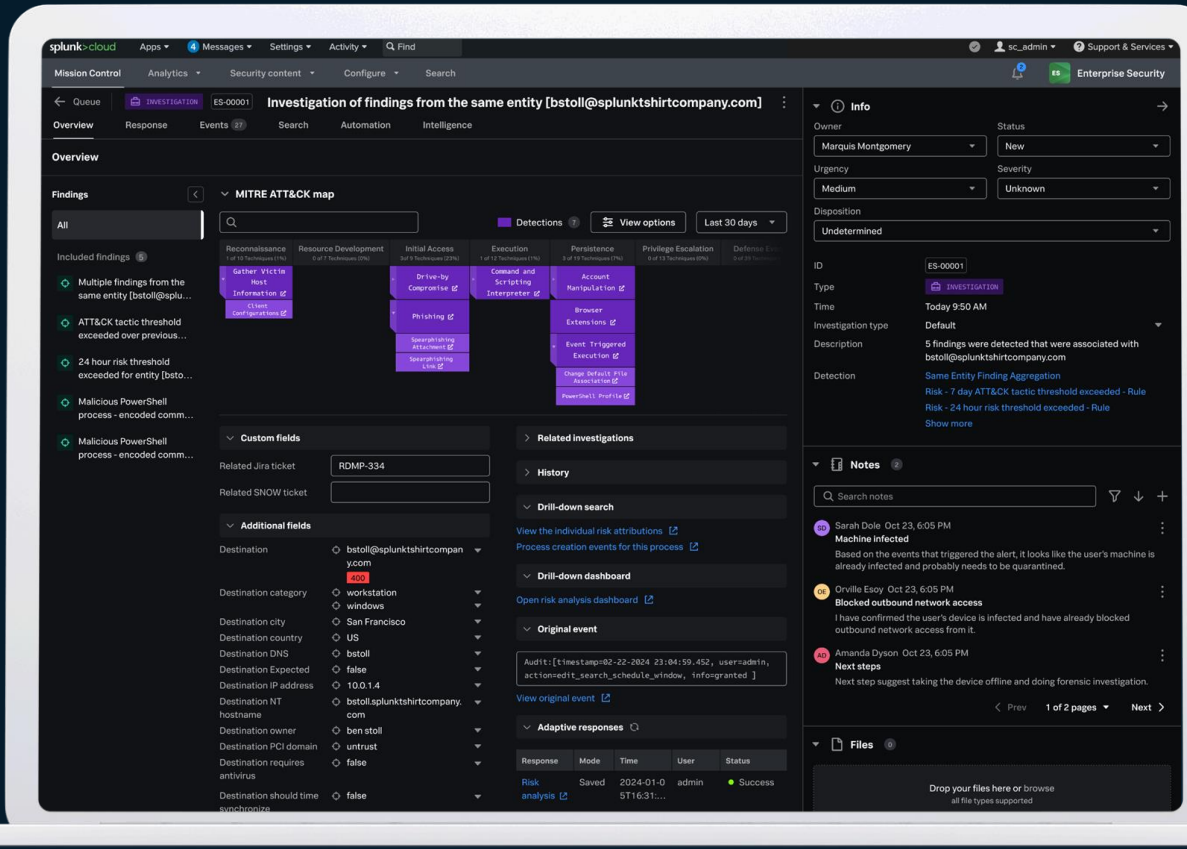
The SOC of the future will be federated and distributed.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk Enterprise Security 8.0

The Market-Leading SIEM to Power the SOC of the Future

- Handle full TDIR workflows from start to finish
- Native Splunk® SOAR integration
- Enhanced detection engineering capabilities



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

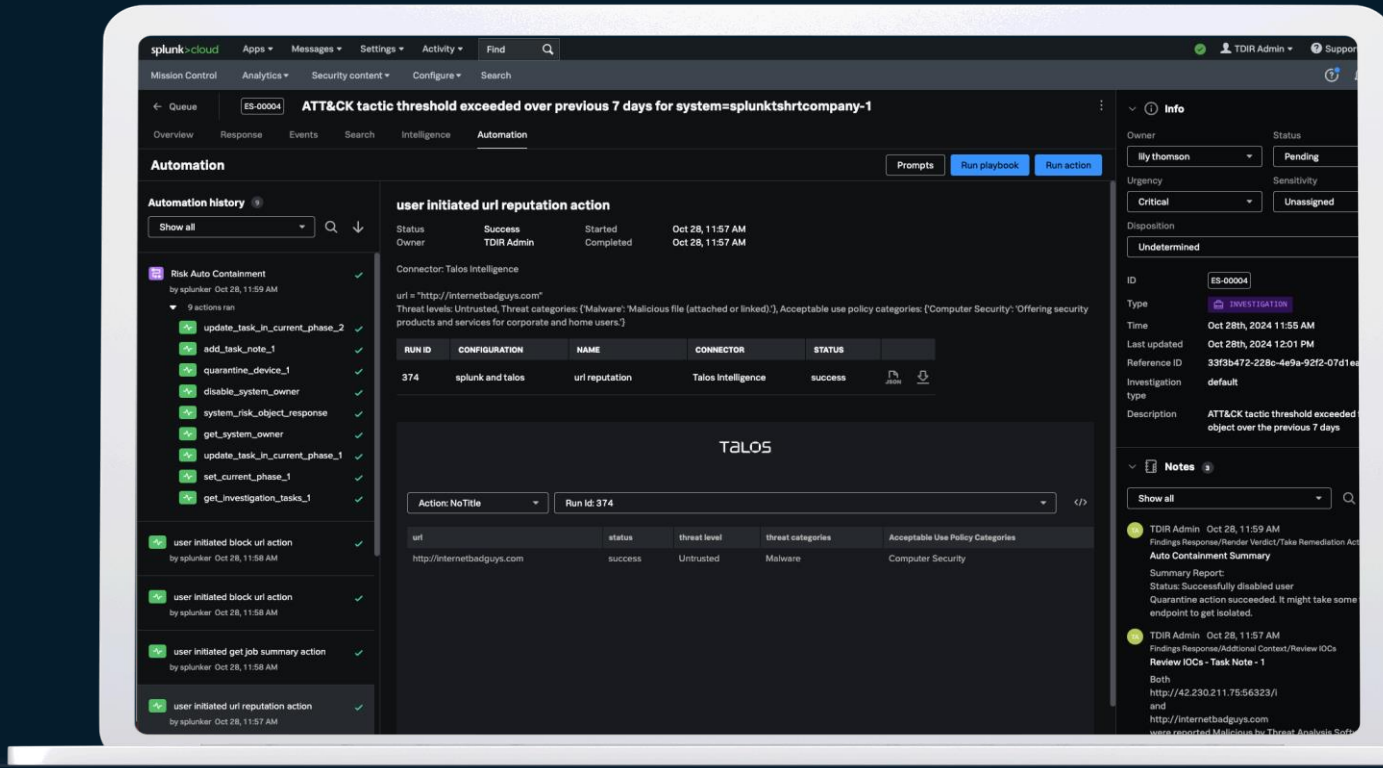
Cisco XDR

Email	DNS	Endpoint	Network
Every email	Every web request	Every process	Every flow

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Talos Integration

Threat intelligence to enrich TDIR workflows within Splunk Attack Analyzer



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What's Next?

Better Technical Add-ons

Talos Integration with ES and SOAR

AI Assistant in ES

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Apple Watch SE

Look under your seat for a winning ticket!

If you are a winner, please see a team member at the front of the room to collect your prize after this session.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC