



Securing User to Application and Everything in Between

Tom Gillis, SVP/GM Cisco Security

KDDSEC-1000

CISCO *Live!*

#CiscoLiveAPJC



CISCO *Live!*

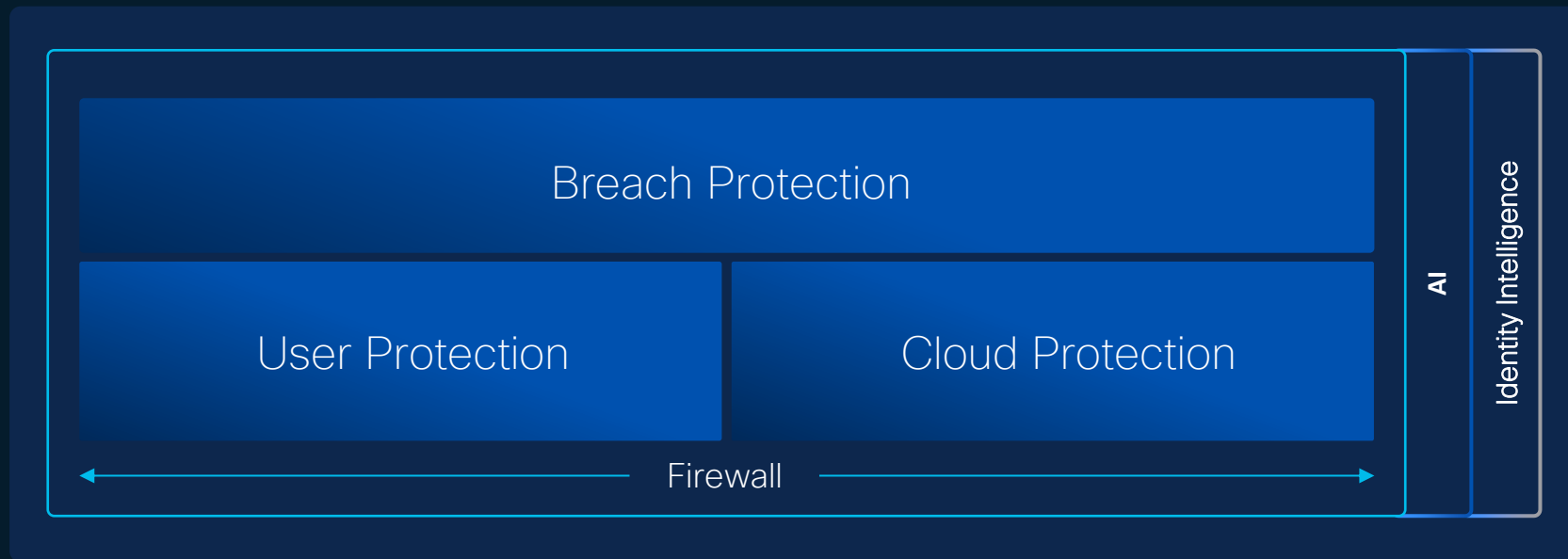
#CiscoLiveAPJC

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

HeartSync Pacemaker



Cisco Security Cloud



Supercharged by **Splunk**

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

One client, multiple functions



Seamless Access

We handle the plumbing

Go to work



Private Apps



Internet Apps

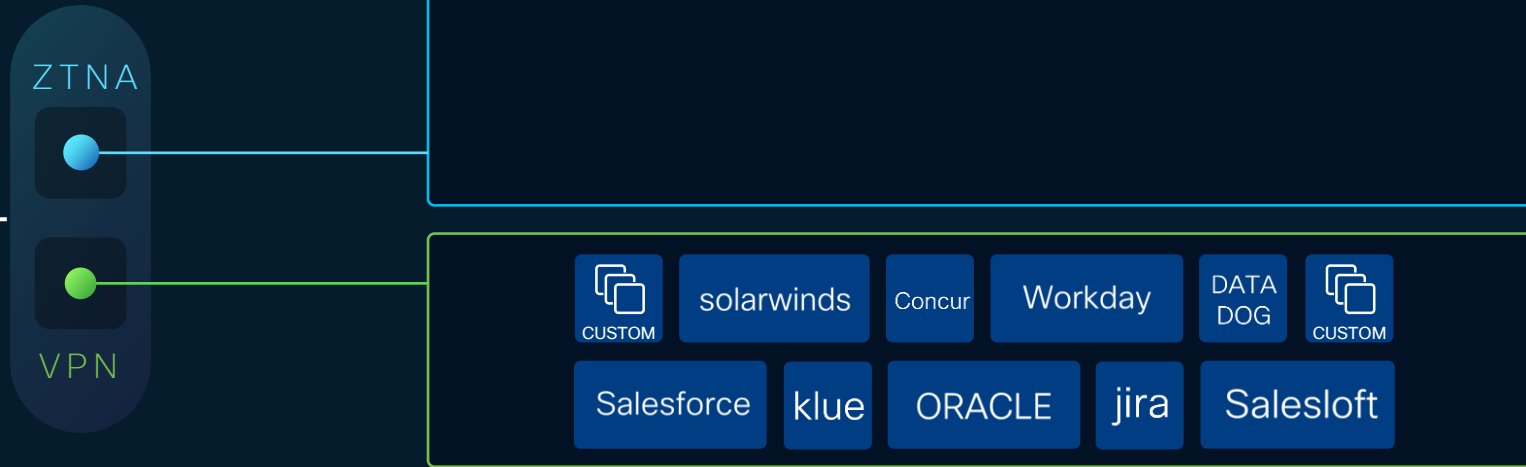


Traditional Apps



SaaS Apps

Seamless Experience

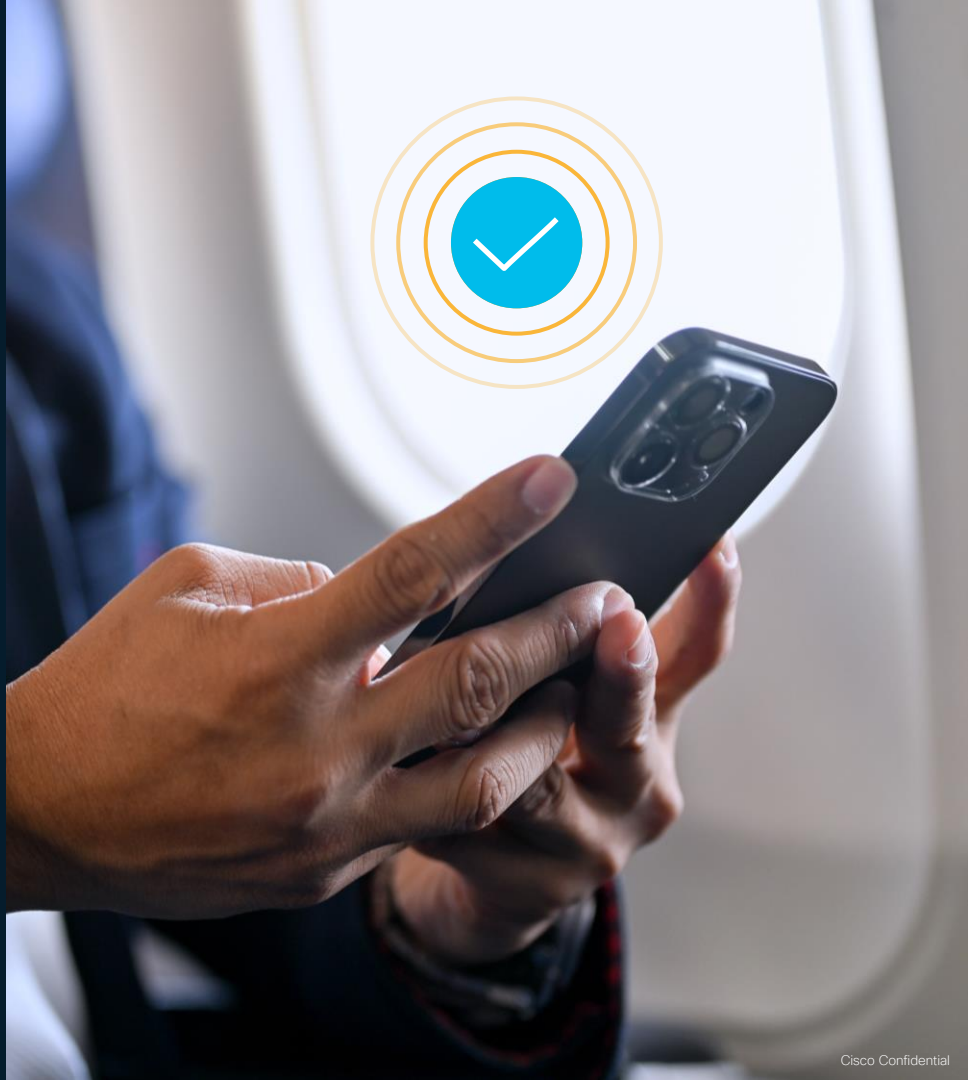


Performance for low
latency applications
wherever you need it



3X faster than VPN

CISCO *Live!*



CISCO

Secure Access

REPLACES

Security Service Edge





Cisco Email
Threat Defense

Microsoft
Defender



API



Email

Business email compromise

Internal phishing

QR code phishing

CISCO *Live!*

#CiscoLiveAPJC

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

MICROSOFT
Defender



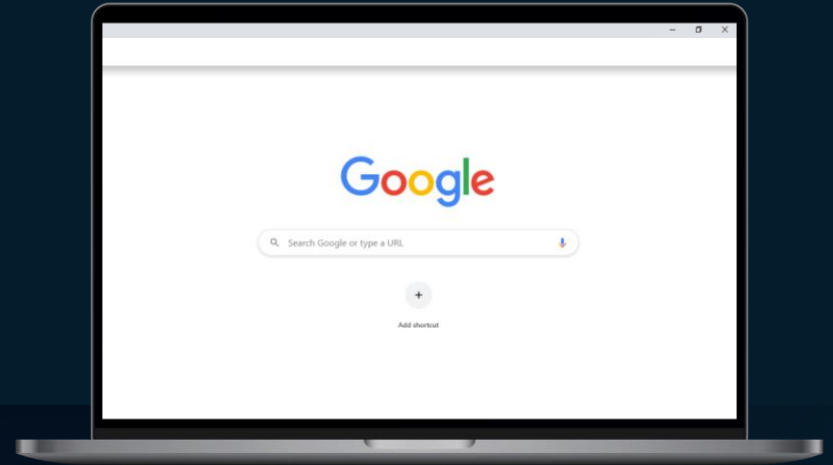
CISCO
Email Threat Defense

REPLACES

Secure Email Gateways

Point BEC Products





Enterprise Browser

GOOGLE
Chrome Enterprise



CISCO
Secure Access

REPLACES

Enterprise Browser



Identity is the new spam.

Identity Intelligence



Authentication

Access

SailPoint

Dragos

CrowdStrike

Salesforce

Okta

PingIdentity

Cisco ISE

Auth0

Cyberark

Microsoft

Google

Amazon

Cisco Identity Intelligence



USERS



MACHINES



SERVICES



HRIS



DATA



APPS



PLATFORMS



SailPoint

Dragos

CrowdStrike

Salesforce

Cisco ISE

Okta

PingIdentity

Auth0

Microsoft

Google

Cyberark

CISCO *Live!*

#CiscoLiveAPJC

Amazon

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



Cisco Identity Intelligence

Frustrate attackers, not users.



MICROSOFT
Active Directory



CISCO
MFA & Posture

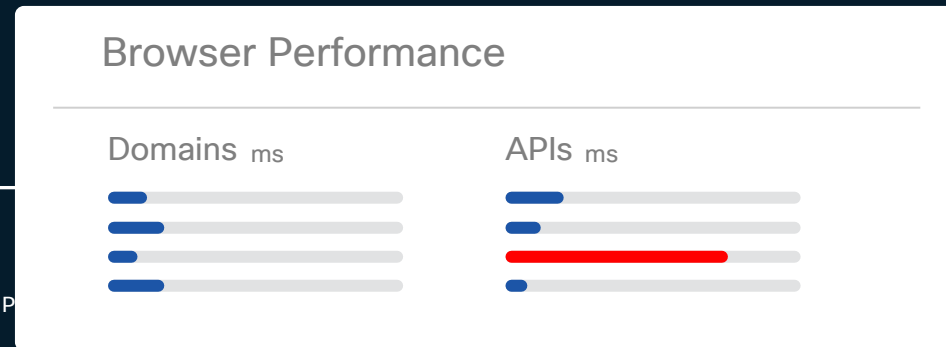
REPLACES

Point ITDR Products



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

End-to-end Visibility



CISCO

ThousandEyes Client

REPLACES

Service assurance tools



Customer perspectives

Changing the fundamentals of
data center security.

SOFTWARE DEFINED
INFRASTRUCTURE

SOFTWARE DEFINED
INFRASTRUCTURE

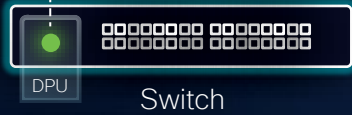


Not the next gen of anything.
The incumbent network fabric.
It's the first generation of something new.

No rip and replace

Security Cloud Control

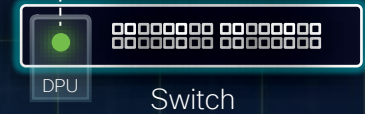
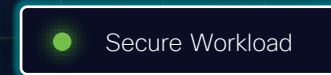
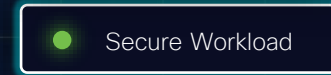
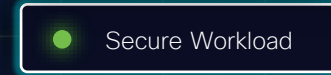
Hypershield



Hypershield/
Secure Workload



Hypershield



Enforcement points change, rules don't

Stopping lateral movement Segmentation That Works

40+

days to segment
an application

CISCO *Live!*

#CiscoLiveAPJC

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



ACCURACY



TIME

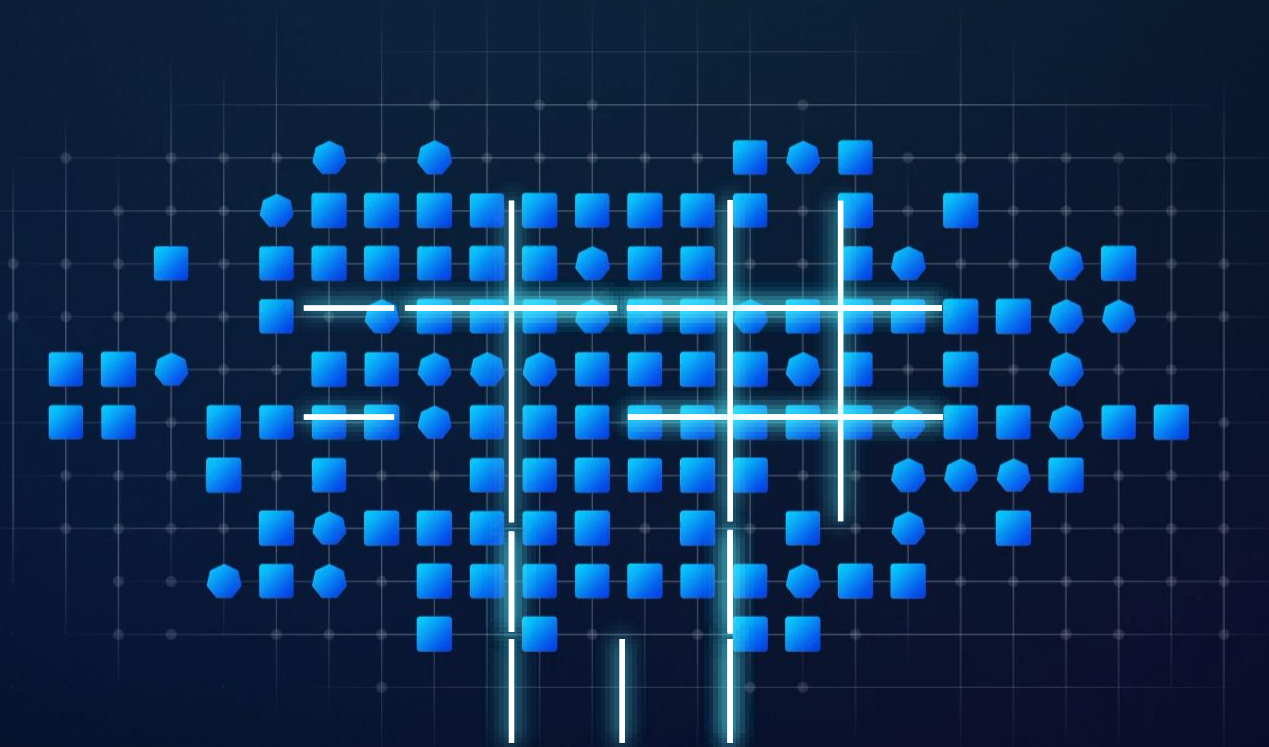
Unprecedented Visibility



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

2 million flows/second, near real-time

CONFIDENCE



CISCO Segmentation

REPLACES

Microsegmentation point products



Compensating controls Distributed Exploit Protection

Qualys

RedSeal

Tenable

WIZ

Risk Engine

HIGH	C V E - 2 0 2 4 - 5 3 7 5 7
MED	C V E - 2 0 2 4 - 5 6 6 4
MED	C V E - 2 0 2 1 - 2 8 8 1 0
LOW	C V E - 2 0 2 3 - 4 5 2 2

Is it running in memory?

Is it being exploited in the wild?

Is it a high value asset?

Private

Public

IoT

OT



AI

CI/CD Tooling Auth Bypass CVE-2024-27198

CVSS 2 Score 9.8

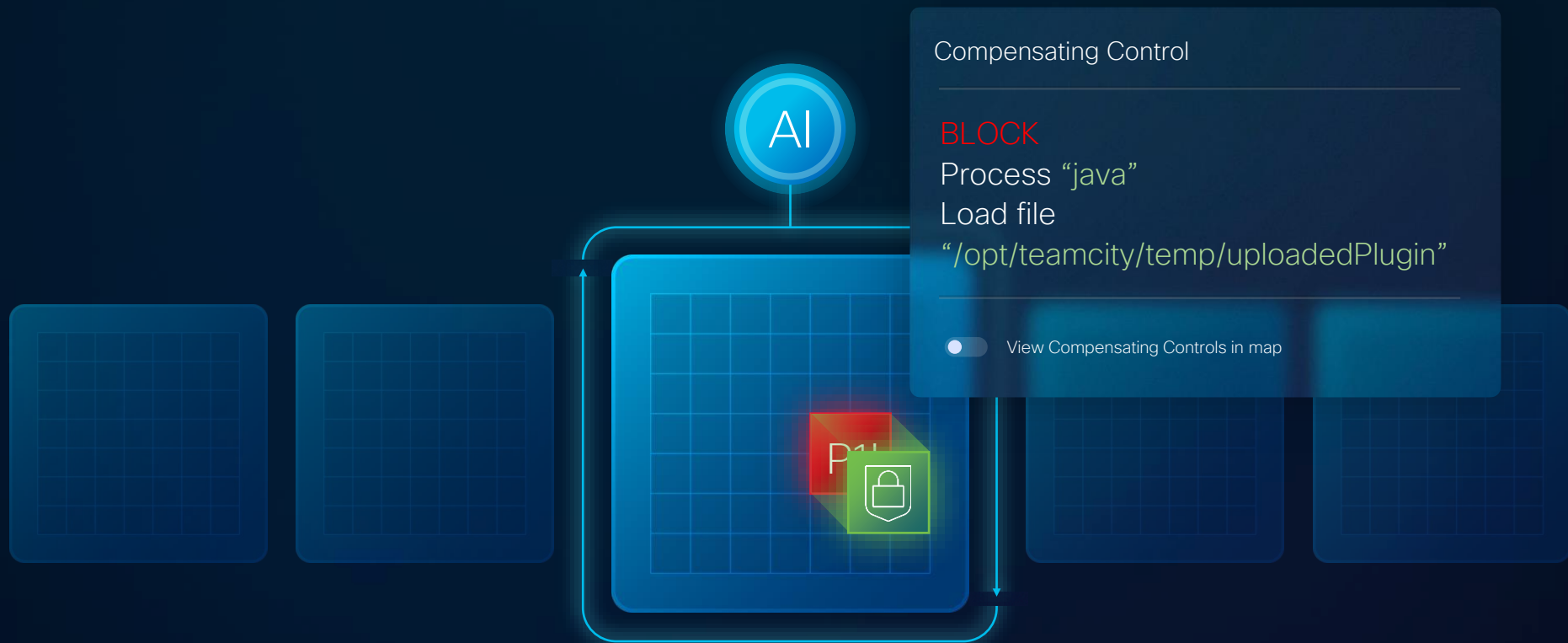
CVSS 2 Score 10

LAST SEEN

Oct 21, 2024 at 6:53 AM

Virtual Machine	Cloud Platform	Status	External ID	Internet Exposure	Operating Sys.
test-fdsek	Google Cloud	Active	2313482482374	Yes	Linux

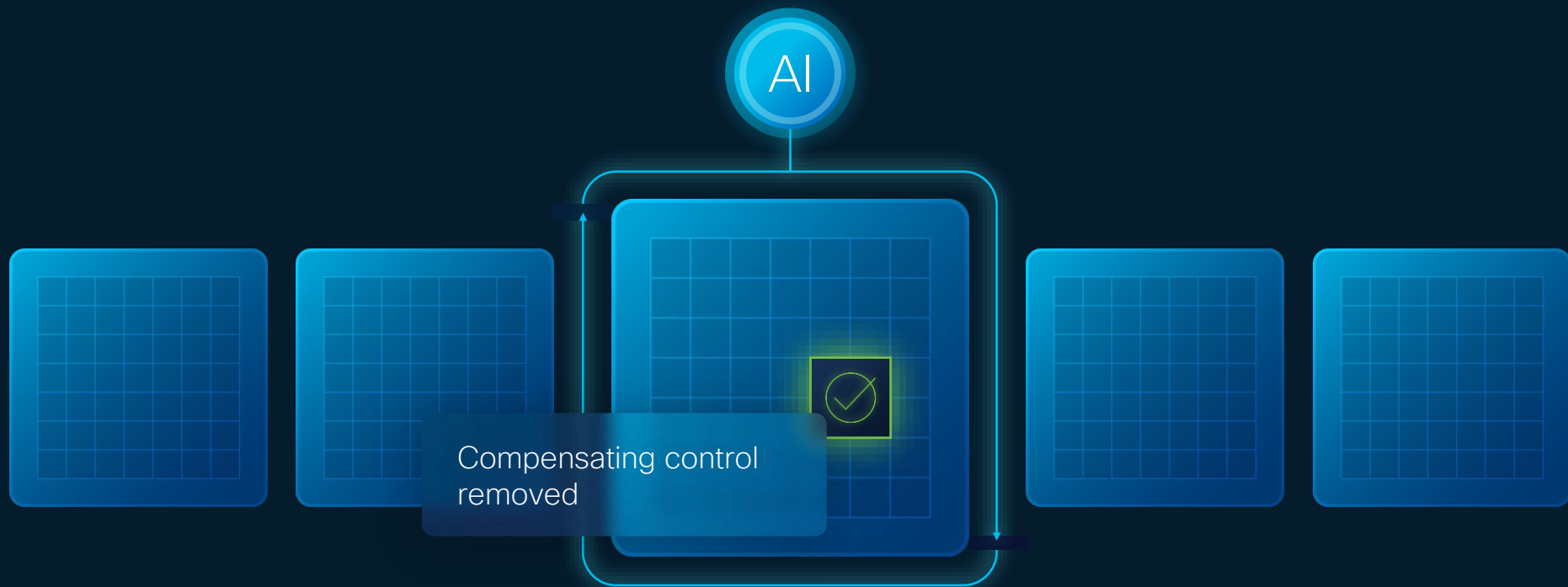
P1



Perfect fit

Tested against real world traffic

Optimal placement



CISCO

Distributed Exploit Protection



Powering the SOC of the future.

SIEM / SOAR / ANALYTICS

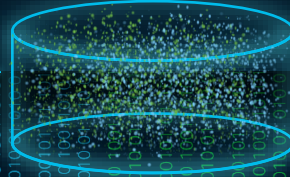
User ID
Device ID
Device process ID



+



App ID
Server ID
Server process ID





You can't have **everything**.
Where are you going to put it all?

splunk>

SIEM / SOAR

101 10 11001 011 0111001 0101 10 00 010101 10 11001 011 01110 11001 0110 00
01110 0001 1111010101 0110 100 111001100101 10 11001 011 0111001 0101 100
0 010101 10 11001 011 01110 11001 0110 11001110 0001 1111010101 0110 100

101 10 11001 011 0111001 0101 10 00 010101 10 11001 011 01110 11001 0110 00
01110 0001 1111010101 0110 100 111001100101 10 11001 011 0111001 0101 100
0 010101 10 11001 011 01110 11001 0110 11001110 0001 1111010101 0110 100

ANALYTICS

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

Innovations to Transform Security Operations



Power the
SOC of the future

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.

Figure 1: Magic Quadrant for Security Information and Event Management



Gartner

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



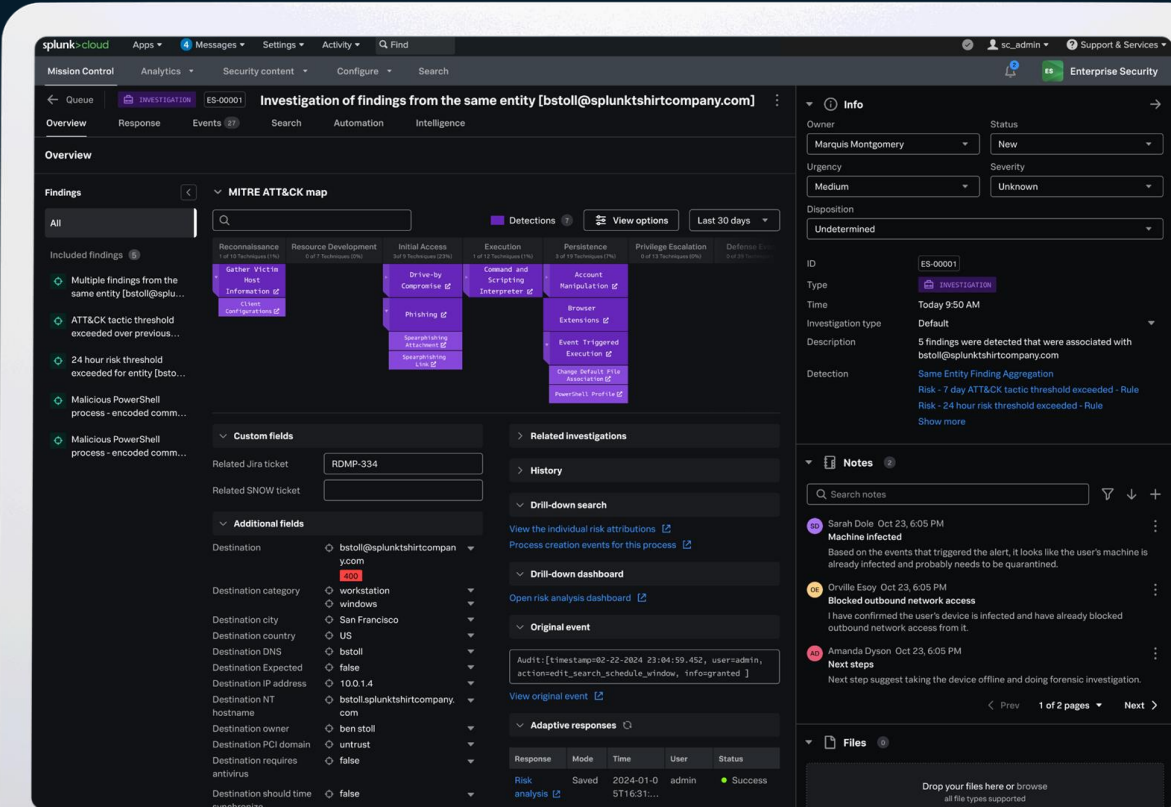
Applications

The SOC of the future will be
federated and distributed.

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



Cisco XDR

Email



Every
email

DNS



Every
web request

Endpoint



Every
process

Network



Every
flow

Talos Integration

Threat intelligence to
enrich TDIR workflows
within Splunk Attack
Analyzer

The screenshot displays the Splunk Attack Analyzer interface, specifically the Automation section. The main title is "ATT&CK tactic threshold exceeded over previous 7 days for system=splunkshrtcompany-1". The interface is divided into several panels:

- Automation history:** A list of actions run by splunk on Oct 28, 11:59 AM. The actions include: update_task_in_current_phase_2, add_task_note_1, quarantine_device_1, disable_system_owner, system_risk_object_response, get_system_owner, update_task_in_current_phase_1, set_current_phase_1, get_investigation_tasks_1, user initiated block url action, user initiated block url action, user initiated get job summary action, and user initiated url reputation action.
- Automation details:** A section titled "user initiated url reputation action" showing the status (Success), owner (TDIR Admin), and start time (Oct 28, 11:57 AM). It also displays the connector (Talos Intelligence) and the URL being checked ("http://internetbadguys.com").
- Automation table:** A table showing the results of the automation run. The table has columns: RUN ID, CONFIGURATION, NAME, CONNECTOR, and STATUS. The row shows: 374, splunk and talos, url reputation, Talos Intelligence, and success.
- Talos Integration:** A section titled "Talos" showing the action "Action: NoTitle" and the Run ID "374". It displays the URL "http://internetbadguys.com" and the status "success".
- Threat Intelligence:** A table showing the threat intelligence data. The table has columns: url, status, threat level, threat categories, and Acceptable Use Policy Categories. The row shows: http://internetbadguys.com, success, Untrusted, Malware, and Computer Security.
- Info Panel:** A panel on the right side of the interface showing details about the automation run, including the owner (My thomson), status (Pending), urgency (Critical), and disposition (Undetermined).

What's Next?

Better Technical
Add-ons

Talos
Integration with
ES and SOAR

AI Assistant
in ES



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.



Thank you

CISCO *Live!*

#CiscoLiveAPJC