

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive

Cisco Webex App

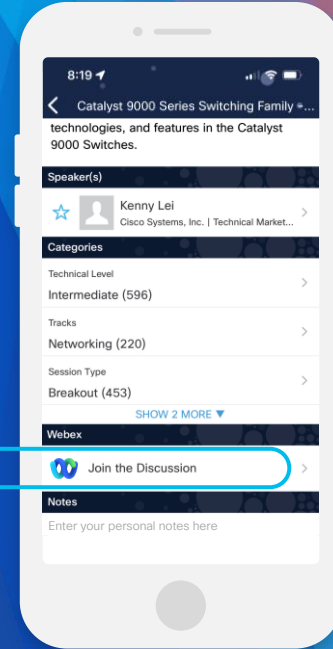
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-1456>



The bridge to possible


Automate and Simplify Your Ransomware Defence with Cisco's XDR

Elia Maracani, System Engineer & Project Manager
Cisco Cybersecurity Co-Innovation Center Milan
DEVNET-1456

CISCO *Live!*

#CiscoLive



A photograph of two skydivers in freefall. The instructor, in the background, wears an orange jumpsuit and sunglasses, with his hands on the student's shoulders. The student, in the foreground, wears a yellow and orange jumpsuit and goggles, with a wide-mouthed expression of surprise or excitement. They are suspended by a single rope against a bright blue sky with scattered clouds. Below them, a vast landscape of fields and small towns is visible from a high altitude.

I hope it
will open



Agenda

- The Ransomware Problem
- The Solution (?)
- A Better Solution
- Demo
- Future Improvements
- Conclusion

The Ransomware Problem

The rise and evolution of the threat



Gaining Trust

*Trust is the base
for it all*

The hacker
encrypts data and
devices.



The Ransomware Problem

The rise and evolution of the threat



Gaining Trust

*Trust is the base
for it all*

The hacker
encrypts data and
devices.



Data Sale

*Data is the most
valuable thing*

The hacker copies
and exfiltrates the
data.



The Ransomware Problem

The rise and evolution of the threat



Gaining Trust

Trust is the base for it all

The hacker encrypts data and devices.



Data Sale

Data is the most valuable thing

The hacker copies and exfiltrates the data.



Lateral Movement

Everything is fair game

The hacker uses the copied data to hack other services.



The Ransomware Problem

The rise and evolution of the threat



Gaining Trust

Trust is the base for it all

The hacker encrypts data and devices.



Data Sale

Data is the most valuable thing

The hacker copies and exfiltrates the data.



Lateral Movement

Everything is fair game

The hacker uses the copied data to hack other services.



Blackmail

Reputation is everything

The hacker threatens to publish all the sensitive data.



The Ransomware Problem

The rise and evolution of the threat



Gaining Trust

Trust is the base for it all

The hacker encrypts data and devices.



Data Sale

Data is the most valuable thing

The hacker copies and exfiltrates the data.



Lateral Movement

Everything is fair game

The hacker uses the copied data to hack other services.



Blackmail

Reputation is everything

The hacker threatens to publish all the sensitive data.



Next?

Evolution never stops

Same as in biological life, computer viruses keep evolving.



The Ransomware Problem

Real-life impacts

Attack Frequency*

2 seconds
(2031)



11 seconds
(2021)

Damage Costs*

\$265B
(2031)



\$20B
(2021)

Patients unable to receive
real-time care at hospitals

Residents unable to reach
first responders via 911

Clients unable to **transact**
with offline financial banking
systems

* Source: [Cybersecurity Ventures Cybercrime Magazine](#)

The Solution (?)

Backup is all you need.. Ish



nixCraft @nixcraft · 21h

This is how most organisations' backup and disaster recovery (DR) plan looks in case a ransomware attack, hacking or Alien invasion occurs right now ...



24

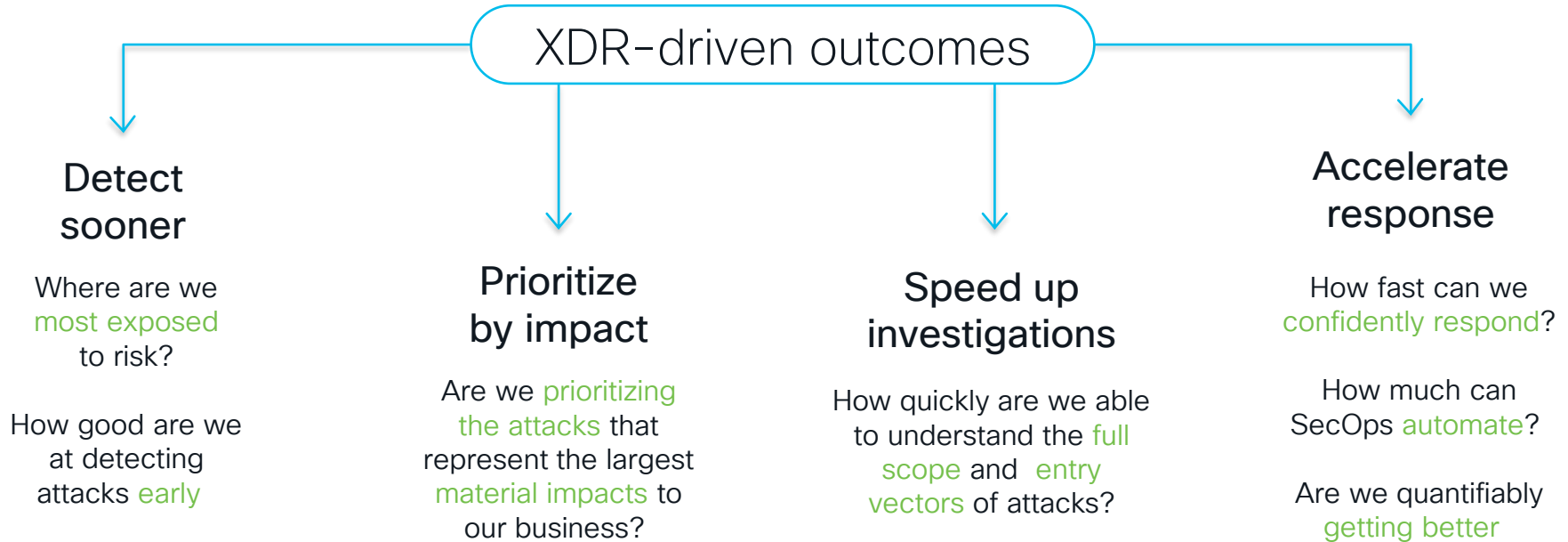
358

1,624



A Better Solution

Shift the focus to outcomes



A Better Solution

Simplify security operations



Open and flexible approach, optimized for multi-vendor, multi-vector experience

Simplify the user experience and gain visibility and identify threats across network, cloud, endpoint, email, and applications for effective security regardless of vendor or vector.



Threat correlation and clear prioritization to help users see what's most important

Correlate and prioritize alerts across multiple telemetry sources using AI and ML to improve incident response.



Rapid and guided responses to quickly remediate threats and improve analyst efficiency

Rapidly remediate threats and take appropriate action quickly with automation capabilities, orchestration workflows, and guided remediation, freeing up time and resources to focus on strategic tasks.



Essential network insights, providing better understanding of your environment

Leverage network insights to protect against complex threats and bring clarity to security operations. By making the network foundational and going beyond EDR, organizations can identify and prevent advanced threats from evading detection and improve XDR outcomes.

Cisco's XDR

Quickly position teams to achieve incremental XDR milestones

Integrate

Consolidate solutions and technology with an integrated platform



Orchestrate

Enable prioritized detection and response using AI & ML



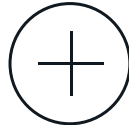
Optimize

Evolve, and fine tune security by proactively executing against that baseline



Unify

Build an ecosystem that aggregates, enriches data and telemetry from all part of your environment



Automate

Automate detection and response workflows that require minimal human intervention



A Better Solution

Cisco's XDR comes to the rescue



The screenshot displays the Cisco XDR Incidents management console. On the left is a navigation sidebar with options like Control Center, Incidents, Investigate, Intelligence, Automate, Exchange, Workflows, Runs, Targets, Account Keys, Variables, Triggers, Tasks, Options, Devices, and Administration. The main area is titled 'Incidents' and shows a summary of 1,504 incidents, with 8 new and 221 open. A table lists individual incidents with columns for Priority, Name, Source, and Created. A detailed view of incident 'c9-9300-1g1-0-19-win10 in group Pluto Clients @...' is shown on the right, including its MITRE ATT&CK mapping (TA0043: Reconnaissance, TA0042: Resource Development, etc.) and a risk score breakdown (3 Detection, 10 Asset Value).

Priority	Name	Source	Created
529	c2-3850-4-g1-6-win10 in group Mars Clients @ 20230413 16:37:17	Secure Endpoint	4 Days
523	c1-4506-1-g3-14-win10 in group Mars Clients @ 20230411 20:27:12	Secure Endpoint	6 Days
502	c1-9300-1-g1-13-win10 in group Mars Clients @ 20230411 18:26:19	Secure Endpoint	6 Days
733	c2-3850-1-t1-0-15-win10 in group Mars Clients @ 20230411 16:20:28	Secure Endpoint	6 Days
713	c3-9300-1-g1-0-7-win10 in group Audit @ 20230411 08:48:34	Secure Endpoint	8 Days
722	c9-9300-1g1-0-19-win10 in group Pluto Clients @ 20230410 15:35:17	Secure Endpoint	7 Days
513	C3-9300-2-g1-0-7-win10 in group Titan Clients @ 20230410 15:20:52	Secure Endpoint	7 Days
1000	Heartbeat Connection Count for Cisco - Lawrenceville Lab (Earth)	Cisco Secure Cloud Analytics...	8 Days
261	c4-2960xr-stk-g1-8-win10 in group Earth Clients @ 20230407 12:29:36	Secure Endpoint	10 Days
513	c4-2960xv-stk-g1-8-win10 in group Earth Clients @ 20230407 12:29:33	Secure Endpoint	10 Days
722	c1-4506-2-g3-13-win10 in group Mars Clients @ 20230406 13:52:31	Secure Endpoint	11 Days
722	c9-9300-1g1-0-19-win10 in group Pluto Clients @ 20230406 14:05:07	Secure Endpoint	11 Days
722	c5-9300-1-g1-9 in group Audit @ 20230406 14:04:36	Secure Endpoint	11 Days
1000	c5-9300-1-g1-8-win10 in group Pluto Clients @ 20230406 13:52:57	Secure Endpoint	11 Days
1000	c4-3850-1-g1-8-win10 in group Earth Clients @ 20230406 13:51:58	Secure Endpoint	11 Days
513	c1-3850-2-g1-0-3-win10 in group Mars Clients @ 20230403 19:10:55	Secure Endpoint	14 Days

Incidents

Incident Response Workflow

LWR-John-Windows in group LW-Endpoints @ 20230117 08:55:10

Reported by Secure Endpoint on 2023-01-17T08:55:10.000Z - 3 Linked Incidents

Add short description...
View Long Description

Overview Detection **Response** Worklog

Identification
Containment
Eradication
Recovery

- Contain Incident Domains
Contain indicators of compromise to stop the spread of malicious activity
- Contain Incident URLs
Contain indicators of compromise to stop the spread of malicious activity
- Contain Incident File Hashes
Contain indicators of compromise to stop the spread of malicious activity
 - Determine the appropriate containment technique either with soft block (localized blocking of a specific indicators) or hard block (regionalized blocking, quarantine whole hosts, net blocks, etc) techniques
 - Determine if the containment is working and stopping additional infections or activity. This phase is not complete if containment is not working.

Incident responders use the atomic indicators found in the investigation to block and contain malicious activity.
By using host and network protection tools to block, pause, drop, or quarantine affected machines to apply the preventative protection from additional infections.
Incident responders want to be able to move up to the highest level of indicator possible (e.g. using the pyramid of pain is a good example).
- Contain Incident Assets
Contain identified assets of the incident
- Implement additional monitoring
Implement additional monitoring that reviews not only host/network containment or eradication success.
- Identify vulnerabilities
Scan host(s) for vulnerabilities and add a note on the recommended patches to be applied and service request to have them installed, if submitted.

Back Go to Eradication

7 Observables

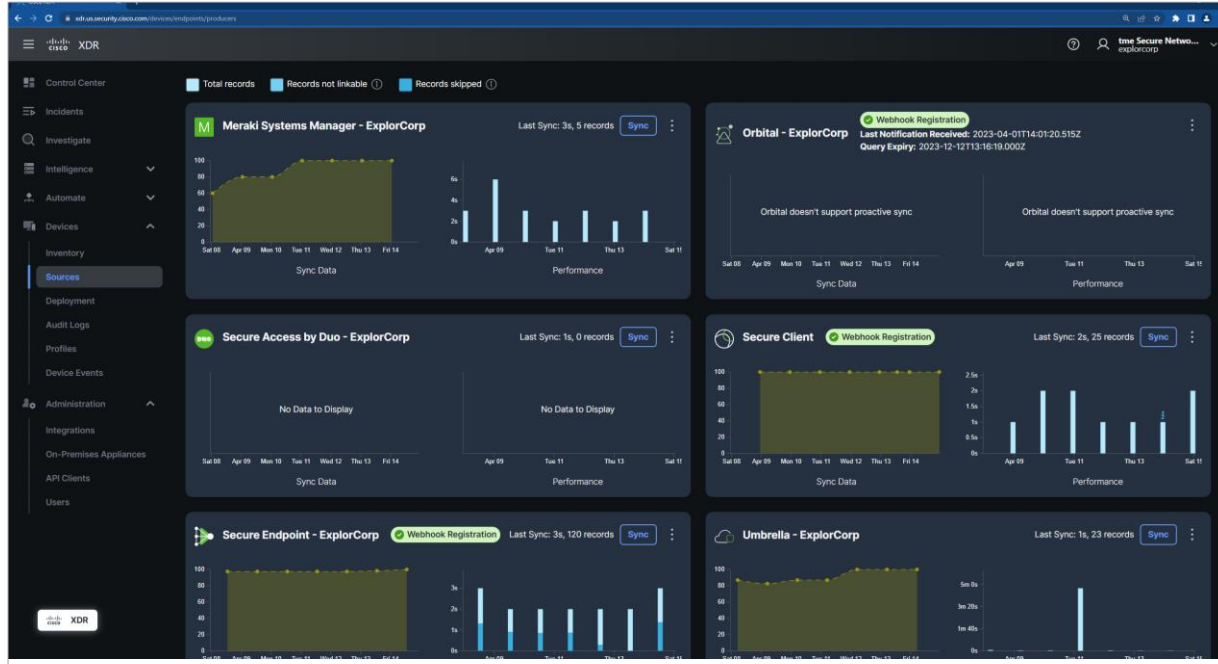
SHA256

- 000000000000000000000000... 12 events
- df6a9e8c316d90c118b45480c... 7 events
- add883a8910abb0fc28b557fa... 7 events
- e8fc5a2b0ca52d24b095ee... 5 events
- 751cd7ab78b18a2d8a55c47a7... 5 events
- d8c14b47c26a05eb5c3a315fd... 2 events
- b89881a874728bd0918a0eb... 2 events

Actions taken
log goes here

Execute

Incident response



Inventory



Control center

A Better Solution

Detect more, act faster, elevate productivity, build resilience

Detect
the most
sophisticated
threats



Multi-vector detection:
network, cloud, endpoint,
email, and more
Enriched incidents with
asset insights, threat intel
Optimized for
multi-vendor environments

Act on
what *truly*
matters, faster



Prioritize threats by
greatest material risk
Unified context to
streamline investigations
Evidence-backed
recommendations

Elevate
productivity



Focus on what matters and
filter out the noise
Boost limited resources for
maximum value
Automate tasks and focus
on, strategic tasks

Build
resilience



Close security gaps
Anticipate what's next
through actionable intel
Get stronger, everyday
with continuous,
quantifiable improvement

A Better Solution

Improve your **cyber resiliency** with Cohesity



- First data protection solution integrated with Cisco XDR and Cisco UCS X-Series
- Complementary Cohesity & Cisco platforms **eliminate** data management and security **silos**
- **Unites** security, network, and IT Ops **teams** for improved data-security posture & productivity
- Accelerates **threat discovery, investigation** and **response** to ransomware
- **Exceptional** Cisco experience end to end

A Better Solution

Improve your **cyber resiliency** with Cohesity



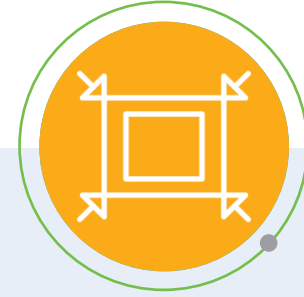
Protect
Immutability

Untouchable backup with
granular access controls



Detect
Intelligence

Data-centric threat detection
and SecOps integrations



Recover
Rapid Recovery @ Scale

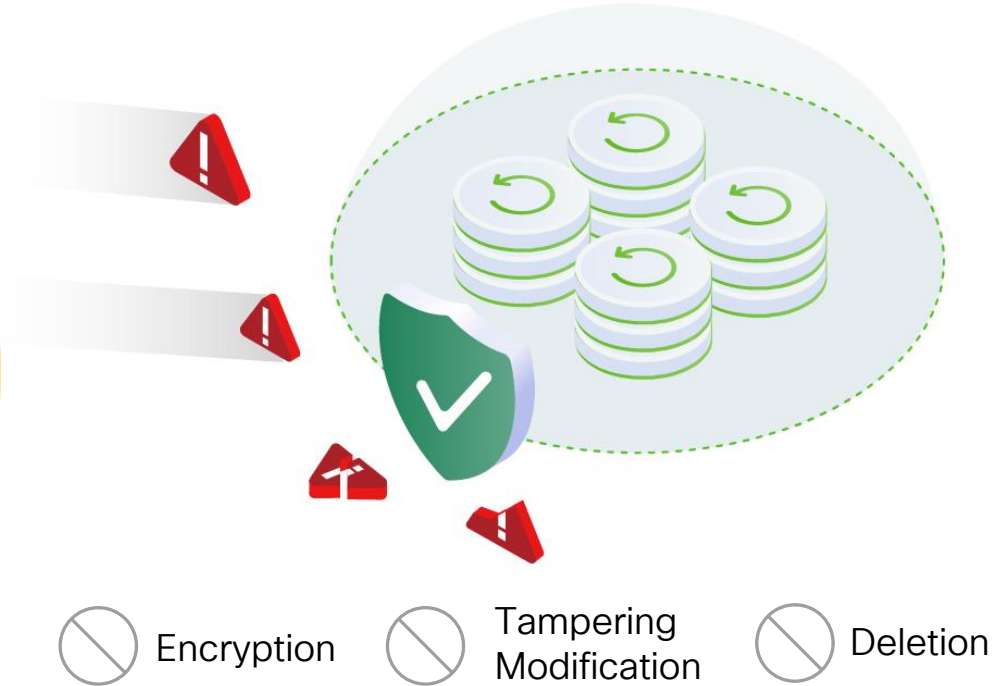
Accelerated recoveries

A Better Solution

Improve your **cyber resiliency** with Cohesity

Protect Data

Enforce data integrity, confidentiality, and reliability thanks to immutable backups, strict access controls, encryption and high built-in fault tolerance



A Better Solution

Improve your **cyber resiliency** with Cohesity

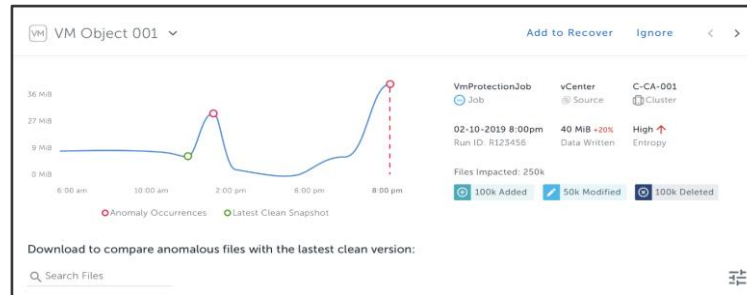
Detect anomalies

Watch data for attack indicators and integrate with Security Operations



Machine-driven Anomaly detection based on:

- Time Series of **Data written**
- **Entropy** (randomness of data)
- Nature of **File System changes** (bulk files added, deleted, modified)



A Better Solution

Improve your **cyber resiliency** with Cohesity

Recover

Accelerate recovery to support 24x7 operations and SLAs

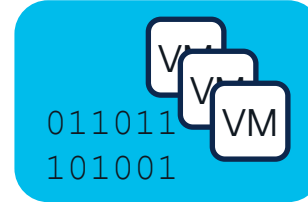
Rapid Recovery @Scale

- **Immediately restore VMs**
 - Instant Mass Restore
- **Immediate availability of files and objects**
 - Instant File Access
- **Determine best recovery point**
 - Any-time recovery
 - Recommend last known-good recovery point
- **Assist with investigation of cyber event**

A Better Solution

The power of integration and cooperation

Main parachute



Reserve



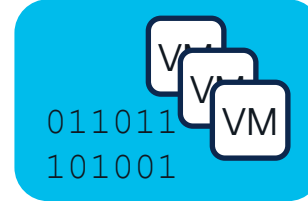
A Better Solution

The power of integration and cooperation



Onboard
computer (AAD)

Main parachute

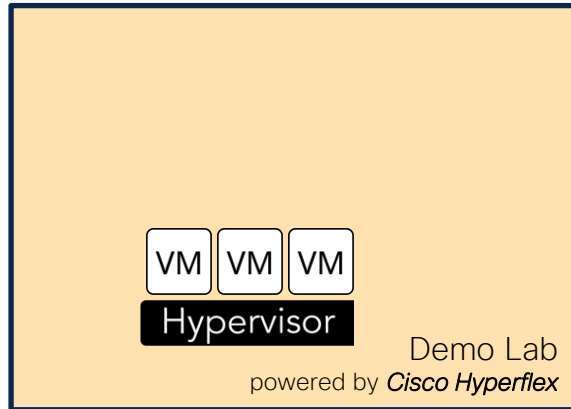


Reserve



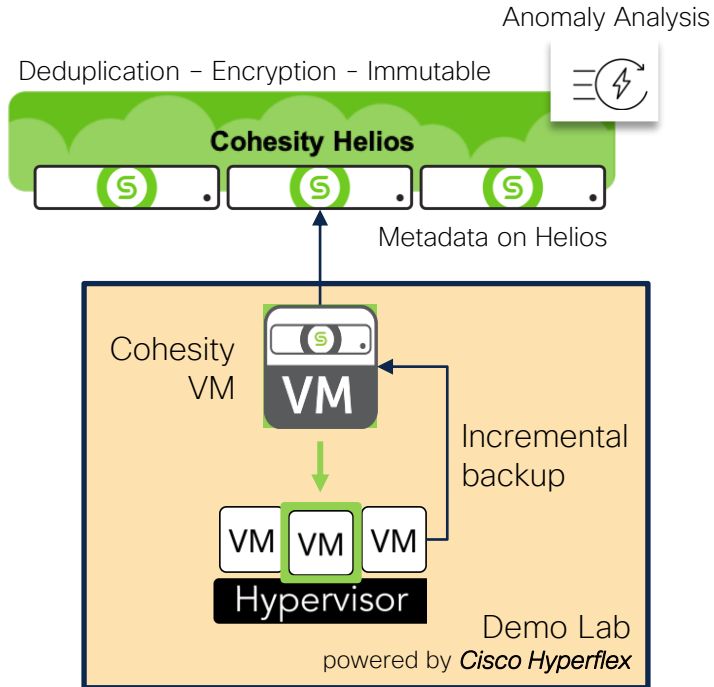
A Better Solution

Demo's Architecture - How it works now



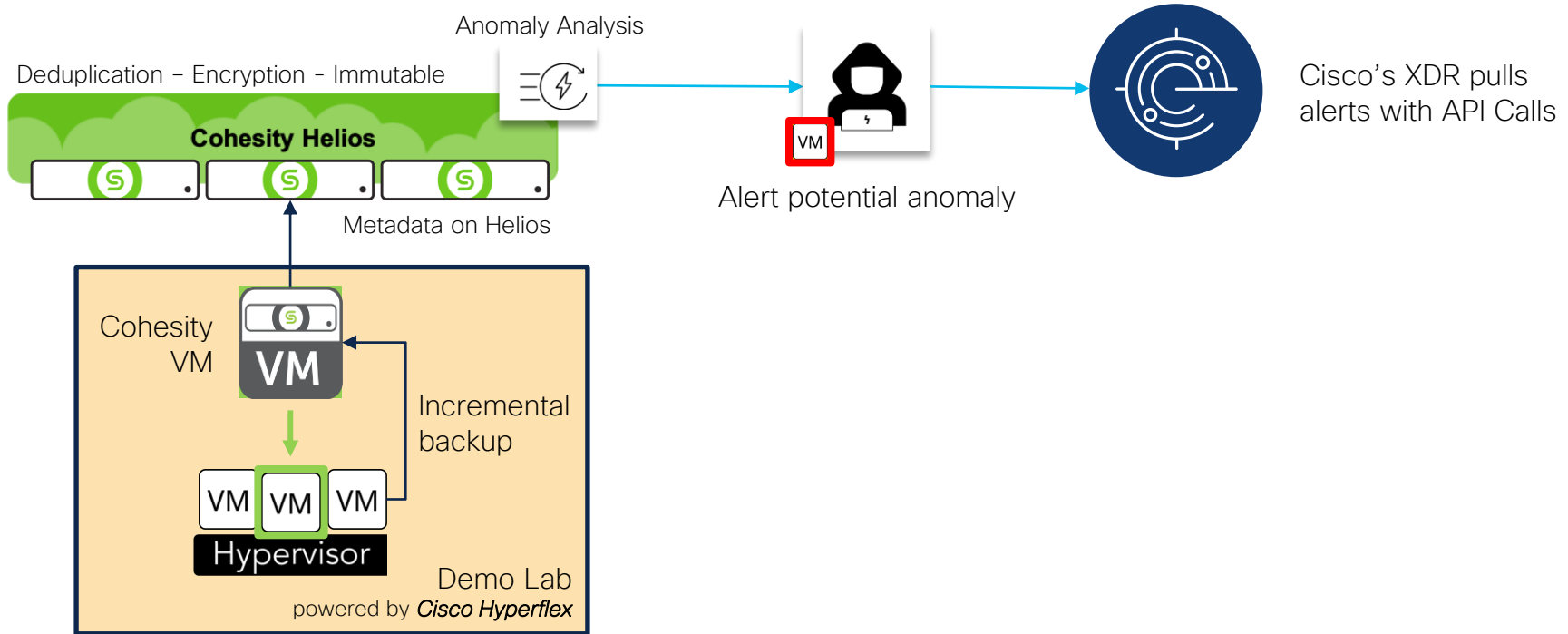
A Better Solution

Demo's Architecture - How it works now



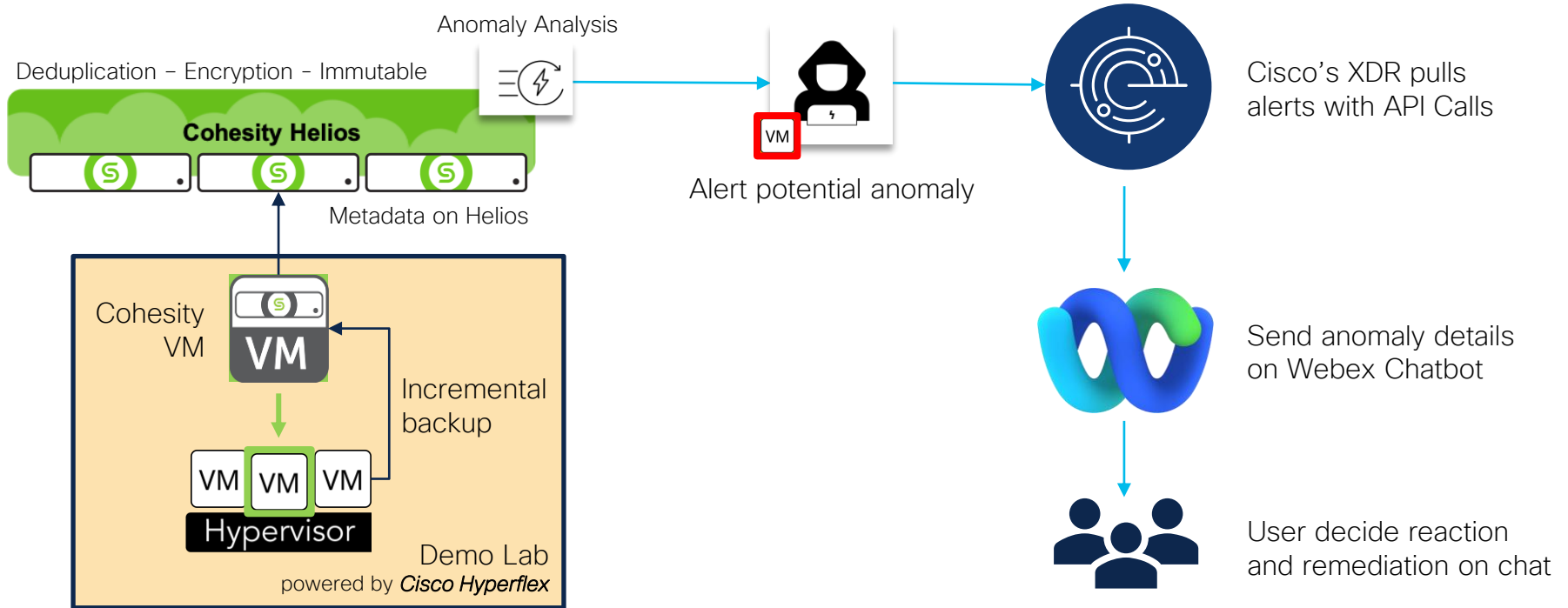
A Better Solution

Demo's Architecture - How it works now



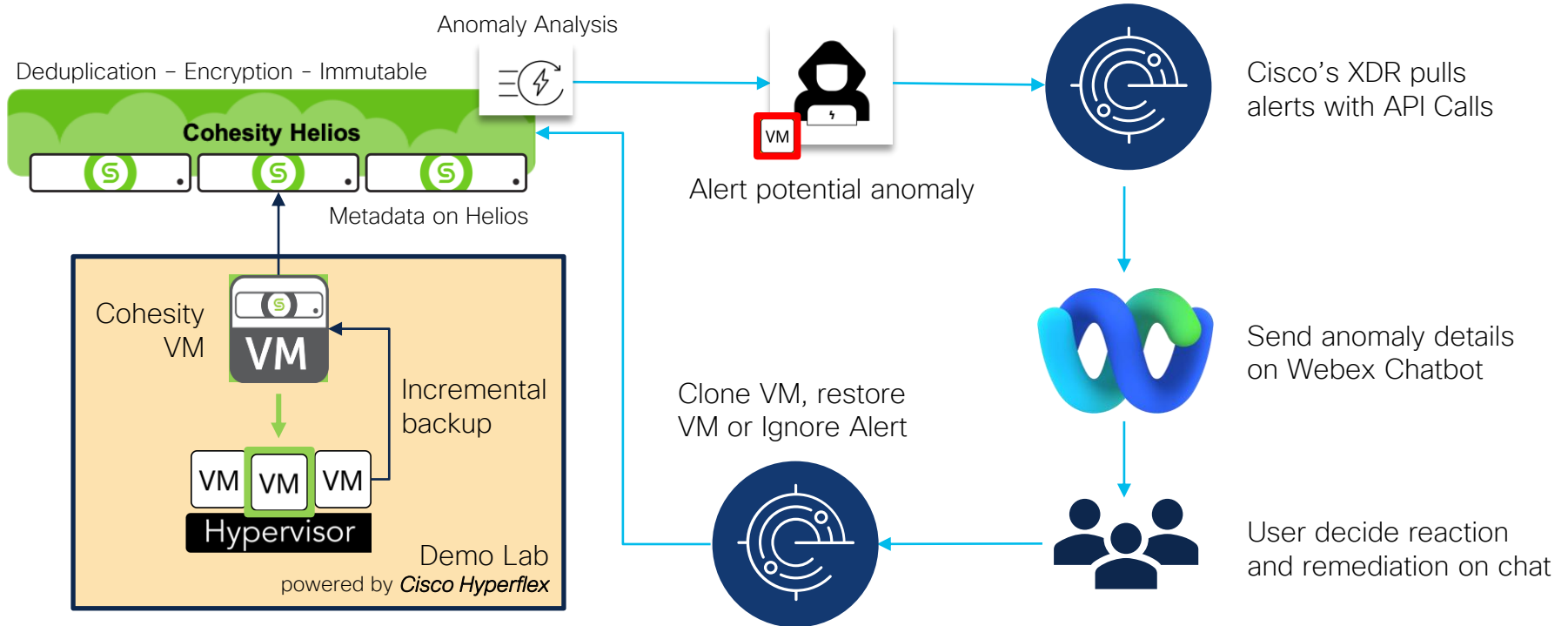
A Better Solution

Demo's Architecture - How it works now



A Better Solution

Demo's Architecture - How it works now





Demo

CISCO *Live!*

Behind the scenes

SecureX Orchestrator

Future improvements

To infinity.. And beyond!



Secure Endpoint

gathers the timestamp of the device before the malware

Future improvements

To infinity.. And beyond!



Secure Endpoint

gathers the timestamp of the device before the malware

Most recent backup, less secure **OR**
Most secure backup, less recent

Future improvements

To infinity.. And beyond!



Secure Endpoint

gathers the timestamp of the device before the malware

Most recent backup, less secure **OR**
Most secure backup, less recent



Umbrella

checks for suspicious DNS requests and web traffic

Future improvements

To infinity.. And beyond!



Secure Endpoint

gathers the timestamp of the device before the malware

Most recent backup, less secure **OR**
Most secure backup, less recent



Umbrella

checks for suspicious DNS requests and web traffic

Reduce false positives



The bridge to possible

“Diversity is a mix and inclusion is making the mix work.”

Andrés Tapia

Power in diversity, thanks to Cisco XDR

CISCO *Live!*

#CiscoLive



The bridge to possible



Thank you
... and remember your parachute

CISCO *Live!*

#CiscoLive

Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes



Continue your education



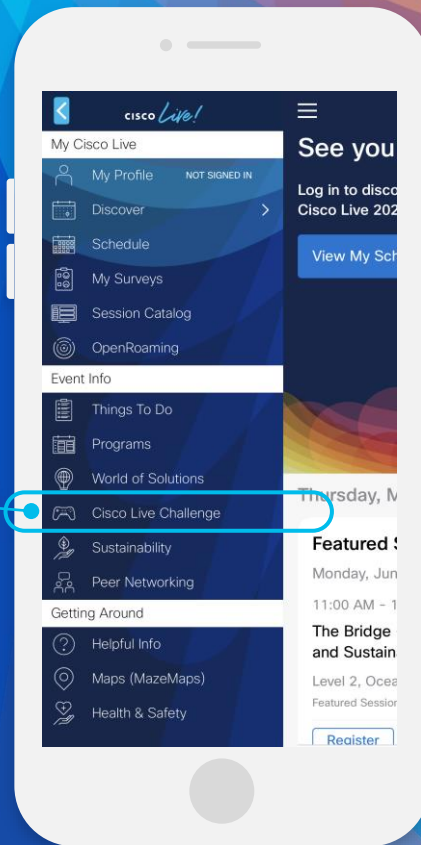
- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive