Enterprise Strategy Group™ by TechTarget

uptycs

Less Drama, Better Security Data: Unifying Your Cloud and Endpoint Security Solutions

uptycs

Enterprise Strategy Group by TechTarget

Your Expert Panel

@Uptycs
@ESG_Global

Dave Gruber

Principal Cybersecurity Analyst, ESG

Melinda Marks

Sr. Analyst of Application & Cloud Security, ESG

Kevin Paige

CISO & VP of Product Strategy, Uptycs

Agenda

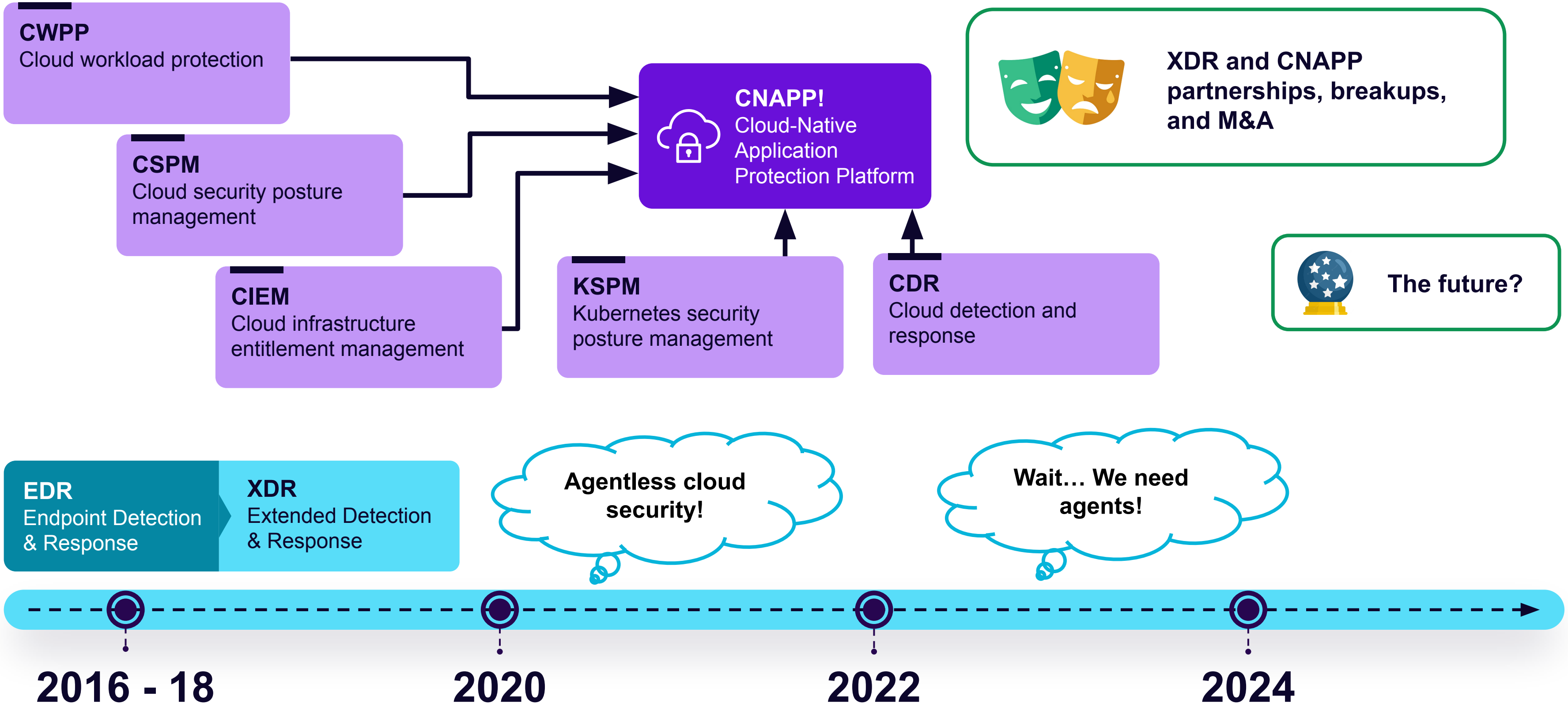
The (recent) evolution of cloud and endpoint security

Security challenges with digital transformation

- Increased IT complexity
- Remote work
- Cloud adoption
- A wide range of incidents
- Too many siloed tools and data

Closing the gaps

Evolution, convergence, partnerships, breakups, M&A, oh my!



CWPP
Cloud workload protection

CSPM
Cloud security posture management

CIEM
Cloud infrastructure entitlement management

CNAPP!
Cloud-Native Application Protection Platform

KSPM
Kubernetes security posture management

CDR
Cloud detection and response

XDR and CNAPP partnerships, breakups, and M&A

The future?

EDR
Endpoint Detection & Response

XDR
Extended Detection & Response

Agentless cloud security!

Wait… We need agents!

2016 - 18

2020

2022

2024

Security Challenges with Digital Transformation

Increased IT complexity

What do you believe are the **biggest reasons your organization's IT environment has become more complex?**

#1

Increase in remote and hybrid work concerns

Source: ESG's Securing the Cloud-native Attack Surface with Unified XDR and CNAPP(Percent of respondents, N=392, five responses accepted out of thirteen)

Security Challenges with Digital Transformation

Increased IT complexity

What do you believe are the **biggest reasons your organization's IT environment has become more complex?**

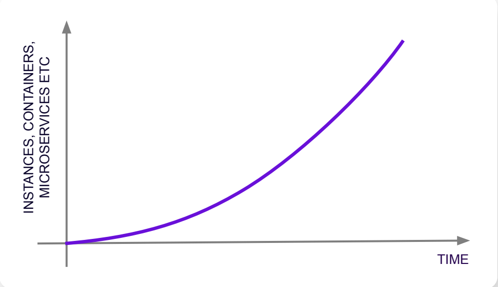
#2

Higher data volumes

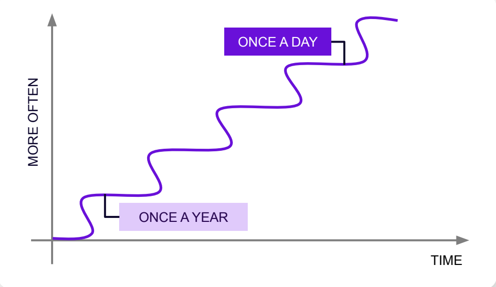
Source: ESG's Securing the Cloud-native Attack Surface with Unified XDR and CNAPP(Percent of respondents, N=392, five responses accepted out of thirteen)

The cybersecurity industry has been on a collision course with a growing volume, variety, and velocity of data…

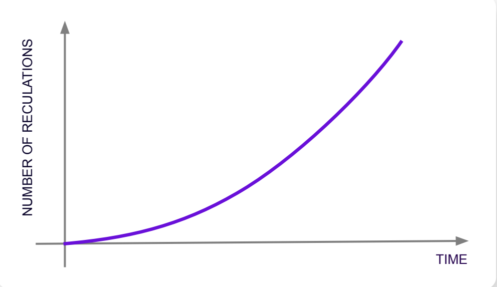
NUMBER INFRASTRUCTURE/DATA UNITS



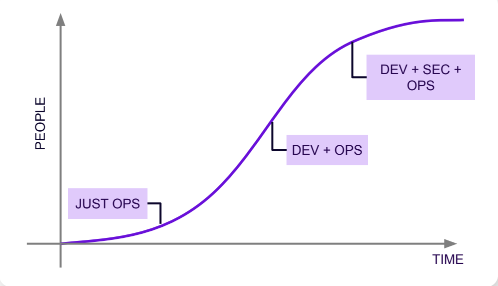
FREQUENCY OF CHANGES



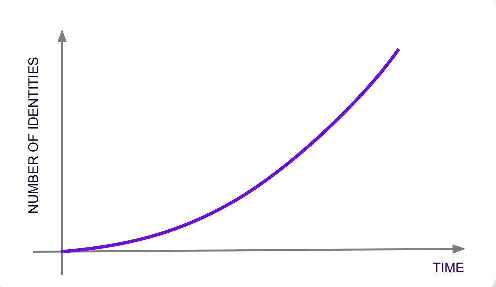
NUMBER OF CYBERSECURITY REGULATIONS



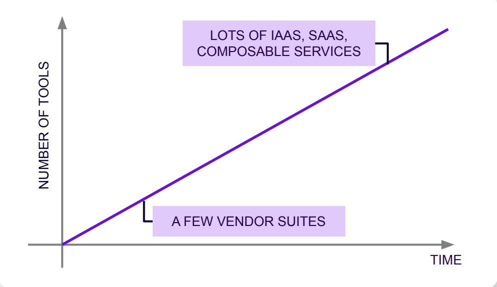
ENGINEERS INVOLVED



MACHINE IDENTITIES AND ENTITLEMENTS



TOOLS AND SERVICES USED



Security Challenges with Digital Transformation

Cloud Adoption

What are the biggest challenges your organization has faced, or expects to face, with its cloud-native applications?

#1

Security

Source: ESG's Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=387, multiple responses accepted out of five)

Security Challenges with Digital Transformation

Cloud Adoption

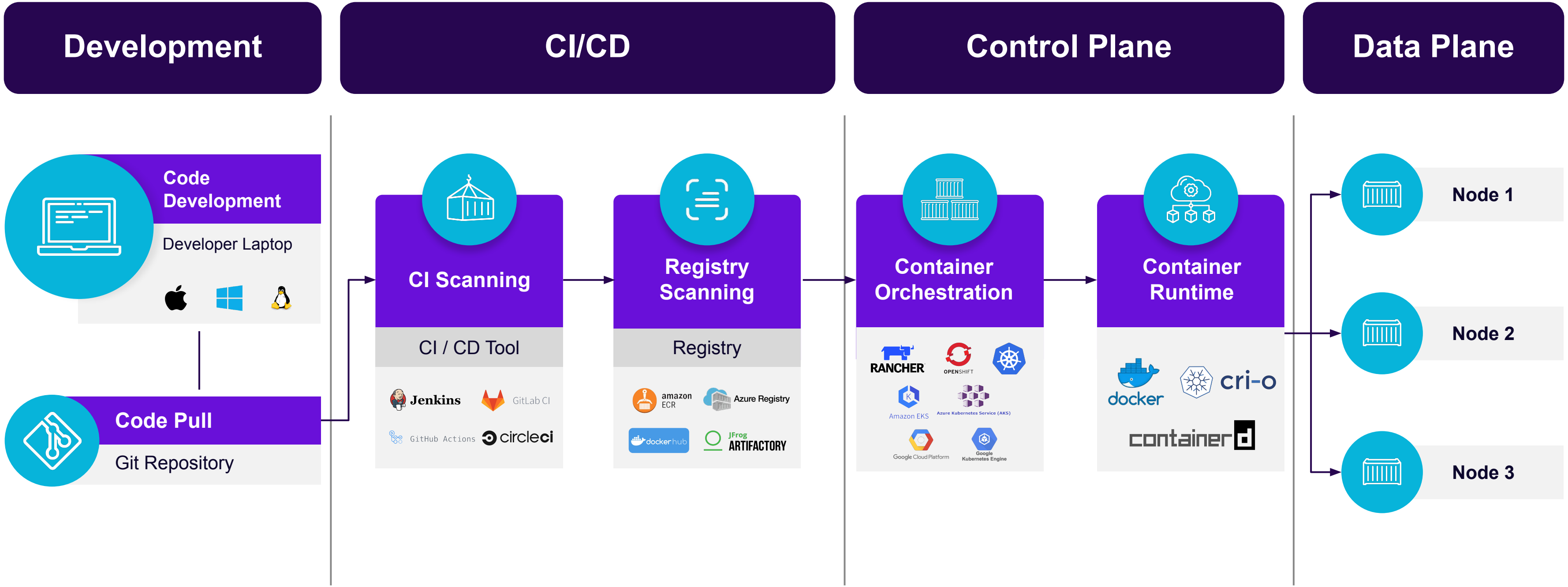
What are the biggest challenges your organization has faced, or expects to face, with its cloud-native applications?

#2

Compliance

Source: ESG’s Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=387, multiple responses accepted out of five)

Securing the innovation pipeline is challenging



Development

CI/CD

Control Plane

Data Plane

Code Development

Developer Laptop

Code Pull

Git Repository

CI Scanning

CI / CD Tool

Registry Scanning

Registry

Container Orchestration

Container Runtime

Node 1

Node 2

Node 3

Security Challenges with Digital Transformation

Cloud Adoption Means Faster Release Cycles

What security challenges does your organization face with faster development cycles of CI/CD?

#1

Software is released without going through security checks and/or testing

Source: ESG's Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=350, multiple responses accepted out of eight)

Security Challenges with Digital Transformation

Cloud Adoption Means Faster Release Cycles

What security challenges does your organization face with faster development cycles of CI/CD?

#2

Security lacks visibility and control in development processes

Source: ESG’s Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=350, multiple responses accepted out of eight)

Security Challenges with Digital Transformation

Cloud Adoption Means Faster Release Cycles

What security challenges does your organization face with faster development cycles of CI/CD?

#3

New builds are deployed to production with misconfigurations, vulnerabilities, and other security issues

Source: ESG's Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=350, multiple responses accepted out of eight)

Security Challenges with Digital Transformation

Suffering a range of incidents on cloud infra and applications

Which of the following cybersecurity incidents, if any, has your organization experienced in the last 12 months related specifically to cloud-native applications and infrastructure?

#1

The unauthorized or malicious use of a privileged account, secrets, or access keys via stolen credentials

Source: ESG's Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=383, multiple responses accepted out of twelve)

Security Challenges with Digital Transformation

Suffering a range of incidents on cloud infra and applications

Which of the following cybersecurity incidents, if any, has your organization experienced in the last 12 months related specifically to cloud-native applications and infrastructure?

#2

Exploit of a misconfigured cloud service, workload, security group, and/or privileged account

Source: ESG's Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=383, multiple responses accepted out of twelve)

Security Challenges with Digital Transformation

Suffering a range of incidents on cloud infra and applications

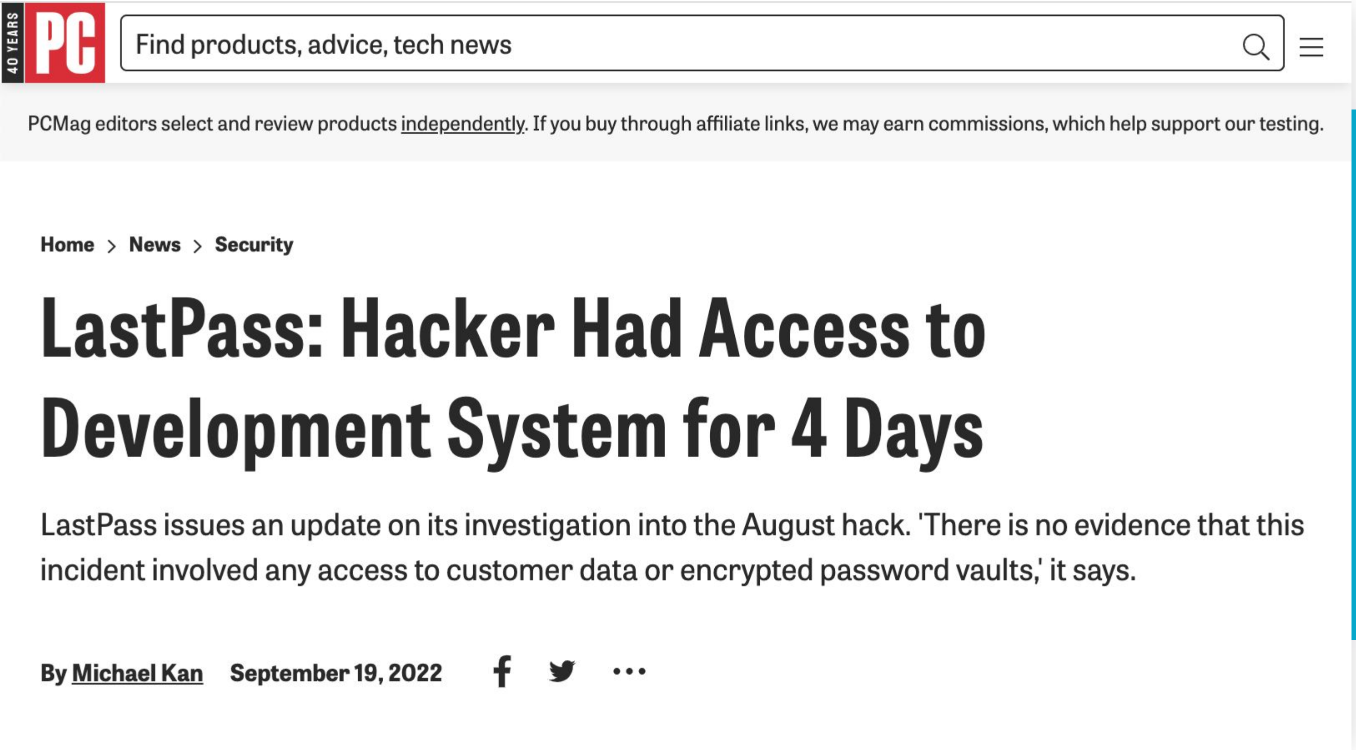
Which of the following cybersecurity incidents, if any, has your organization experienced in the last 12 months related specifically to cloud-native applications and infrastructure?

#3

Malware that moved laterally to cloud workloads

Source: ESG's Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=383, multiple responses accepted out of twelve)

Developer laptop security is crucial



PCMag editors select and review products independently. If you buy through affiliate links, we may earn commissions, which help support our testing.

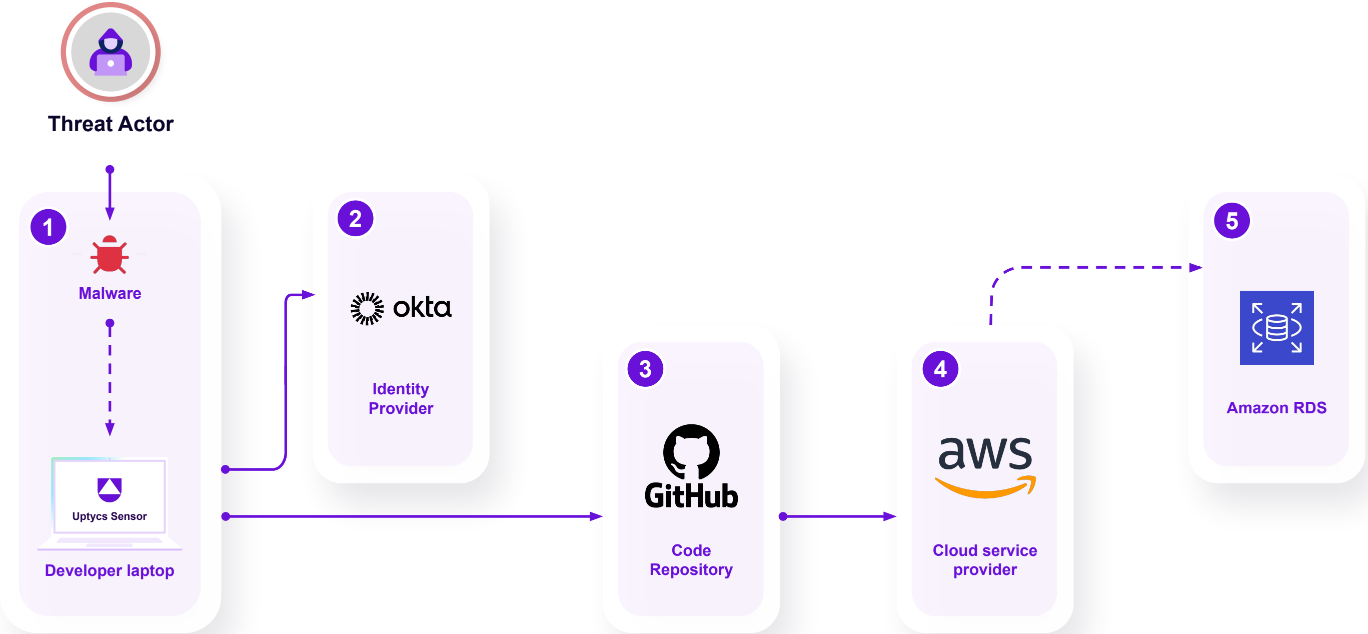
Home > News > Security

LastPass: Hacker Had Access to Development System for 4 Days

LastPass issues an update on its investigation into the August hack. 'There is no evidence that this incident involved any access to customer data or encrypted password vaults,' it says.

By Michael Kan September 19, 2022

Major breaches often start with the developer's laptop



Security Challenges with Digital Transformation

Too many siloed tools and data

Which of the following represent the biggest challenges associated with managing an assortment of security products from different vendors?

Source: ESG’s Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=280, three response accepted out of seven)

#1

Each security technology demands its own training, implementation, management, and operations, straining my organization’s resources

Security Challenges with Digital Transformation

Too many siloed tools and data

Which of the following represent the biggest challenges associated with managing an assortment of security products from different vendors?

#2

It is difficult to get a complete picture of our security status using many disparate security technologies

Source: ESG's Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=280, three response accepted out of seven)

Security Challenges with Digital Transformation

Too many siloed tools and data

Which of the following represent the biggest challenges associated with managing an assortment of security products from different vendors?

Source: ESG's Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=280, three response accepted out of seven)

#3

The security staff has to aggregate results from independent security technologies, making overall security operations complex and time-consuming

Too many siloed tools and data

Which of the following represent the biggest challenges associated with managing an assortment of security products from different vendors?

Source: ESG’s Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=280, three response accepted out of seven)

#4

My organization doesn’t have enough staff or skills to manage our security technologies appropriately

How do we meet these challenges and close the gaps?

How can we meet these challenges and solve our problems?

The XDR movement is helping but gaps exist

Traditional XDR solutions often struggle to…

- Aggregate, correlate, and analyze massive amounts of security telemetry
- Provide complete cloud visibility
- Identify and stop threats underway

How can we meet these challenges and solve our problems?

The XDR movement is helping but gaps exist

Which of the following considerations would you characterize as having the most significant influence on your organization's endpoint security strategy moving forward?

#2

The need to align our endpoint security strategy with our use of cloud computing services

Source: ESG's Securing the Cloud-native Attack Surface with Unified XDR and CNAPP (Percent of respondents, N=359, two responses accepted out of nine)

How can we meet these challenges and solve our problems?

CNAPPs help unify multiple cloud security capabilities, but gaps exist…

CNAPPs lack…

- Visibility into workspaces and data center infrastructure
- Visibility and control of the software supply chain

How can we meet these challenges and solve our problems?

Unifying XDR and CNAPP to gain control at scale

Advantages of a more unified, shift up approach enables secure digital transformation to drive better business results…

- Centralized control and security consistency across environments
- Securely scale development teams and remote work
- Attack path visibility to help security teams better understand their threat exposure
- A more complete picture of software supply chain visibility
- Operational excellence and faster threat detection and remediation

The Shift Up Approach to Cybersecurity

The Five Shift Up Tenets

Structured telemetry

Collect and normalize telemetry close to its source.

Cloud power

Place security analytics processing power in the cloud.

Standards and APIs

Data models and modes of interoperability based on standards, using an API-first approach.

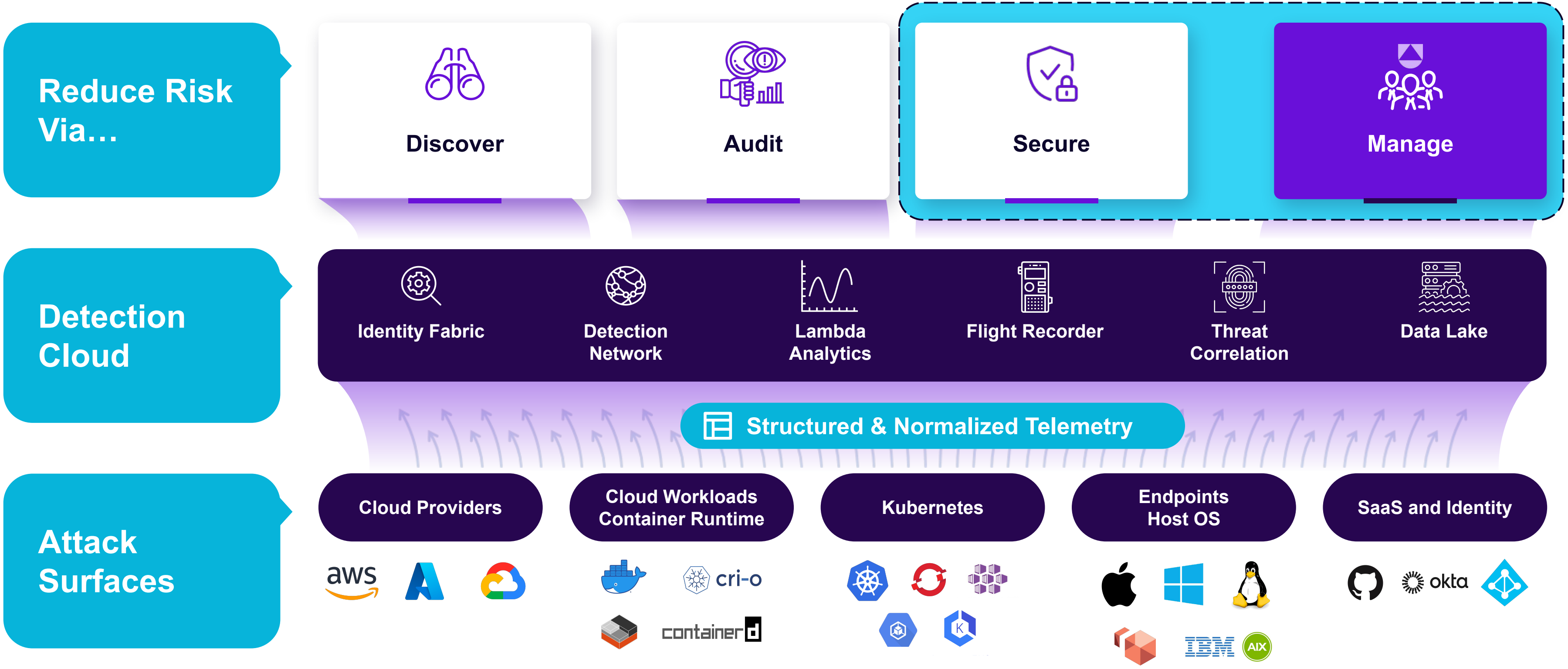
Unified data model

Provide a unified data model and UI for multiple teams and IT environments.

Service mesh

Enable composability, scalability, and interoperability for security controls.

Uptycs Unified CNAPP and XDR



Reduce Risk Via…

Discover

Audit

Secure

Manage

Detection Cloud

Identity Fabric

Detection Network

Lambda Analytics

Flight Recorder

Threat Correlation

Data Lake

Structured & Normalized Telemetry

Attack Surfaces

Cloud Providers

Cloud Workloads Container Runtime

Kubernetes

Endpoints Host OS

SaaS and Identity

Thank You

Shift up your cybersecurity with Uptycs!

- Learn more at uptycs.com

uptycs