

# CLOUDSEC 2023

ENVISION IT

클라우드 위험이 곧 비즈니스 위험입니다

Mike Milner

Hosted by



# Risk Environment

# Threat actor evolution

## Cyber Criminals



Extortion and Ransomware growing

Recession will drive more crime

Increased specialization, targeting, customization

## Nation State Actors



Disruption, destruction, IP theft

Tolerating & harboring criminals

Some regimes profit-driven  
For example, North Korea

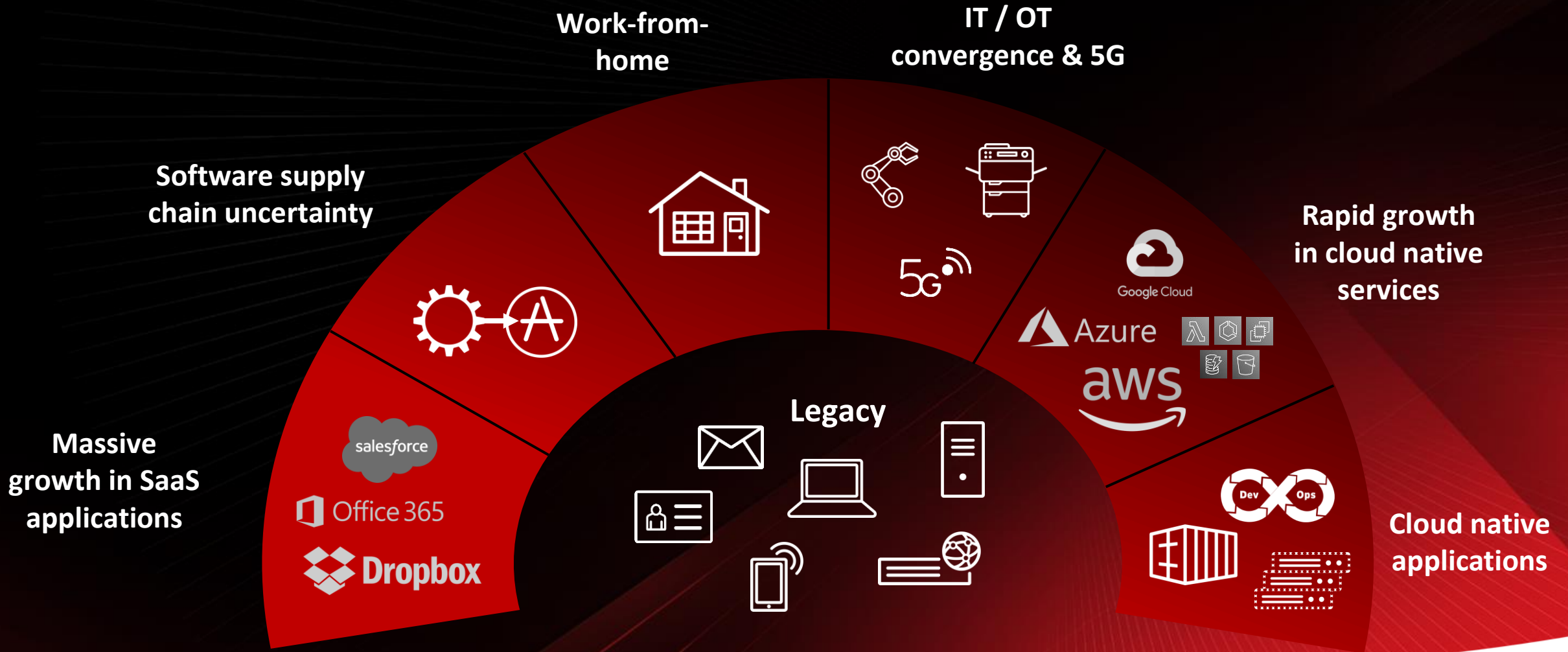
## Insiders



Economic pain will drive increased misbehavior

Cyber-criminals paying insiders for access

# Attack Surface Scale





# Security Tool Sprawl



Overlapping solutions

Siloed data and alerts

Data lake proliferation

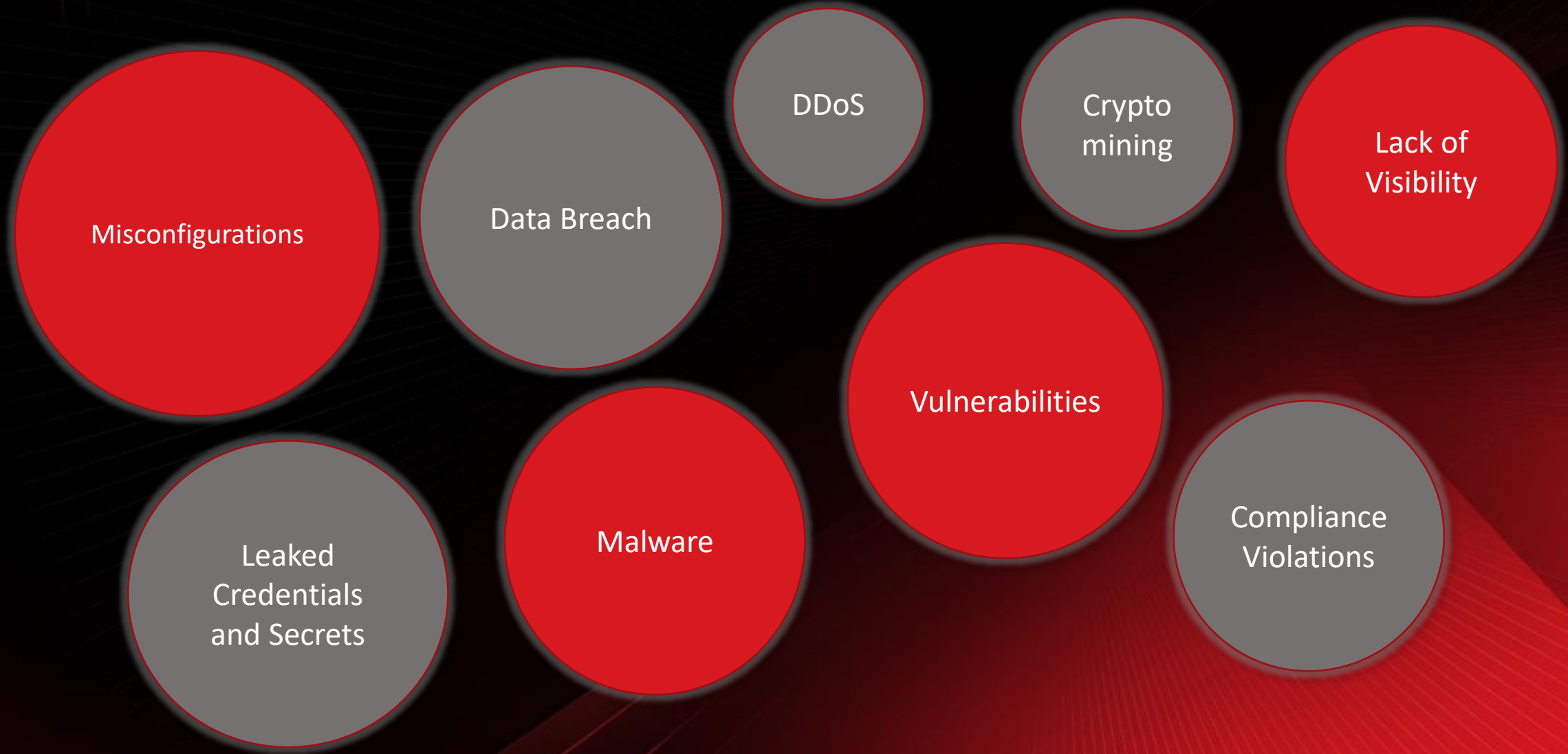
Inefficient licensing

People costs rising

**Challenging to measure effectiveness**

# Cloud Risk

# Common Security Risks in the Cloud



# Security Challenges on your Cloud Journey



## Evolving Environment

Migrating workloads and applications to the cloud-native applications



## Measuring Risk

Identifying blind spots, managing the cloud attack surface, and improving security posture



## Multi-Cloud Complexity

Achieving visibility and consistent security policy management



## Hybrid Requirements

Applying modern security tooling to legacy and on-premise workloads



## Incident Handling

Ensuring SOC visibility and contextual awareness of cloud attacks



# Cloud Security Silo



CSPM



CDR



CNAPP



IaC

# Translation

# Enterprise Security



## Attack Surface Risk Management

Incorporates cloud-focused Attack Surface discovery, assessment, and risk mitigation



## Detection and Response (XDR) + Threat Intelligence

Cloud security correlation for fast detection and response, including XDR for containers, XDR for other cloud resources, etc.



## Cloud Protection and Prevention

Discover and block vulnerabilities and malware across VMs, containers, storage, VPCs, IaC, repos, databases, and APIs.

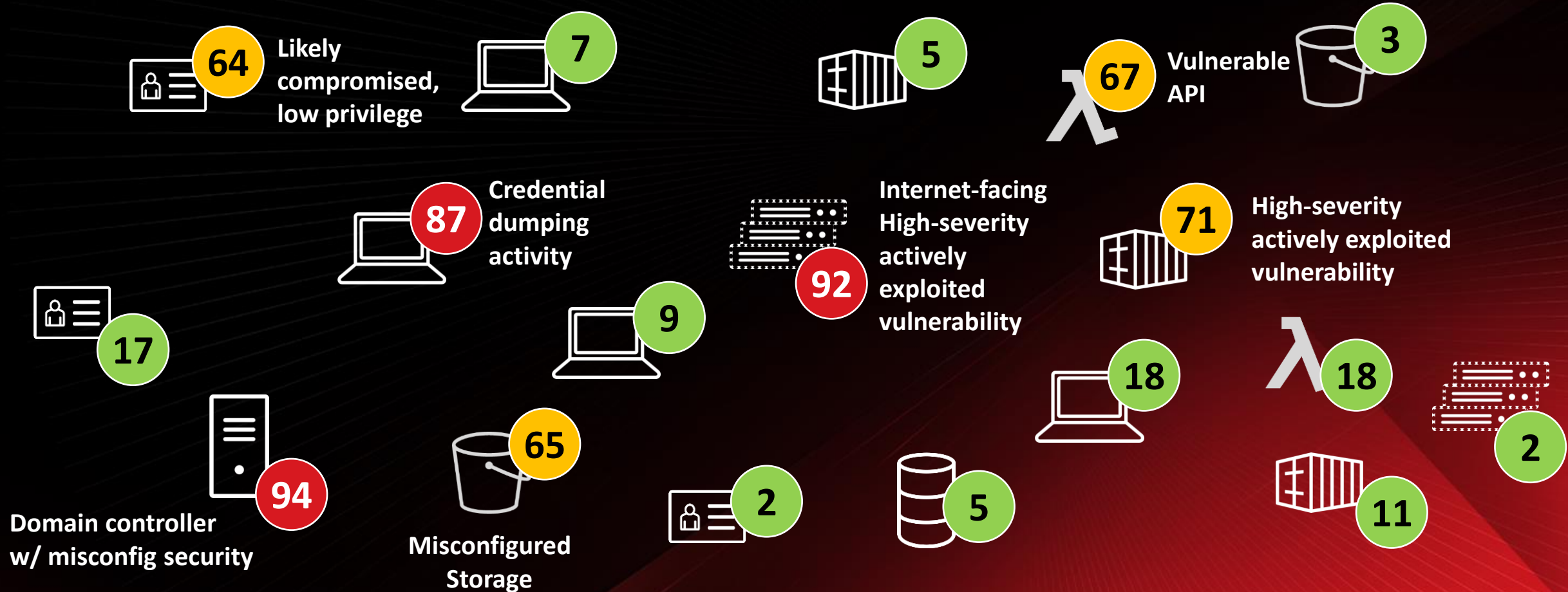
# Improve Visibility

Security Posture and Activity, across all Asset Types





# Assess Risk to Prioritize Remediation



How?

# Let your SOC do Cloud

- Bring cloud events into your detection and response activities
- Visualize cloud infrastructure and data flows
- Include SOC in cloud threat assessments

# Standardize Risk

- Consider risk across asset types
- Developers have endpoints too!
- Map the flow of code to production



# Choose the right tools

- Handle your entire attack surface
- Native sensors for fundamentals
- Integrations for specialty systems

# Trend Micro Can Help

# Trend Vision One™ – Cloud Security

Help organizations quickly identify threats, reduce breach exposure, and respond to security threats across their cloud environments



## Cloud Attack Surface Risk Management

Incorporates cloud-focused Attack Surface discovery, assessment, and risk mitigation



## Cloud Detection and Response (CDR) + Threat Intelligence

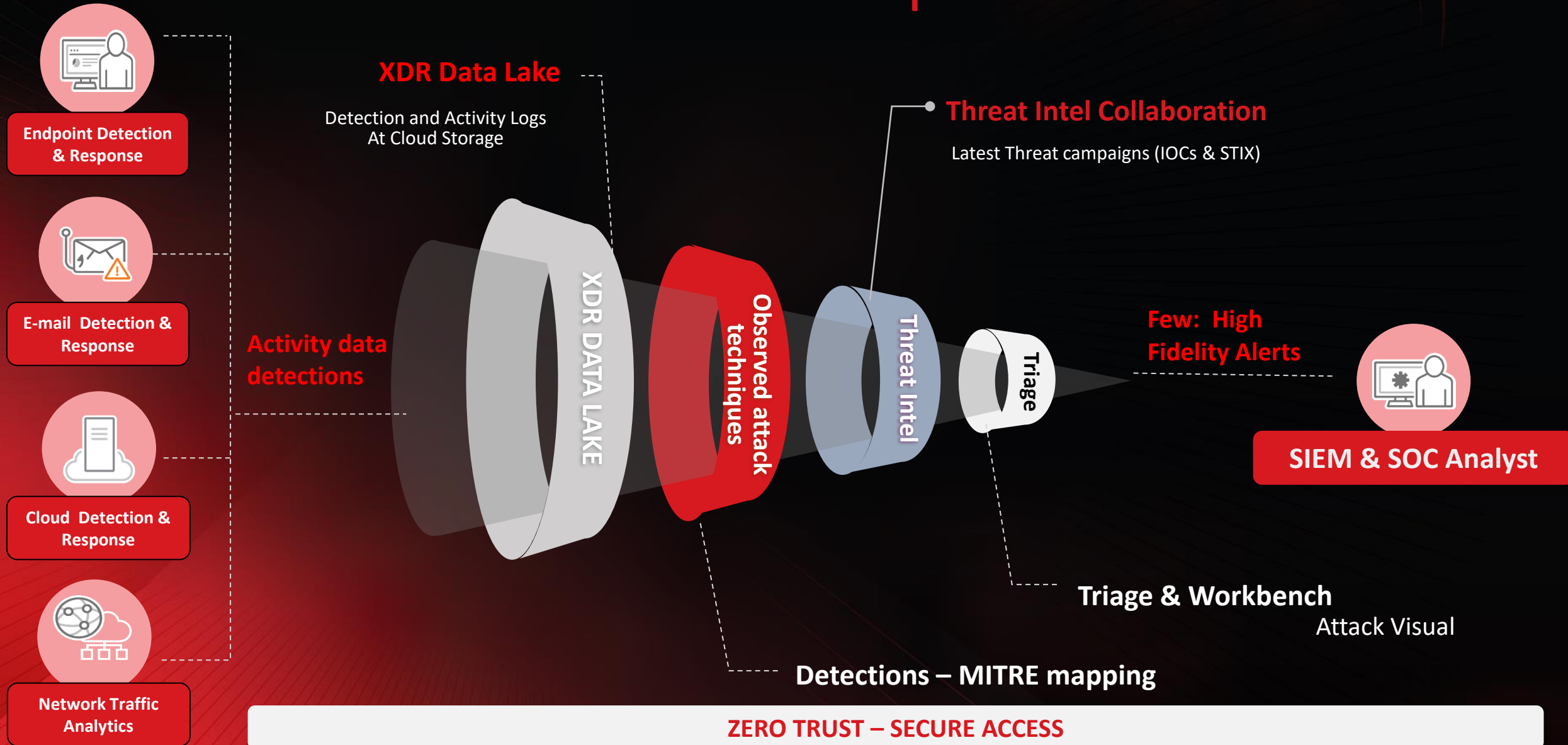
Cloud security correlation for fast detection and response, including XDR for containers, XDR for other cloud resources, etc.



## Cloud Protection and Prevention

Discover and block vulnerabilities and malware across VMs, containers, storage, VPCs, IaC, repos, databases, and APIs.

# Cloud Detection and Response





# XDR for Cloud

Cloud security correlation for fast detection and response, including XDR for containers, XDR for cloud resources, and more.

The screenshot displays three security alerts from Trend Vision One™. Each alert includes a summary, highlights, and a network diagram illustrating the event's context.

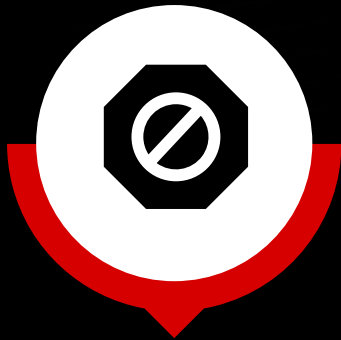
- Alert 1: -AWS IAM Policy Attached To User Or Role Or Group**
  - Summary:** An attachment of an AWS IAM policy to user or group or role was detected.
  - Score:** 26
  - Impact scope:** 1 user, 1 group
  - Created:** 2023-03-19 11:47:56
  - Owner:** None [Assign owner](#)
  - Highlights:** AWS IAM Policy Attached To A Role. Technique: T1078 - Valid Accounts. Data source / processor: Trend Cloud One - AWS CloudTrail Integration.
  - Network Diagram:** Shows a central node representing the policy attachment, connected to nodes for the policy (arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore), the user/role (arn:aws:sts::780477232234:assumed-role/AWS-QuickSetup-HostMgmtRole-ap-...), and the source IP (13.236.119.180).
- Alert 2: AWS S3 Bucket Data Exfiltration**
  - Summary:** A possible data exfiltration from AWS S3 bucket that may result to stolen confidential data was identified.
  - Score:** 43
  - Impact scope:** 1 user
  - Created:** 2023-05-12 19:33:38
  - Owner:** None [Assign owner](#)
  - Highlights:** AWS S3 Bucket Listing. Technique: T1580 - Cloud Infrastructure Discovery. Data source / processor: Trend Cloud One - AWS CloudTrail Integration.
  - Network Diagram:** Shows a central node for the bucket listing event, connected to nodes for the user (arn:aws:iam::218213273676:user/not-attacker), the bucket (AKIATFTUGKBGDRJO4AR5), and the source IP (47.161.29.12).
- Alert 3: AWS S3 Object Sync**
  - Summary:** (Not explicitly shown in the summary box, but implied by the highlights).
  - Score:** (Not explicitly shown).
  - Impact scope:** (Not explicitly shown).
  - Created:** (Not explicitly shown).
  - Owner:** (Not explicitly shown).
  - Highlights:** AWS S3 Object Sync. Technique: T1530 - Data from Cloud Storage. Data source / processor: Trend Cloud One - AWS CloudTrail Integration.
  - Network Diagram:** Shows a central node for the object sync event, connected to nodes for the user (arn:aws:iam::218213273676:user/not-attacker), the bucket (AKIATFTUGKBGDRJO4AR5), and the source IP (47.161.29.12).

# Setting a New Standard for Cybersecurity Platforms

Unified Security for Greater Threat Defense and Security Posture

Earlier detection. Faster response. Reduced Risk.

*Stop adversaries  
faster*



**Market-leading XDR**

*Take charge of  
cyber risks*



**Most robust attack surface  
risk management**

*Converge, simplify,  
harmonize SecOps*



**Broadest, single  
platform**



**Mike Milner**

**VP Cloud Technology**

**mike\_milner@trendmicro.com**

**@secretmike**