DELL Technologies

Secure Your Digital Transformation Journey

Samer El Kodsi

Senior Director Channel Sales – Emerging Markets

Palo Alto Networks

It Can Feel Like Attackers Have the Upper Hand

Their opportunity expands with every new trend

Effort to execute an attack is going down

They only have to be right once

Cybersecurity Is Possible with Three Core Principles

Incredible Tech

AI and Automation

Native Integration

Our Next-Gen Platforms and Services Are Designed to Keep You Ahead of What's Next

Network Security

STRATA | PRISMA SASE

Best-in-class security delivered across hardware, software and SASE

Cloud Security

PRISMA CLOUD

Comprehensive platform to secure everything that runs in the cloud

Security Operations

CORTEX

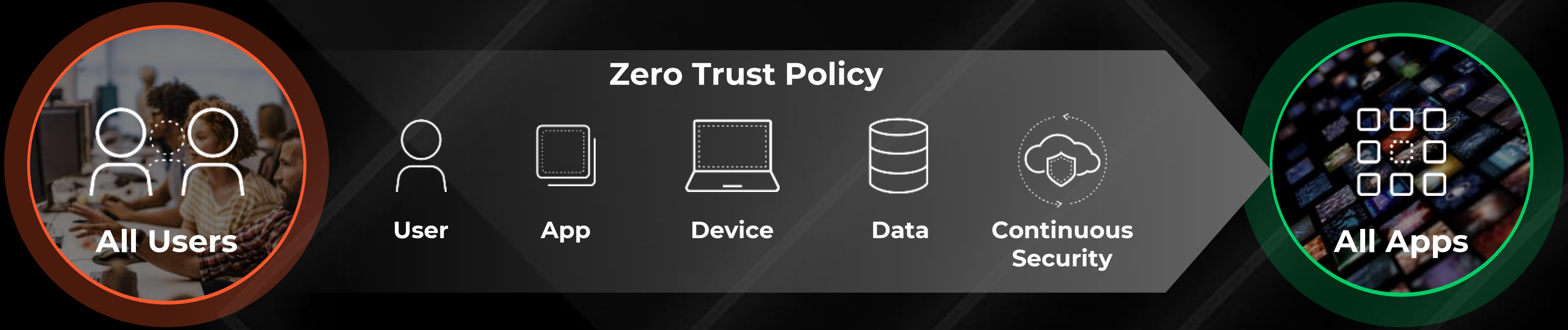
A new approach to SOC with fully integrated data, analytics and automation

Threat Intel, Incident Response and Advisory Services

World-renowned threat intelligence, cyber risk management and advisory services

NETWORK SECURITY

Conceptually, Zero Trust Is Very Simple



All Users

Zero Trust Policy

User

App

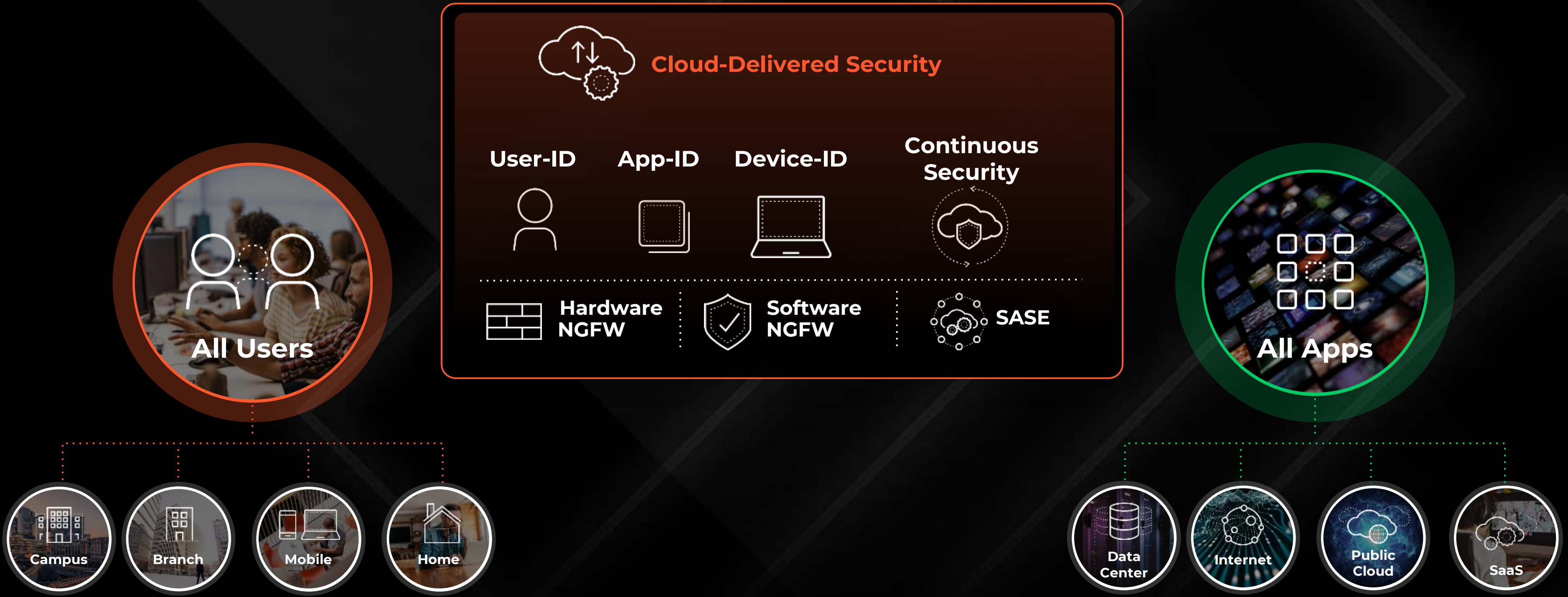
Device

Data

Continuous Security

All Apps

Enterprise Zero Trust Is Only Possible with a Platform



Cloud-Delivered Security

User-ID

App-ID

Device-ID

Continuous Security

Hardware NGFW

Software NGFW

SASE

All Users

Campus

Branch

Mobile

Home

All Apps

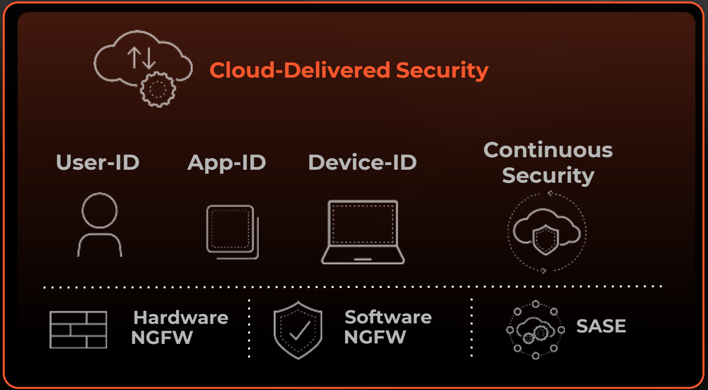
Data Center

Internet

Public Cloud

SaaS

Incredible Outcomes for the Entire Enterprise With A Platform Approach



Cloud-Delivered Security

User-ID

App-ID

Device-ID

Continuous Security

Hardware NGFW

Software NGFW

SASE

Best-in-class security

for all users and applications

Integrated security services

across hardware, software and SASE

Optimized end-user experience

at all locations

Unified

security operations

Superior Protection With Cloud-Delivered Security Services

Good Data Makes for Great AI

Our Security Services have a tremendous Network effect

Each day we analyze

3.5 billion

new and unique events

AI + ML Deliver Zero-Day Detection

The escalating threat landscape requires a new approach

Each day we detect

275,000

new and unique attacks that weren't there the day before

Attack Prevention Happens Inline

Moving detection inline prevents even the first attack

Each day we block* nearly

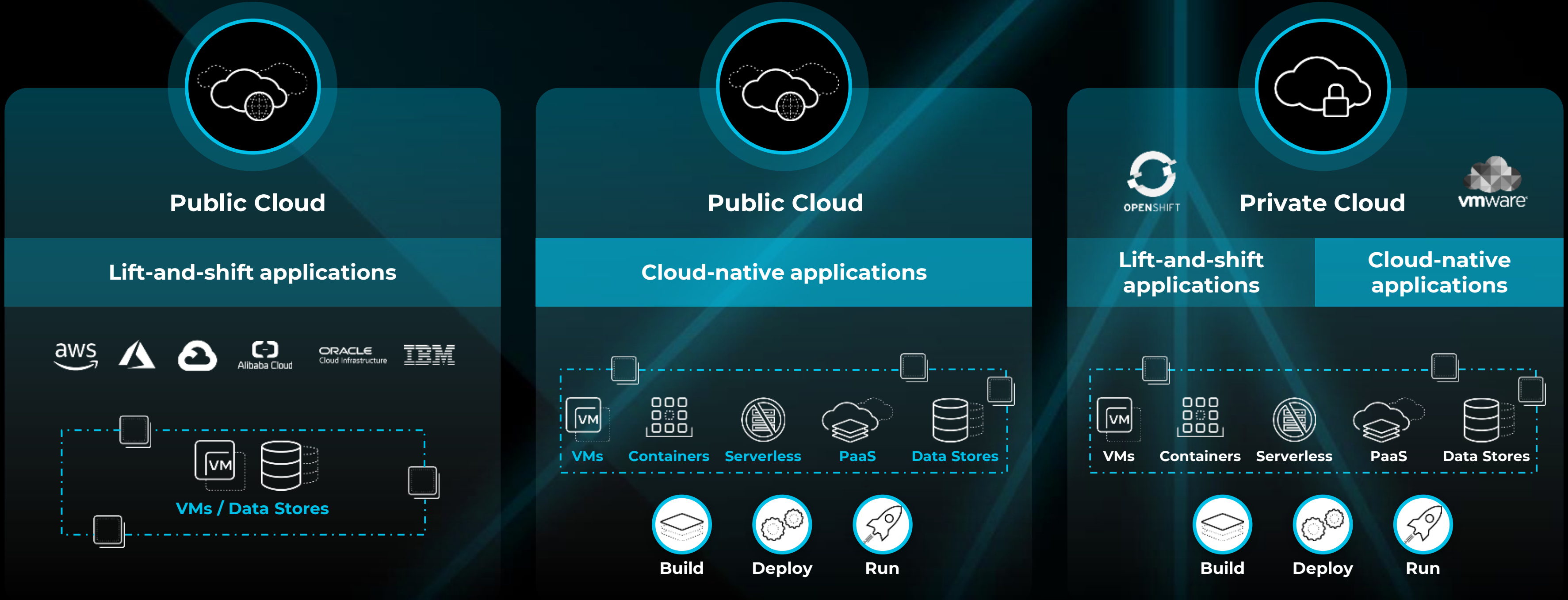
5 billion

attacks

*estimated by averaging # preventions per FW where telemetry is enabled by the total # firewalls in use

Cloud Security

Applications Are Increasingly Cloud-Native, Multicloud and Hybrid



Public Cloud

Lift-and-shift applications

VMs / Data Stores

Public Cloud

Cloud-native applications

VMs, Containers, Serverless, PaaS, Data Stores

Build, Deploy, Run

Private Cloud

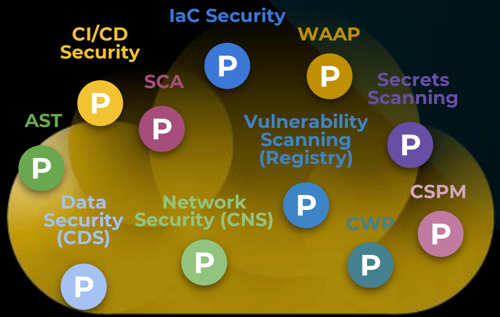
Lift-and-shift applications

Cloud-native applications

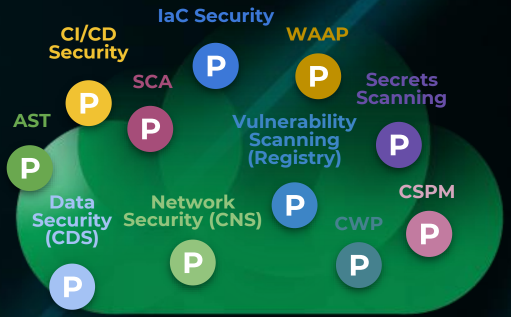
VMs, Containers, Serverless, PaaS, Data Stores

Build, Deploy, Run

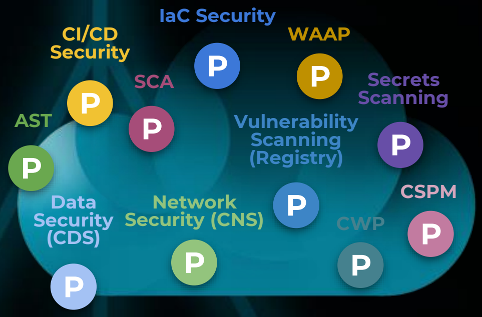
The Typical Industry Response Is to Address with Point Products



AWS



GCP



Azure

Three Core Pillars To Cloud Security

Secure App Development

Proactively address issues during dev/devops

Secure Deployment

Secure app & cloud infrastructure configuration

Real-Time Attack Protection

Runtime protection from active attacks

The Results Speak for Themselves

100M+
Cloud resources

100K+
Containers

>38K
Open source libraries

10K+
Repos

ZERO Major incidents

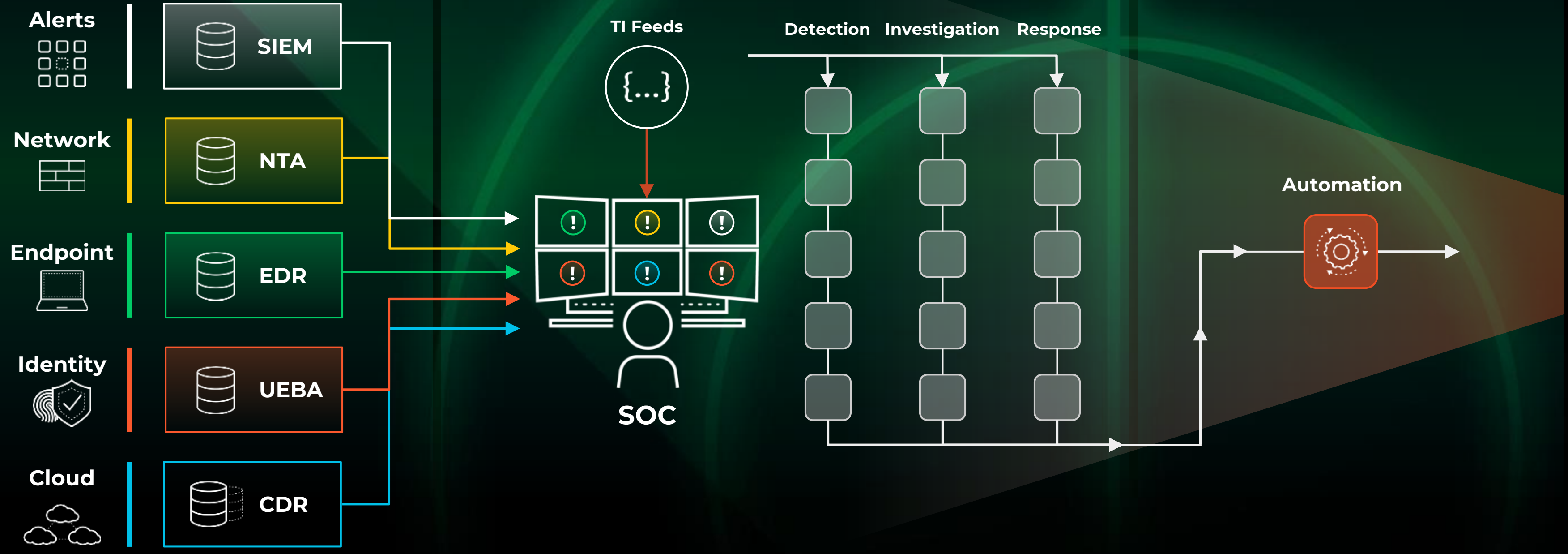
Security Operations

Why Can’t SOCs Stop Attacks in Real Time?

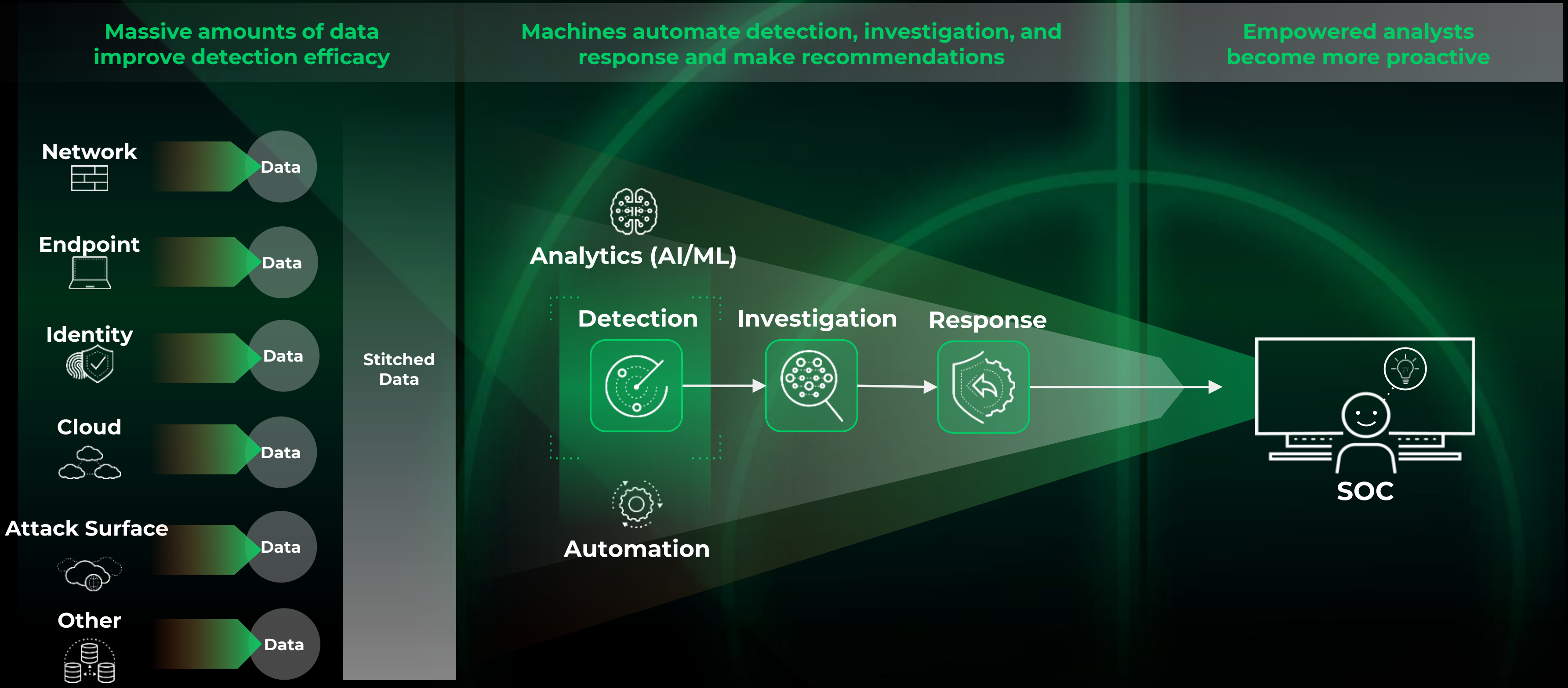
Too many data silos make it hard to detect attacks

Teams build and maintain detection content, use multiple tools to manually investigate & respond

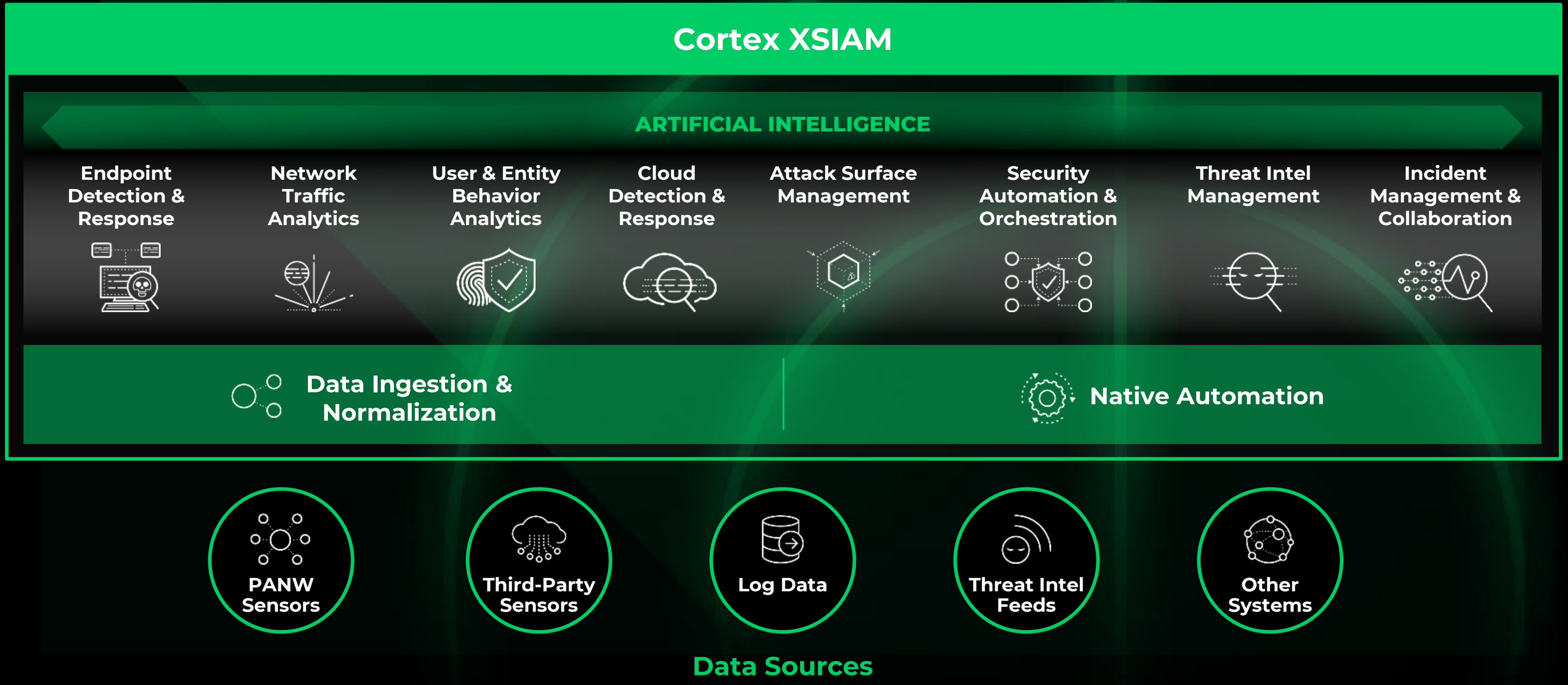
Automation is bolted on at the end to scale it



We Must Transform the SOC to be Machine-led, Human Empowered


Massive amounts of data improve detection efficacy
Machines automate detection, investigation, and response and make recommendations
Empowered analysts become more proactive
Network
Data
Endpoint
Data
Identity
Data
Cloud
Data
Attack Surface
Data
Other
Data
Stitched Data
Analytics (AI/ML)
Detection
Investigation
Response
Automation
SOC

XSIAM Completely Reimagines How the SOC Works



Cortex XSIAM

ARTIFICIAL INTELLIGENCE

Endpoint Detection & Response

Network Traffic Analytics

User & Entity Behavior Analytics

Cloud Detection & Response

Attack Surface Management

Security Automation & Orchestration

Threat Intel Management

Incident Management & Collaboration

Data Ingestion & Normalization

Native Automation

PANW Sensors

Third-Party Sensors

Log Data

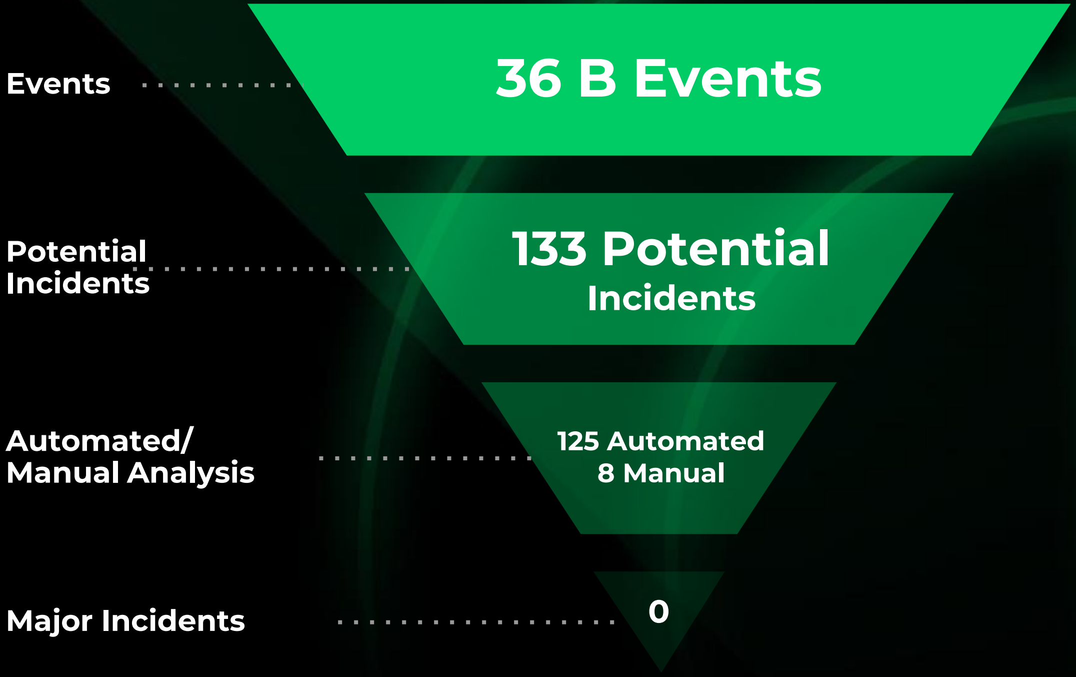
Threat Intel Feeds

Other Systems

Data Sources

What Our SOC Has Achieved With Cortex XSIAM

WHAT'S POSSIBLE WITH THE AUTOMATED SOC



Events — 36 B Events

Potential Incidents — 133 Potential Incidents

Automated/ Manual Analysis — 125 Automated 8 Manual

Major Incidents — 0

10 SECONDS

Mean Time to Detect

1 MINUTE

Mean Time to Respond
(High priority)

Thank You