



IT NATION™

SECURE

hosted by  CONNECTWISE

# How EDR and SIEM Deliver Faster and More Efficient Security Protections

Roopak Patel



IT NATION™ **SECURE**

# Agenda

**1** Current challenges and key trends

**2** Common problems solved today

**3** Improving the approach

**4** ConnectWise approach

**5** Near-term deliverables (EDR + SIEM)

**6** Broader strategy (with details)

# Current Challenges and Key Trends

Driving forces behind new platforms, product convergence, and new technologies

Lack of skilled resources  
Not enough hunters



Convergence  
Multi-cloud  
Data lakes / mesh



Cybersecurity risk  
Org resilience

Attack surface complexity  
Ransomware  
OT weaponization



Automation  
Decentralized  
As A Service



Regulations  
Insurance  
Data privacy

# Modern Security Challenges

A Day in the Life of a SOC Analyst

## Novel Malware

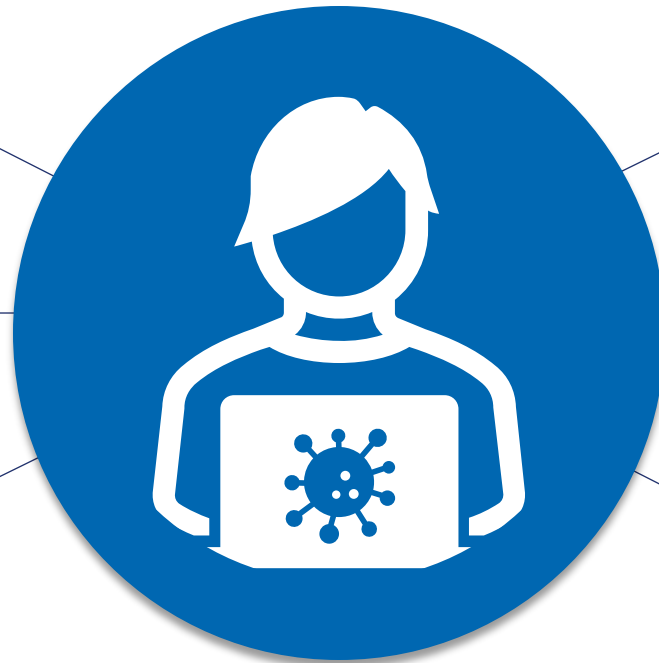
1.1M novel malware created daily

## Siloed Products

40+ point products in SOC

## Data Ingest

Filtering noise out of alerts



## Manual Data Collection

Endpoint, network, cloud, apps, user

## Alert Fatigue

11,000 alerts per day

## Automation

Only 17% of alerts are touched

# Evolution of Security Platform Technology—Improving the Approach

## SIEM

- First-pillar product collects data from variety of sources
- Analytics evolved from basic correlation to ML/AI
- Extensive hunting
- Lacked easy investigation, orchestration, and response
- Bridged gaps by plugging in EDR, SOAR, threat platforms, etc.

## EDR

- First cloud-native product to provide integrated detect, investigate, and respond UX (solved gap in SIEM UX)
- Analytics built in age of MITRE, extensive use of ML, anomaly detection
- Expanded with APIs and integrations with other data sources (SIEM, email, web, etc.)
  - **Alerts combine with endpoint events into prioritized incident**
  - More complete investigation picture to understand endpoint incident
  - Response workflows trigger actions beyond endpoint (e.g., network quarantine)

## SIEM + EDR

- Evolving, but general definition
  - Cloud-native solution built on modern data lake and analytics architectures
    - EDR: Early advantage and market leaders
    - Cloud-native SIEM
    - Or both
- Must have at least:
  - EDR
  - Additional primary sources natively connected (email, web, cloud, network, identity)
  - SIEM/log source data (native or 3rd party API connectors)
- Extending upon baseline EDR UX (alerts, incidents, investigation, hunting, triage, remediation)
- Expanding to include risk, resiliency, recovery, automation across natively integrated products

# Extended Detection and Response (XDR)

## XDR Generic Definition

*“Extended Detection and Response (XDR) is a security threat detection and incident response capability that natively integrates multiple security products into a cohesive security operations system.”*

## XDR = EDR + NIDS

- Most security interpret the definition of XDR as an advanced version of EDR.
- EDR on its own is restricted to looking at the endpoint and misses out on the intelligence that can be gathered from the network
- By adding the network visibility capabilities of a network-based IDS (NIDS), users get the ability to:
  - Gain visibility and protection across non-managed machines (the ones without the EDR agent deployed)
  - The ability to confirm or deny a possible attack by correlating the endpoint detection from the EDR with the network detection from the NIDS.

## ConnectWise SIEM 3.0 Approach

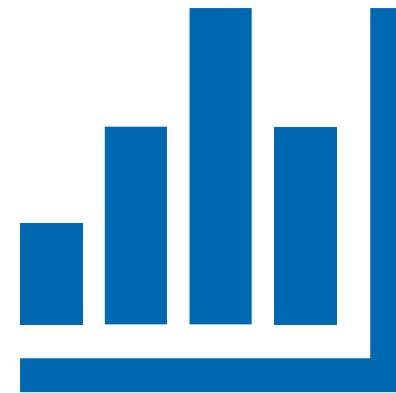
- ConnectWise SIEM delivers on XDR use cases.
- ConnectWise SIEM uses its own network sensor that is part of the SIEM as the network sensor to provide network visibility and detections. The network sensor receives regular CRU updates to signatures.
- CRU signature updates are unique in the market and focused on MSP relevant threats, protecting MSPs and their customers specifically.
- Integrates with multiple EDRs including SentinelOne, Bitdefender, CrowdStrike, Cylance, etc.
- ConnectWise also integrates with over 70 additional data sources for threat detection and attack context.

# Near-Term Deliverables

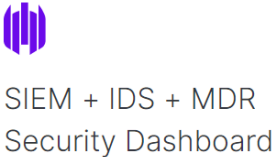


# New EDR + IDS Dashboards


- Shows value of combining high-fidelity alert information
- Targeted to assist with investigations



# EDR + IDS: Threat Details



### Sentinel One New Threats



- Malware
- PUA
- Hacktool
- Adware

### S1 New Threats

Threat	IP	File Path	Hash	Process Arguments	Count
Malware	10.10.1.137		841c8eec4c2fe2240b85d23c8f37581e9253126e	N/A	2
Malware	10.10.1.137		ae197ca540c814e1f9a311be6db37af534efd0ad	N/A	2
Malware	10.10.1.137	j\fonts\ZipV1c.exe	2b90dc9a28d9cc94c0f064d39ce7fa01a92b73ce	N/A	1
Malware	10.10.1.137	or\Adobe Acrobat 7.0 Professional - Keygen by PARADOX 2004.exe	ee2dd7a7db919336df9d2cce6a0d529939455889	N/A	1
Malware	10.10.1.137	Converter Full\Crack\CrackCopyMeToInstallDirAndRun.exe	743073d2a6fdaba0f2e0bd175470619132ea884f	N/A	1
Malware	10.10.1.137		ae197ca540c814e1f9a311be6db37af534efd0ad	N/A	1

### Sentinel One New Threats Details

Time	agentDetails.lastIpToMgmt	agentDetails.computerName	threatDetails.classification	threatDetails.filePath	primaryDescription	threatDetails.fileContentHash	data.escapedMaliciousProcessArguments
> Apr 24, 2023 @ 13:38:38.495	10.10.1.137		Malware		\Quarantine\C\Program Files\MyPC Backup\MyPC Backup.exe	182d4dcb2c2f31e7d971ac4456f4a1be22fa6a	-
> Apr 24, 2023 @ 02:23:20.089	10.10.1.137		Malware		Total Video Converter Full\Crack\CrackCopyMeToInstallDirAndRun.exe	743073d2a6fdaba0f2e0bd175470619132ea8	-

### IDS Alerts

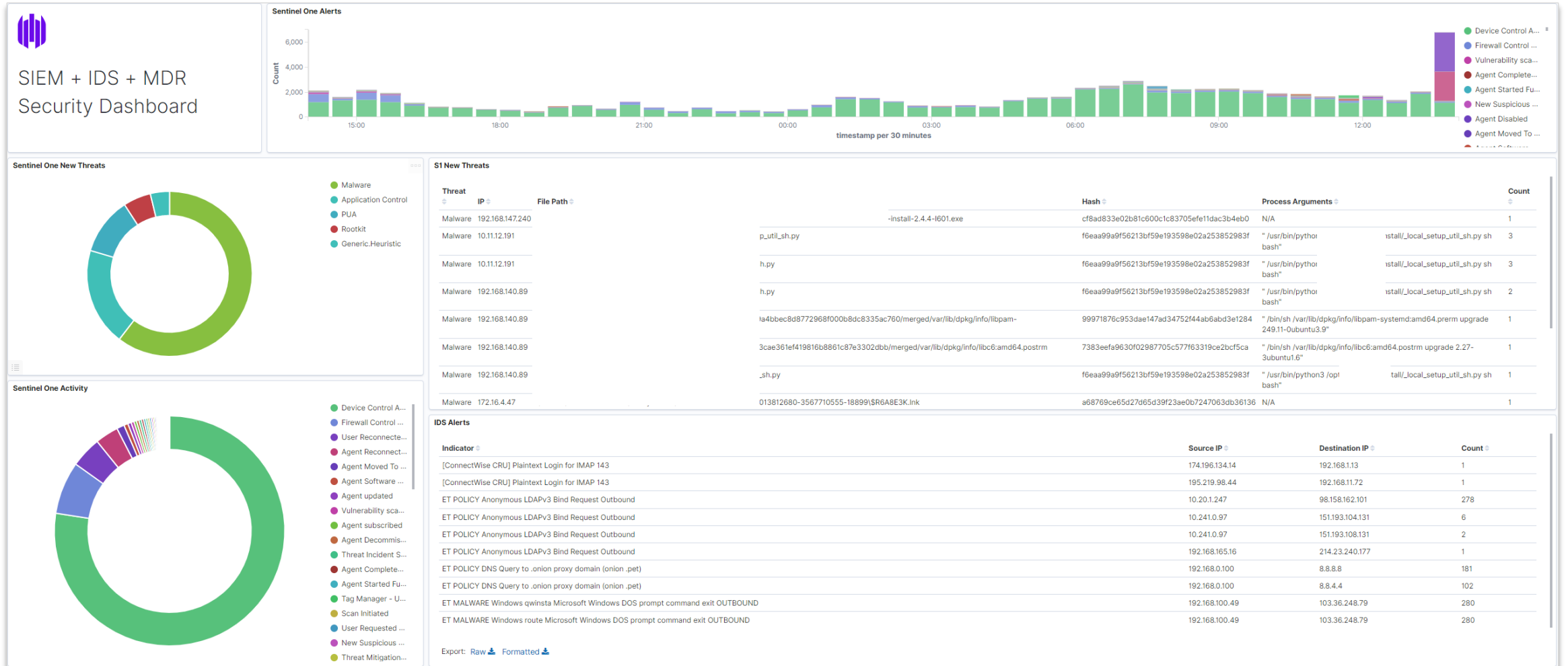
Indicator	Source IP	Destination IP	Count
ET MALWARE Antibody Software Installed (PUA)	10.10.1.137	104.156.52.74	1

Export: [Raw](#) [Formatted](#)

### Windows Least Common Process Command Line

Least Common Process Command Line	Count
/N /P --UseSystemFonts /Q:15	1
-i -cDir ASMedia_USB_Controller -o 5KBB7_temp.xml	1
-i -cDir ASMedia_USB_Controller -o CRNY0_temp.xml	1
-i -cDir ASMedia_USB_Controller -o DZMOX_temp.xml	1
-i -cDir ASMedia_USB_Controller -o IC3J7_temp.xml	1
-i -cDir ASMedia_USB_Controller -o UC184_temp.xml	1
-i -cDir RLtek_Ethernate -o 5KBB7_temp.xml	1
-i -cDir RLtek_Ethernate -o CRNY0_temp.xml	1
-i -cDir RLtek_Ethernate -o DZMOX_temp.xml	1
-i -cDir RLtek_Ethernate -o IC3J7_temp.xml	1

# EDR + SIEM: Summary



# SIEM: New Integrations

## Microsoft Azure (new)

- ConnectWise now covers M365 across all of OneDrive, SharePoint, AD, and Azure
- Requires Microsoft Event Hub
- Azure Tenant Audit logs
- Sign-in logs
- Provisioning logs
- Risky user logs
- Risk detections logs

## Microsoft O365 Monitoring (existing)

### Data-Only Integrations

- **Exium:** monitoring SASE activity across secure internet access and secure private access
- **DNS Filter:** new data source for DNS activity monitoring

*Comprehensive coverage  
of M365 environments*

# Easily View Azure Alert and Activity Sources

Top Users

Azure Top UserID

Export

UserId.keyword: De...	Count
app@sharepoint	38,626
Unknown	11,598
NOT-FOUND	6,106
System	4,161
	3,757
	2,915
	2,667
	2,187
	2,031

< 1 2 3 4 5 ... 500 >

Top Workload

Azure Top Workload

Export

Workload.keywor...	Count
OneDrive	93,256
SharePoint	73,825
Exchange	71,302
AzureActiveDirectory	26,000
CRM	17,037
MicrosoftTeams	16,989
Endpoint	10,354
SecurityCompliance...	6,399
CompliancePosture...	4,161

< 1 2 3 >

Top Operations

Azure Top Operations

Export

Operation: Descending	Count
FilePreviewed	24,537
FileAccessed	21,503
MailItemsAccessed	19,584
CrmDefaultActivity	17,037

Export

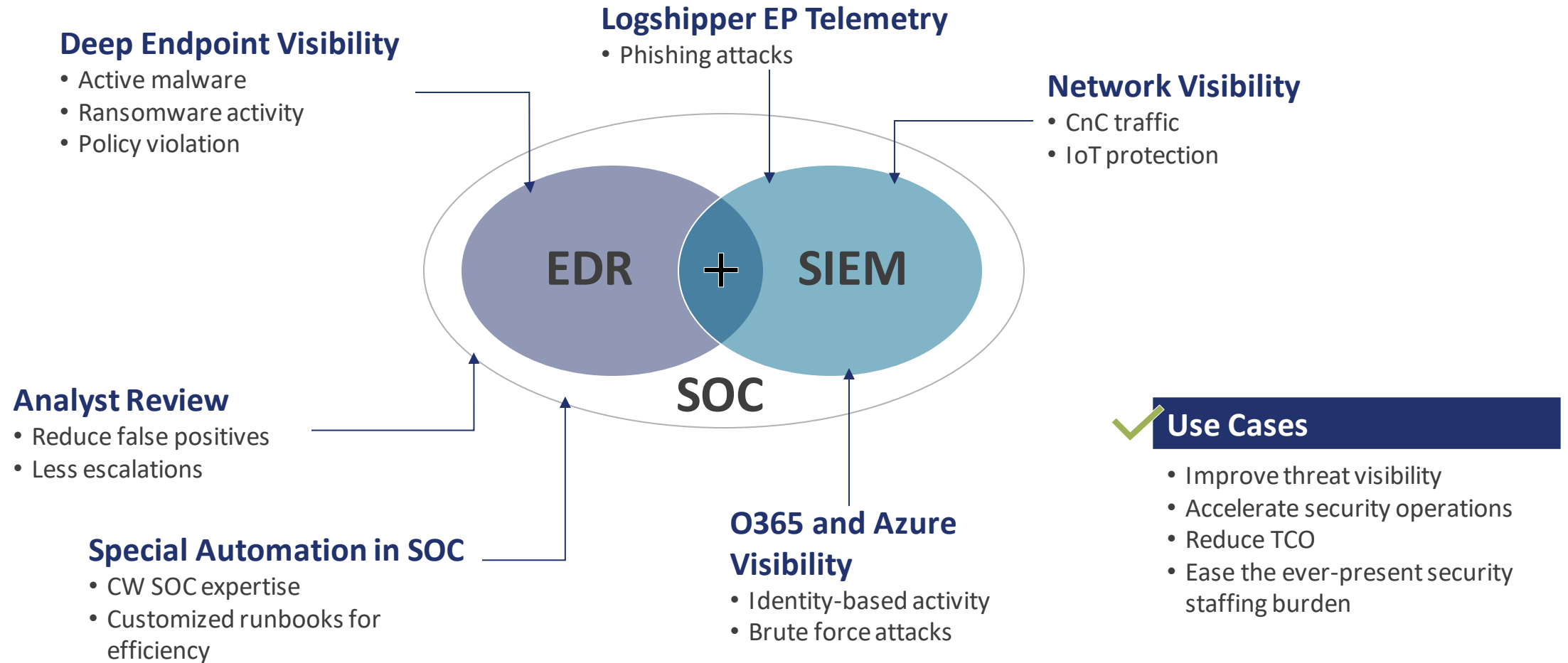
geoiip.country_...	Count
United States	237,916
Canada	11,464
India	4,428
United Kingdom	3,739
Ireland	2,462
France	1,906
China	1,898

5 ... 24 >

# Broader Strategy

# Use Cases and Visibility

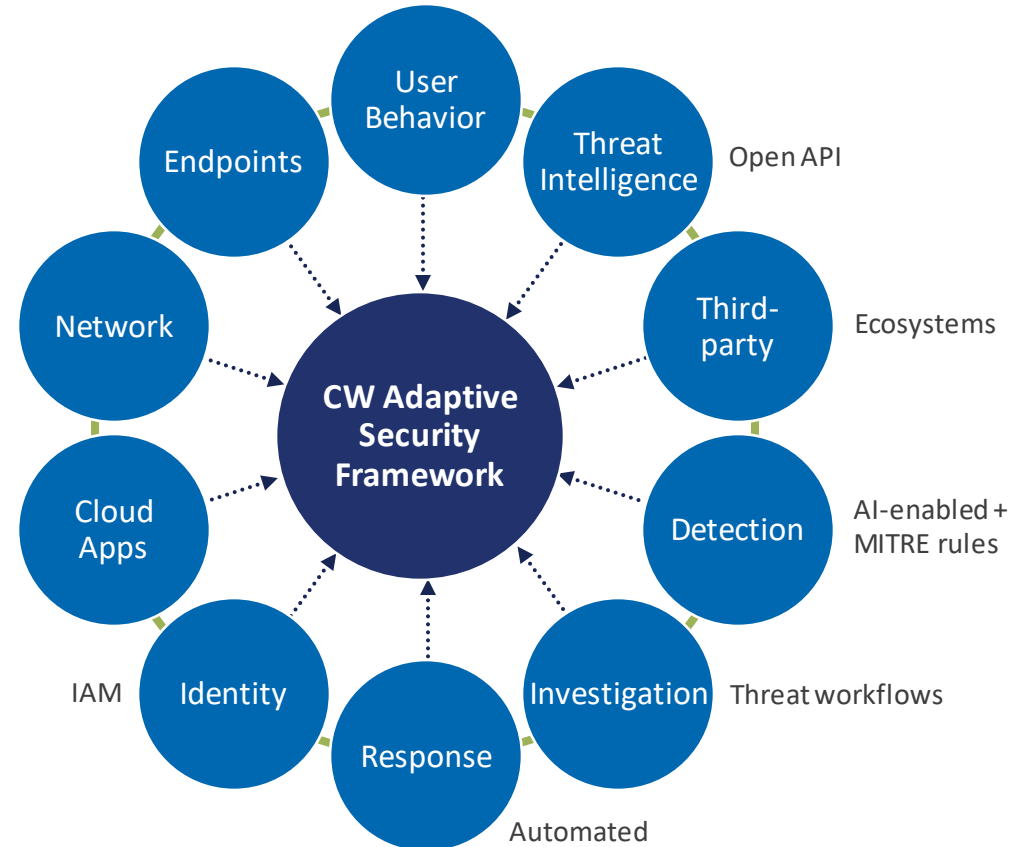
## What is the Adaptive Security Framework?



# Unified Cloud-Native Platform Approach

## Flexible and Adaptive

- Cloud-native SIEM platform
- Leverage and connect native products with essential third-party sources
- Open and seamless data ingestion, correlation, and enrichment
- Advanced threat detection rules
- Pre-built actionable threat workflows
- Orchestrated and automated response

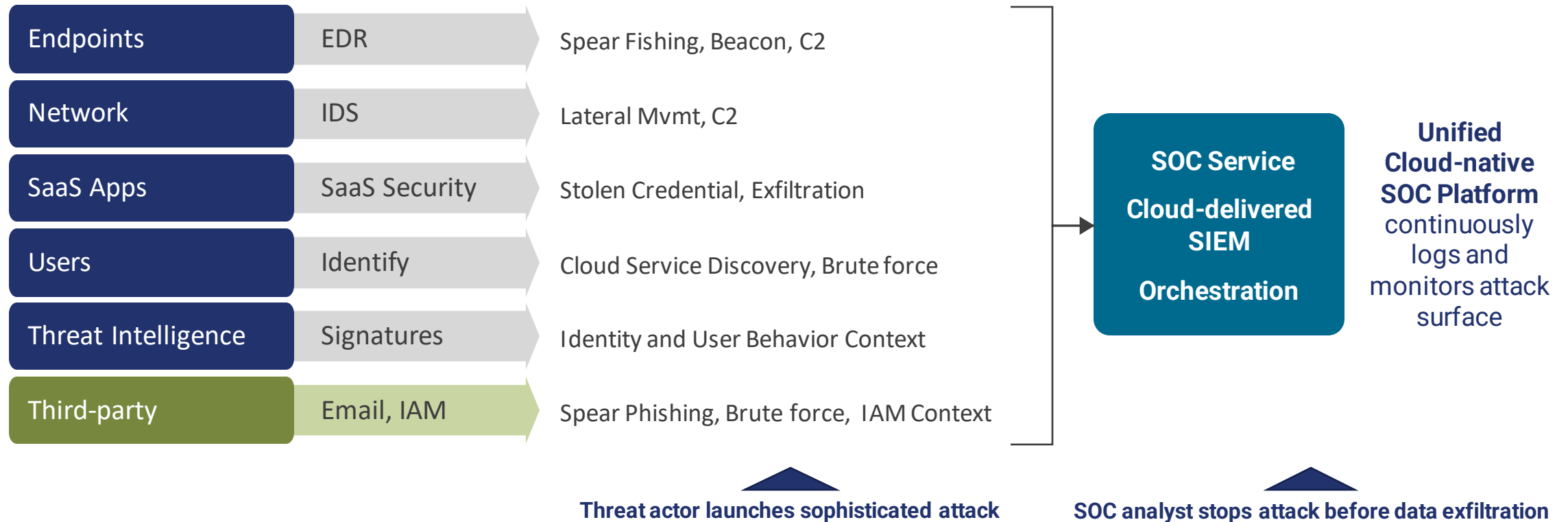


Recon	Resource Dev	Initial access	Execution	Persistence	Priv Esc	Defense Evasion	Credential access	Discovery	Lateral Mvmt	Collection	C2	Exfiltration	Impact
-------	--------------	----------------	-----------	-------------	----------	-----------------	-------------------	-----------	--------------	------------	----	--------------	--------



# Attack Kill Chain and Adaptive Framework In Action

## Attack Anatomy: MITRE ATT&CK Kill Chain Analytics



Recon	Resource Dev	Initial access	Execution	Persistence	Priv Esc	Defense Evasion	Credential access	Discovery	Lateral Mvmt	Collection	C2	Exfiltration	Impact
-------	--------------	----------------	-----------	-------------	----------	-----------------	-------------------	-----------	--------------	------------	----	--------------	--------

# Adaptive Security with ConnectWise SIEM™ & Asio™ as our Vision



## ConnectWise Approach

CW MDR + CW Co-managed SIEM

- 24x7 SOC with MSP focused security analysts
- MSP-focused threat intelligence through dedicated research team (CRU)
- Multiple consumption models



## Other Market Solutions

- Limited visibility (single vendor focus)
- Limited MSP-focused threat intelligence
- Requires full set of modules to work

# Summary

**1** Current challenges and key trends

**2** Common problems solved today

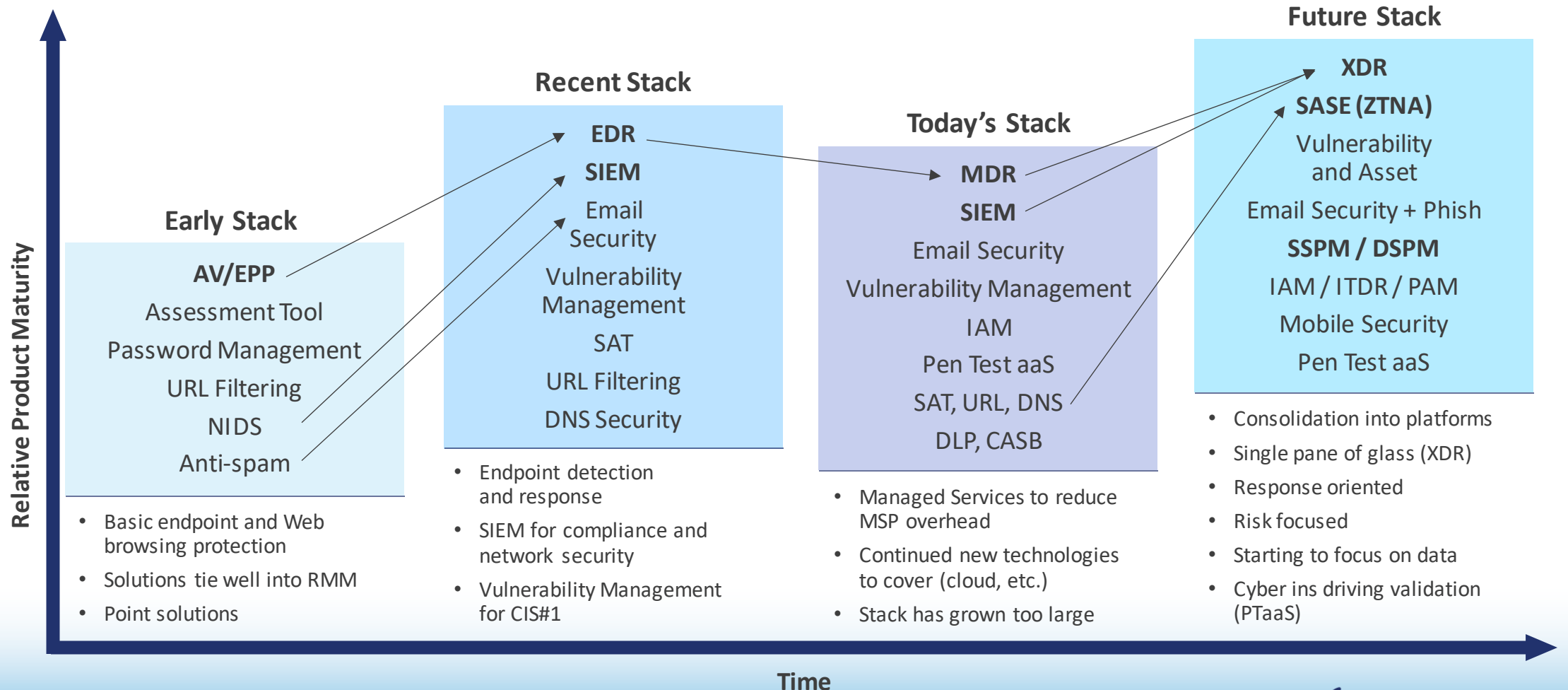
**3** Improving the approach

**4** ConnectWise approach

**5** Near-term deliverables (EDR + SIEM)

**6** Broader strategy (with details)

# MSP Security Trends



*Don't forget to fill out your*

# **SESSION SURVEY**