# Unlock the MSSP/SOC Efficiency w/Cyfusion

Respond Remotely, Right on Time

Logsign Cyfusion

Logsign Cyfusion is a comprehensive platform that enables you to oversee and handle security incidents for your customers from a single, centralized hub.

View, analyze, and promptly respond to all incidents taking place in your customers' environments. Additionally, you can utilize the platform to monitor service status and system health in real-time, ensuring optimal performance and functionality across the hub.
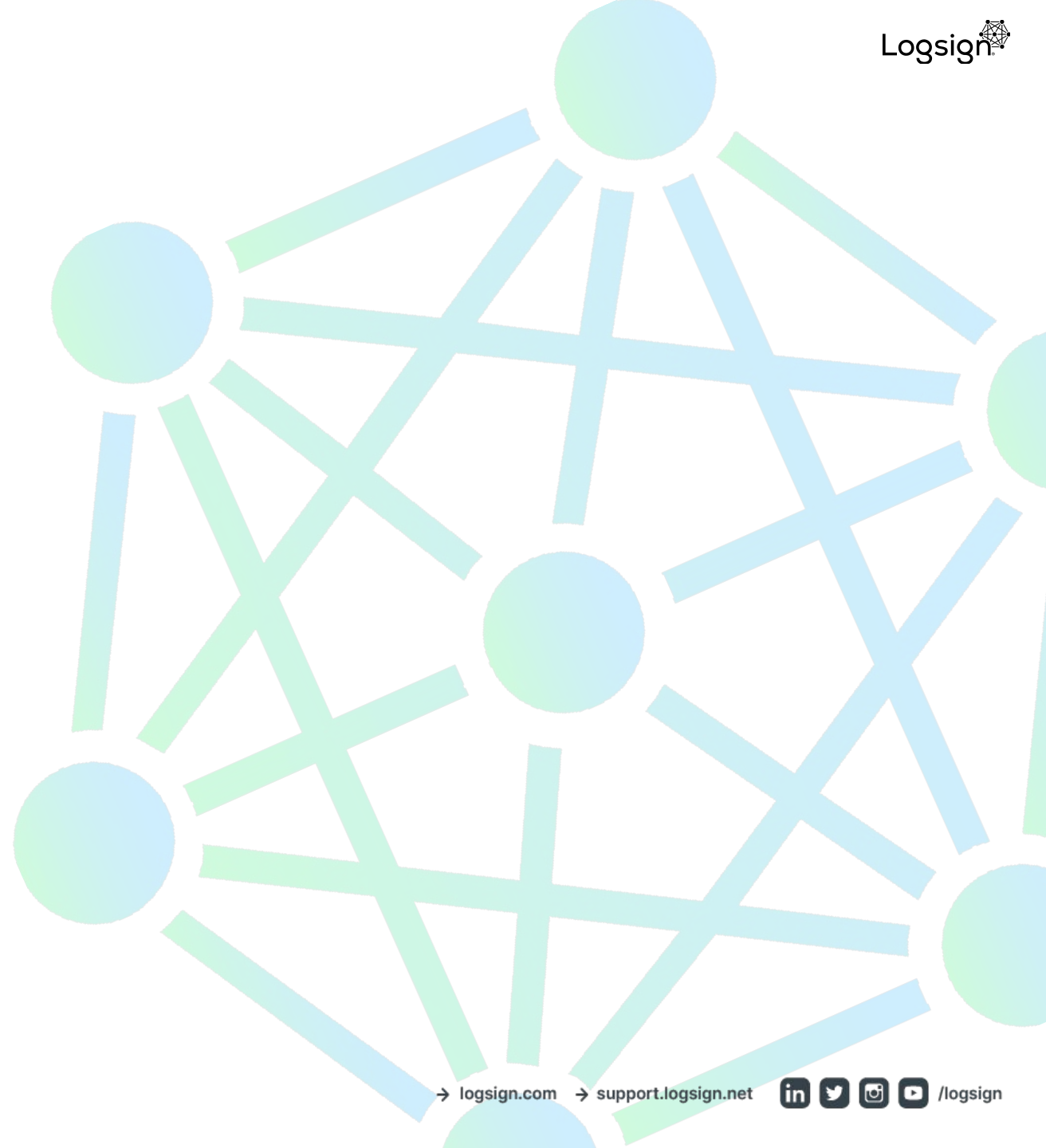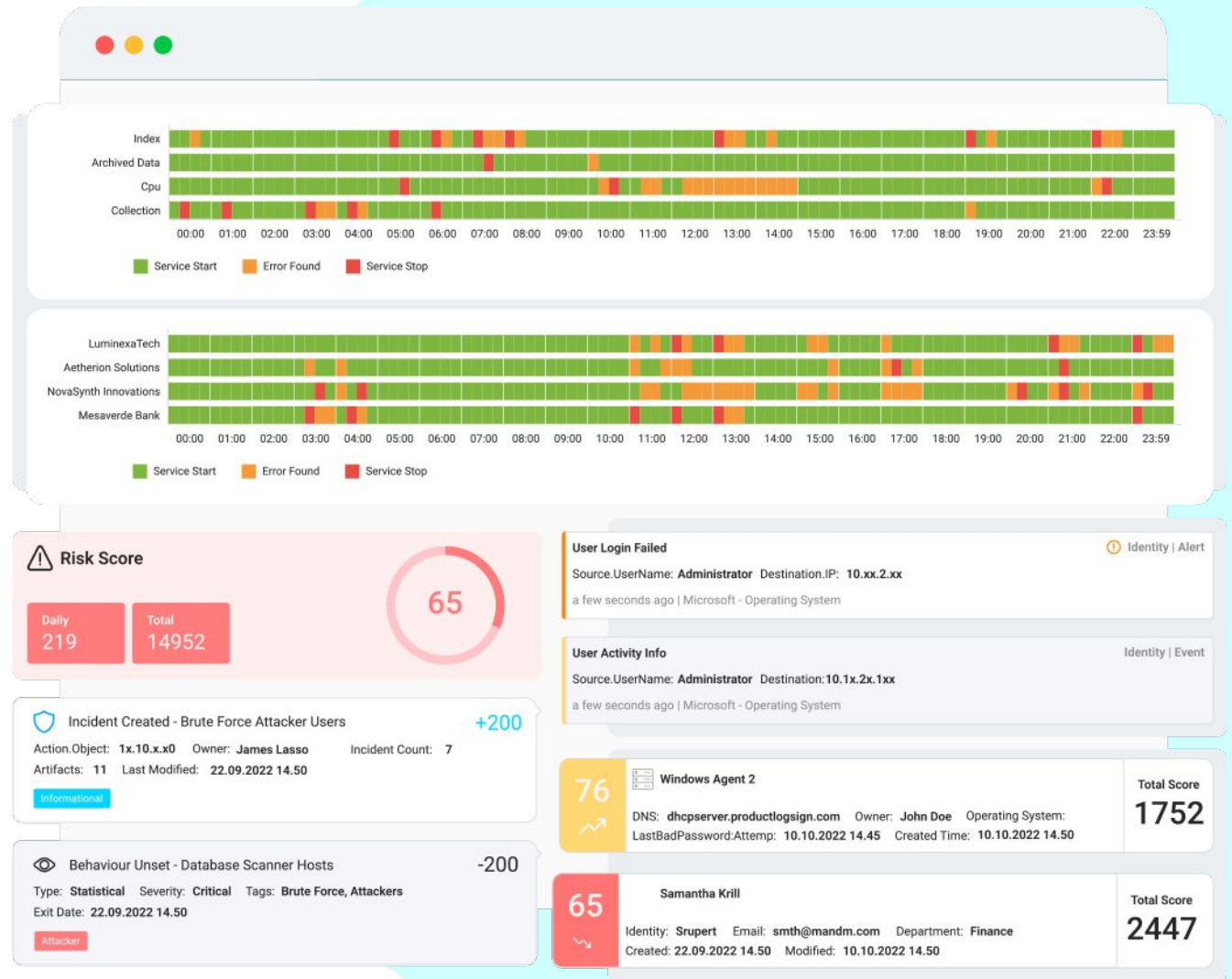
Deliver Value Added Services w/ Cyfusion

Offer your customers the most comprehensive service with remote execution and incident response.
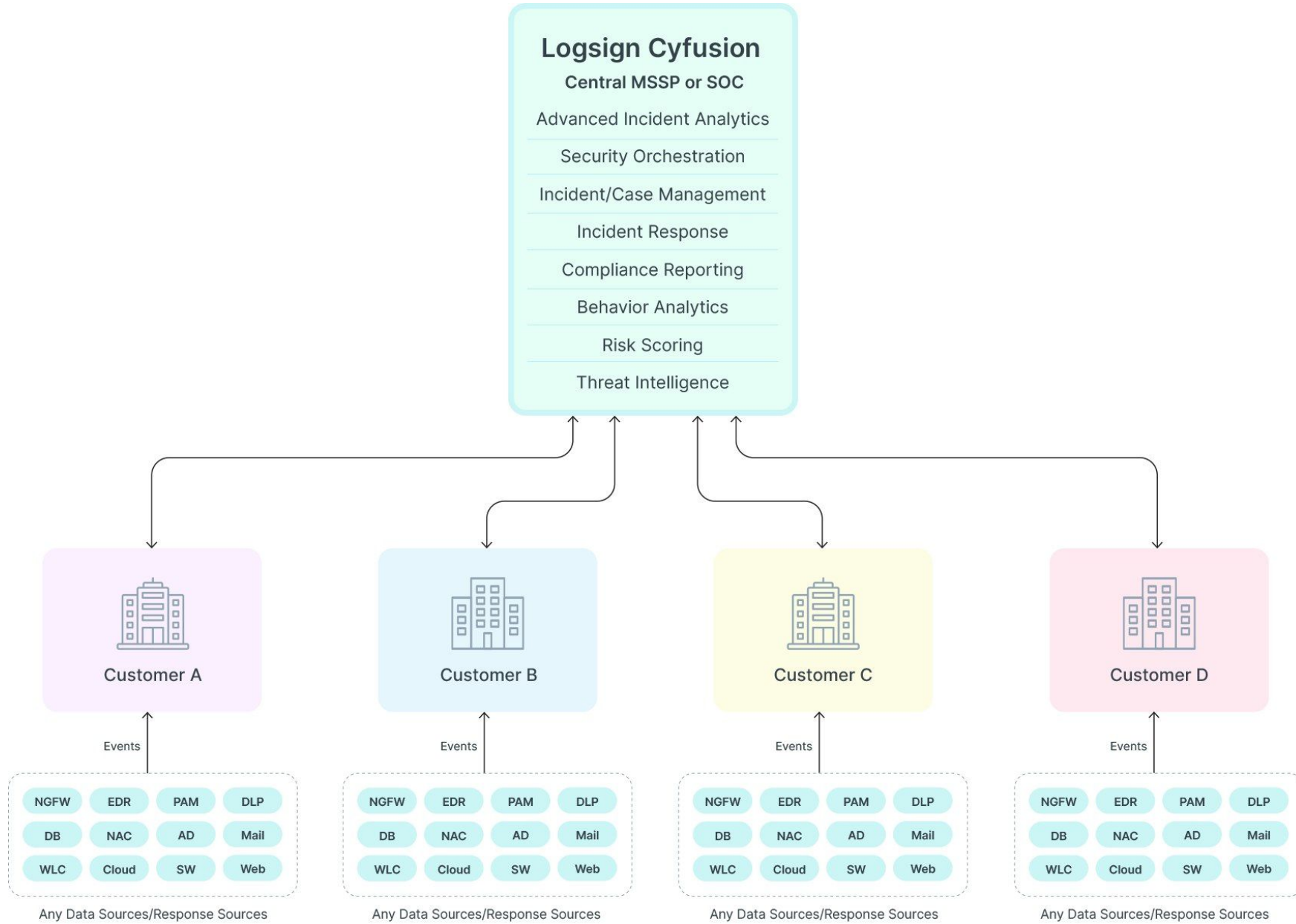
Logsign Cyfusion Highlighted Features

→ Incident Management

→ Security Analysis

→ Central Management

→ Health-Check Monitoring

→ Automation & Orchestration

→ Incident Response

→ Remote Execution
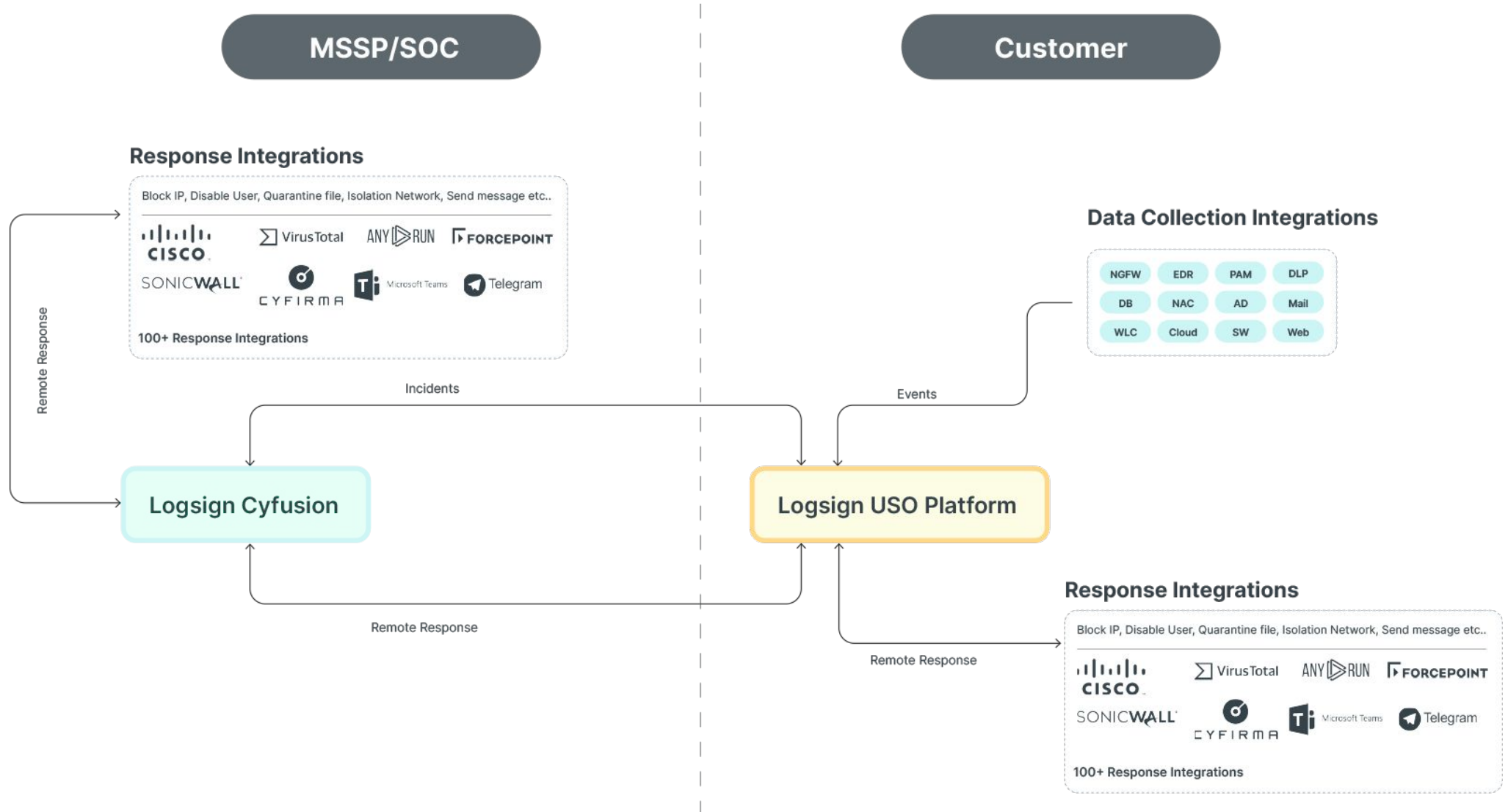
→ Reporting

→ Threat Intelligence

Onboard Your Customers in Minutes

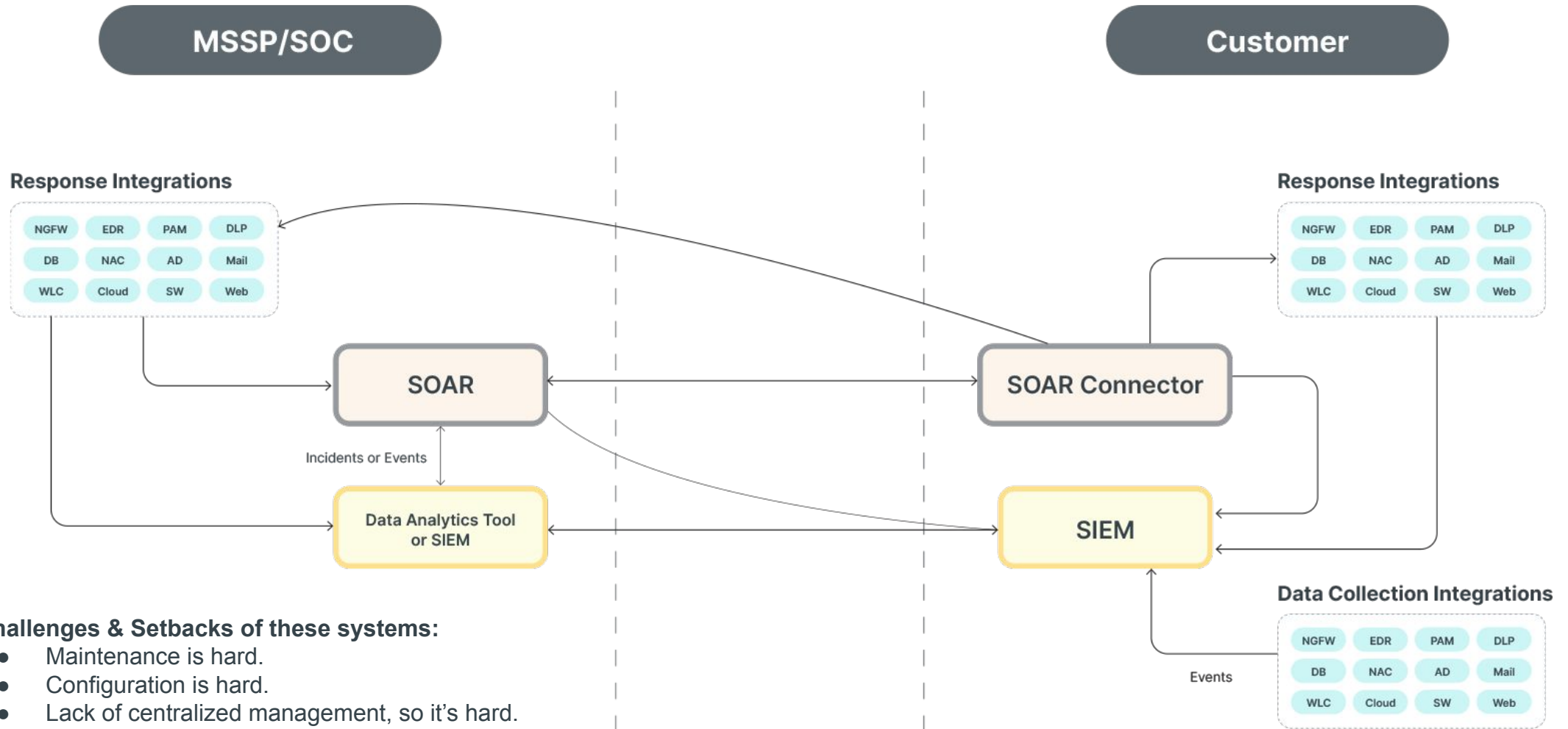Implementing your customers' SIEM takes only minutes!

Logsign

Logsign Cyfusion

Central MSSP or SOC

Advanced Incident Analytics

Security Orchestration

Incident/Case Management

Incident Response

Compliance Reporting

Behavior Analytics

Risk Scoring

Threat Intelligence

Customer A

Customer B

Customer C

Customer D

Events

Events

Events

Events

NGFW	EDR	PAM	DLP
DB	NAC	AD	Mail
WLC	Cloud	SW	Web

NGFW	EDR	PAM	DLP
DB	NAC	AD	Mail
WLC	Cloud	SW	Web

NGFW	EDR	PAM	DLP
DB	NAC	AD	Mail
WLC	Cloud	SW	Web

NGFW	EDR	PAM	DLP
DB	NAC	AD	Mail
WLC	Cloud	SW	Web

Any Data Sources/Response Sources

Any Data Sources/Response Sources

Any Data Sources/Response Sources

Any Data Sources/Response Sources

/logsign

How Cyfusion Works

Ease in Response Achieved:

MSSP/SOC

Customer

Response Integrations

Block IP, Disable User, Quarantine file, Isolation Network, Send message etc..

CISCO ∑ VirusTotal ANY▷RUN ⌐ FORCEPOINT

SONICWALL CYFIRMA Ti Microsoft Teams Telegram

100+ Response Integrations

Data Collection Integrations

NGFW	EDR	PAM	DLP
DB	NAC	AD	Mail
WLC	Cloud	SW	Web

Remote Response

Incidents

Events

Logsign Cyfusion

Logsign USO Platform

Remote Response

Remote Response

Response Integrations

Block IP, Disable User, Quarantine file, Isolation Network, Send message etc..

CISCO ∑ VirusTotal ANY▷RUN ⌐ FORCEPOINT

SONICWALL CYFIRMA Ti Microsoft Teams Telegram

100+ Response Integrations

→ logsign.com → support.logsign.net /logsign

How Others Work - or Chaotic Workflows of Others'

MSSP/SOC

Customer

Response Integrations

NGFW	EDR	PAM	DLP
DB	NAC	AD	Mail
WLC	Cloud	SW	Web

SOAR

Incidents or Events

Data Analytics Tool or SIEM

Response Integrations

NGFW	EDR	PAM	DLP
DB	NAC	AD	Mail
WLC	Cloud	SW	Web

SOAR Connector

SIEM

Data Collection Integrations

NGFW	EDR	PAM	DLP
DB	NAC	AD	Mail
WLC	Cloud	SW	Web

Events

Challenges & Setbacks of these systems:
- Maintenance is hard.
- Configuration is hard.
- Lack of centralized management, so it's hard.
- Lack of Health-check
- Long response times

Take a Deeper Look: Highlighted Features
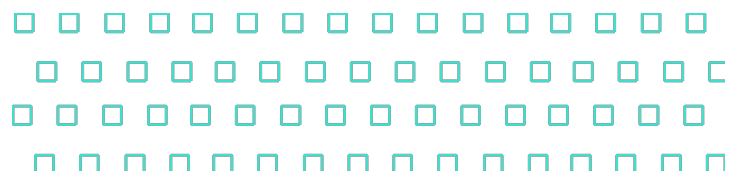
Incident Management

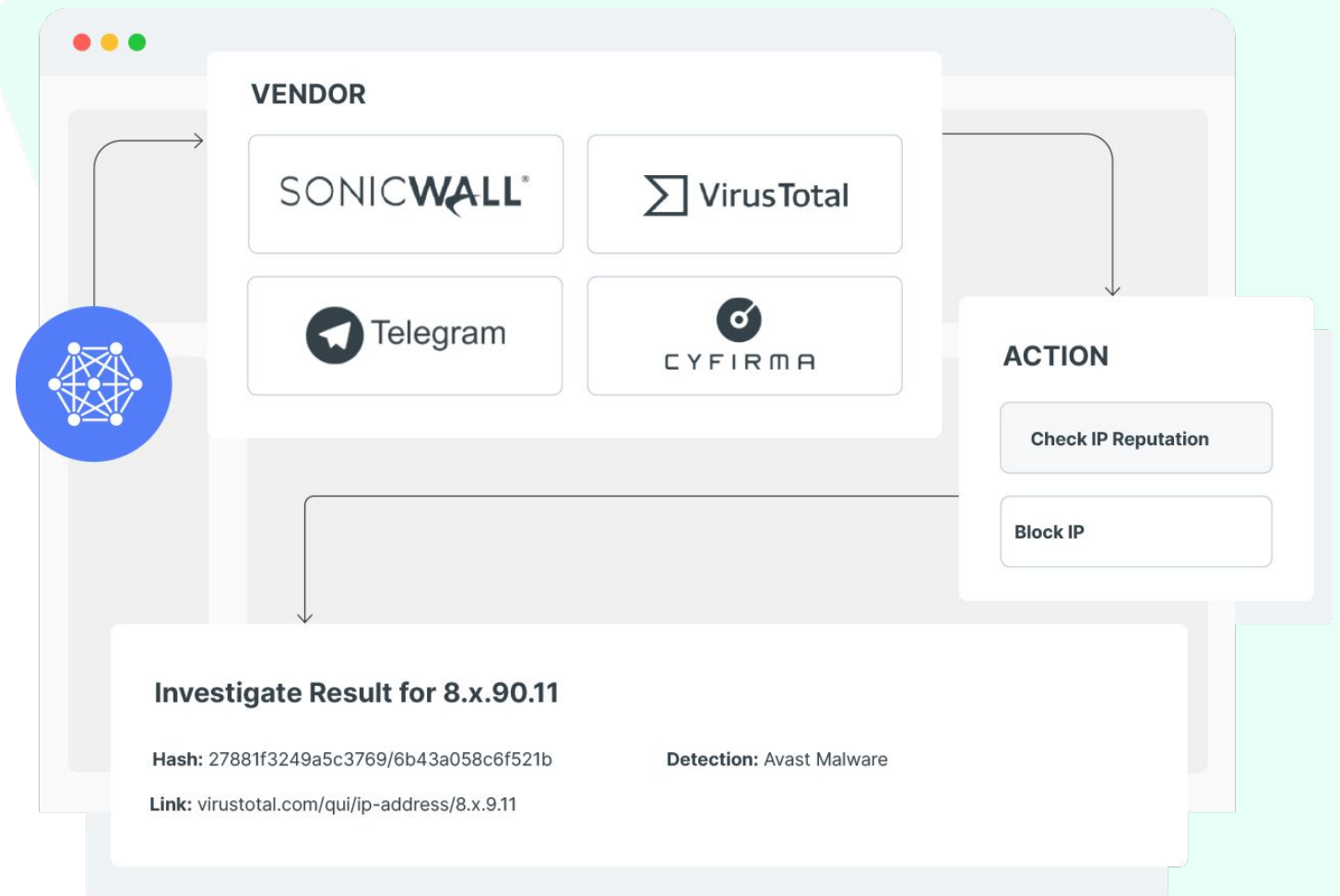Manage your customers' incidents through the centralized hub.

Incident Management

Investigation · **Analytics** · **Response** · **Reporting**
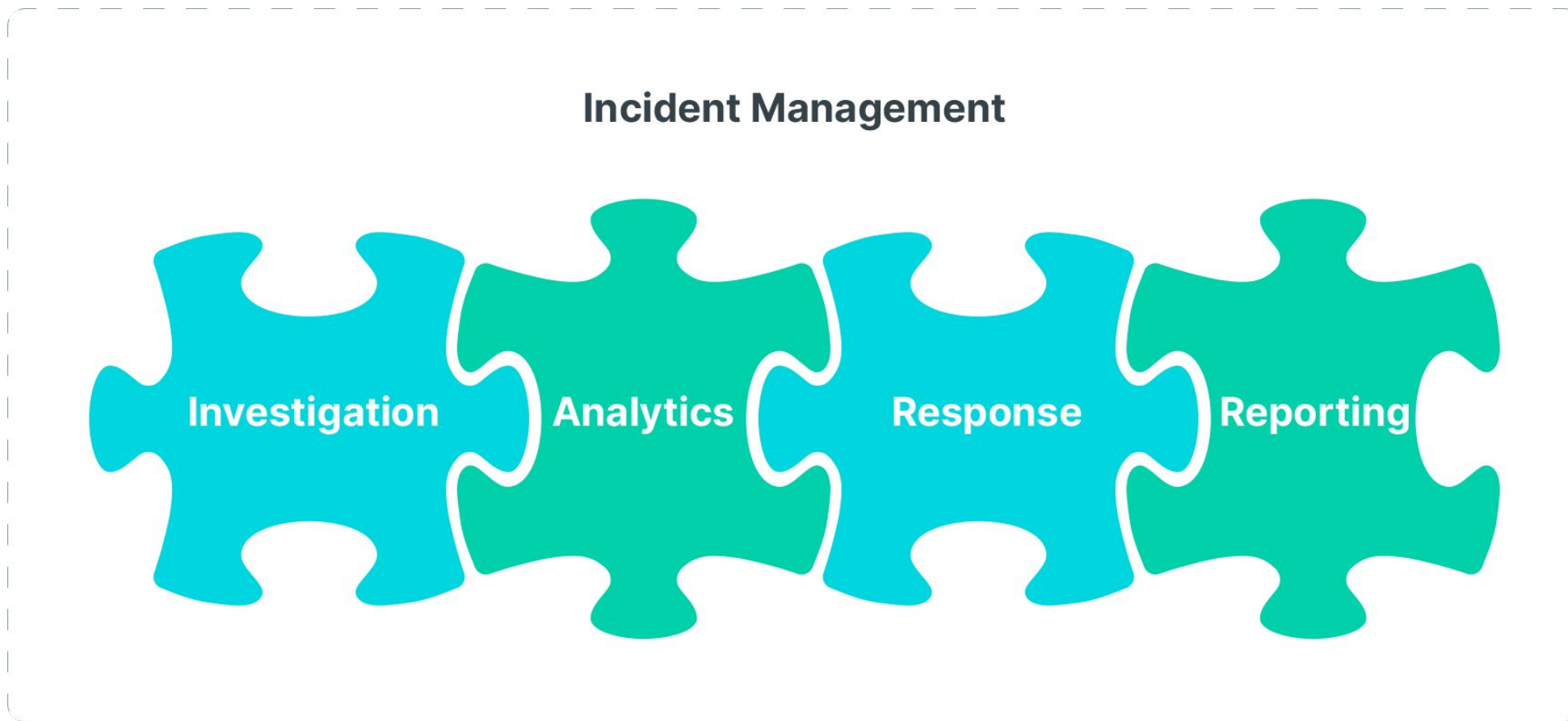
Incident Management/Investigation

Logsign

→ Visual Analysis

→ Deep Investigation

→ Incident Timeline

→ NIST Incident LifeCycle

→ Artifacts, Asset and Identity Management

→ Risk Scoring

Action.Object: 1xx.6.x35.1x

⚡ Responses

🔲 Artifacts

User	Host	IP
3	1	12

⚠ Risk Score

Daily	Total
219	14952

65

⚡ Incident Count

Malware Found   Count: 679

Incident.Category: **Malware**   Owner: **John Black**
Incident.Status: **Open**

a few seconds ago | 2022-03-31 23:42

SERV 0206   Criticality: **Medium**   Incident Count: **55**

IP: **10x.5x.1x0.1xx** DisplayName: **srv0206@logisgn.net** Operating System: **Microsoft Server 2016**
DNSName: **SERV0206.productlogsign.com**   DNSName: **SERV0206.productlogsign.com**
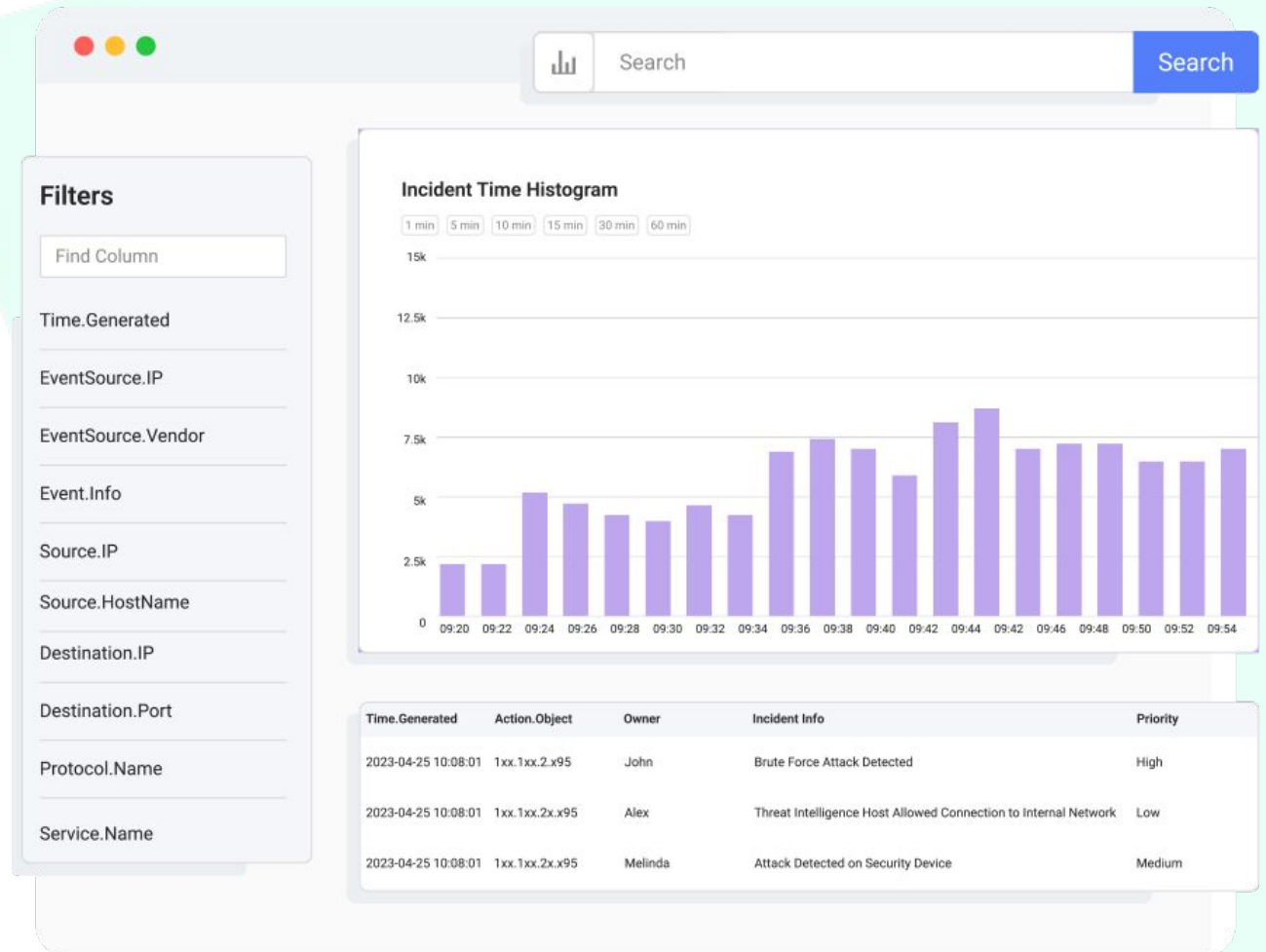
Incident Management/Response

→ Take fast action on the assets your customers use.

→ Perform actions at the endpoint without any additional connections/integrations.

→ Take automatic actions with Action Rules.

→ Execute instant response with the Magic Button.

VENDOR

SONICWALL

VirusTotal

Telegram

CYFIRMA

ACTION

Check IP Reputation

Block IP

Investigate Result for 8.x.90.11

Hash: 27881f3249a5c3769/6b43a058c6f521b   **Detection:** Avast Malware

**Link:** virustotal.com/qui/ip-address/8.x.9.11

Incident Management/Reporting

→ Track and monitor your cybersecurity analysts, and create detailed reports on cybersecurity analysts' actions and performances.

→ Create risk reports for every customer and share.

→ Schedule reports for time efficiency and print them with ease.

→ Create reports with wizards or use the pre-defined reports.

Incident Management/Analytics

→ Enhance your control over the process by visualizing incident data.

→ Perform searches with desired search breakdowns using any filters preferred.

→ Use predefined dashboard libraries.

→ Enjoy ease of use with wizards and the drag-and-drop UI.
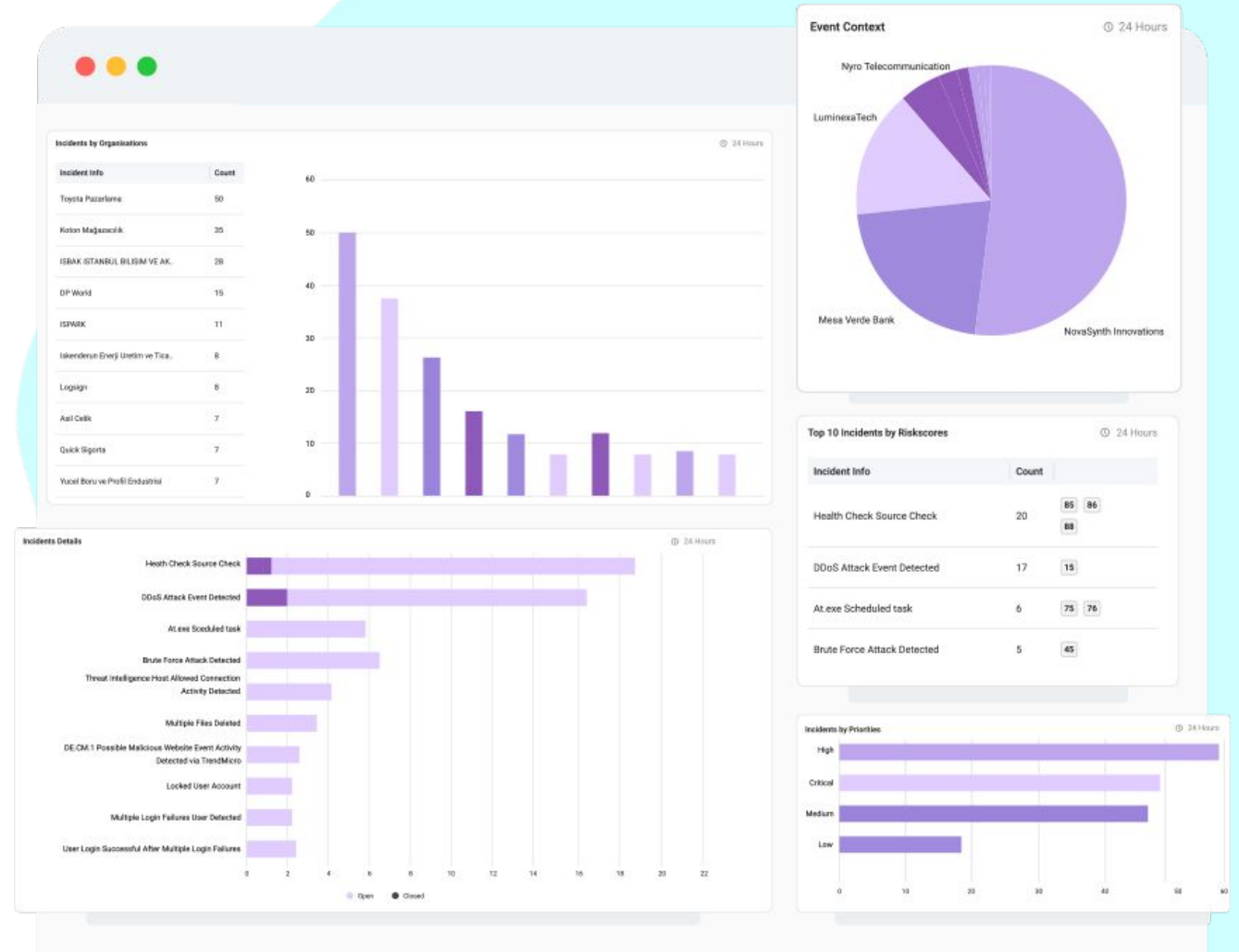
Health-Check Monitoring

→ Track all customer issues on the centralized single hub.   → Report service status in a timely manner.   → Create alerts for any anomalies and be instantly notified.

Secure Remote Support with Teleport

→ Manage all your customers' needs through one channel.

→ Record all sessions.

→ Complete your processes with a secure connection.
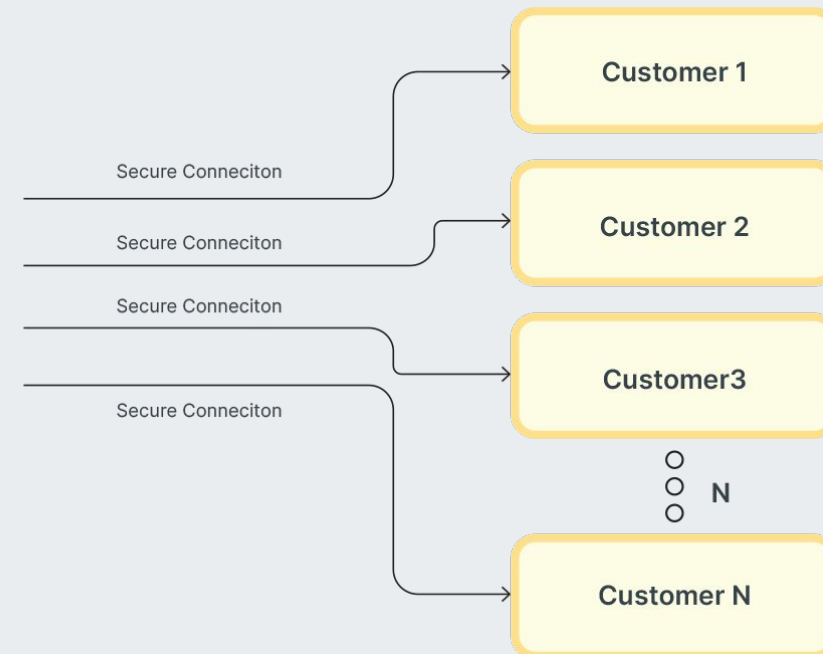
Availability & Scalability

→ Scale horizontally as your customer number increases.

→ Ensure service redundancy with a cluster infrastructure to keep your system working continuously.

→ Back up data for quick access when needed.

Trusted MSSPs

Logsign

viprede

Logsign Next-Gen SIEM is a game changer for VipRede.
The correlation of events is exceptional and enables us to demonstrate our exceptional service to the customer visually.

cyber360

Not very complicated, easy to use. Logsign team solves problems very quickly. Communication with the Logsign team is very easy, we even get responses in an hour.

wateen
جـو چاهو

Our Logsign experience (and support) is really good. We receive prompt responses from the entire Logsign team. Search section is very quick.

BTC
Networks

Working with Logsign is easy, and we have convenient technical support. Remote support makes our life easier. We are able to get prompt responses from the Logsign team. Logsign team is very helpful.

THANK YOU