RedSense

99%

RedSense delivers actionable, context-rich threat intelligence

RedSense delivers actionable, context-rich threat intelligence

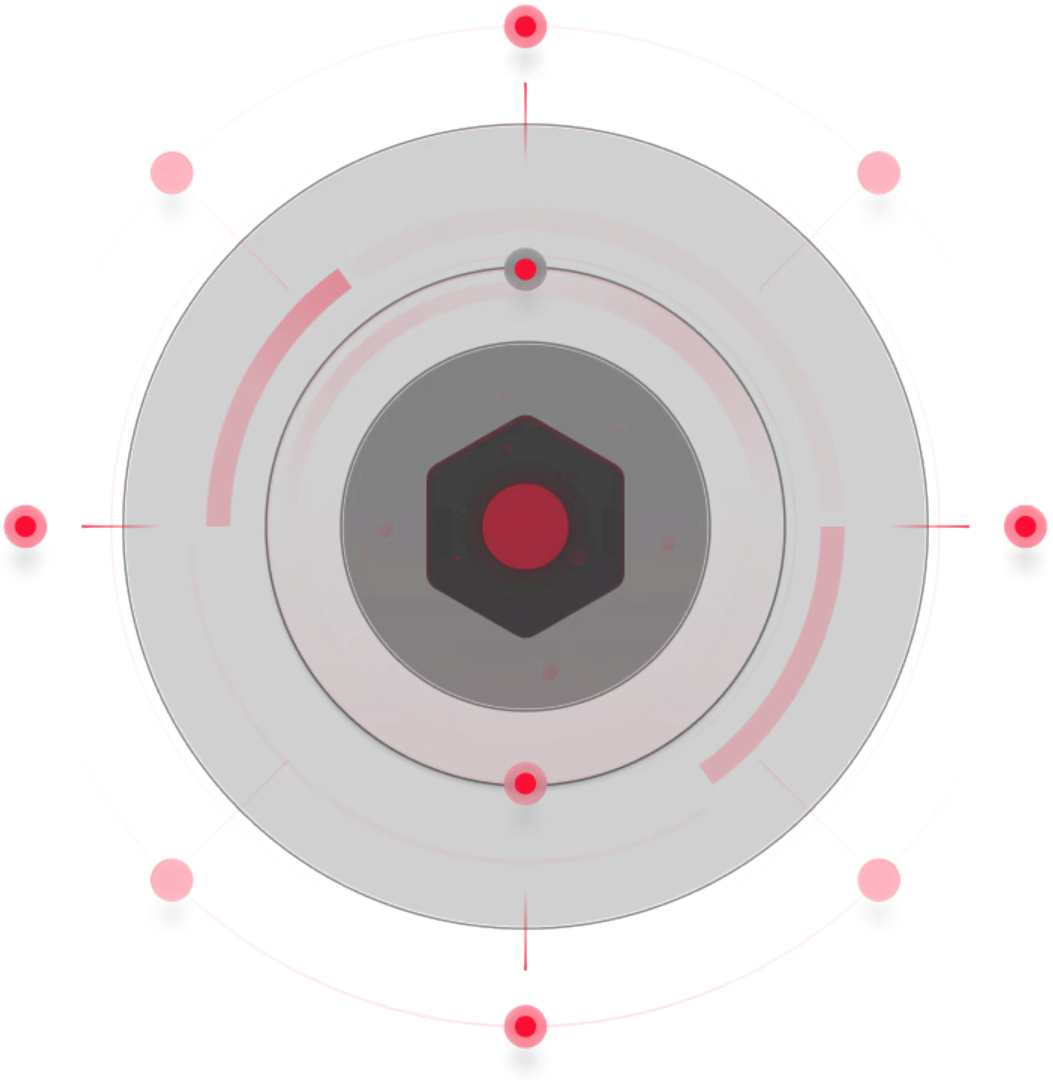
//

//

01

IDENTIFY

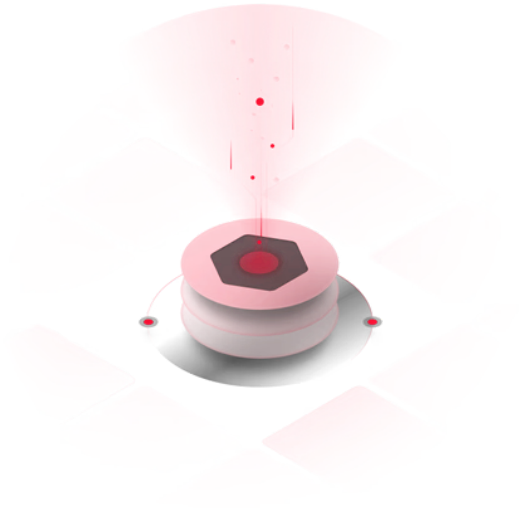
Cultivate Adversary, OSINT, and Telemetry accesses



02

Analyze

AI-based Ingest and Analytics



03

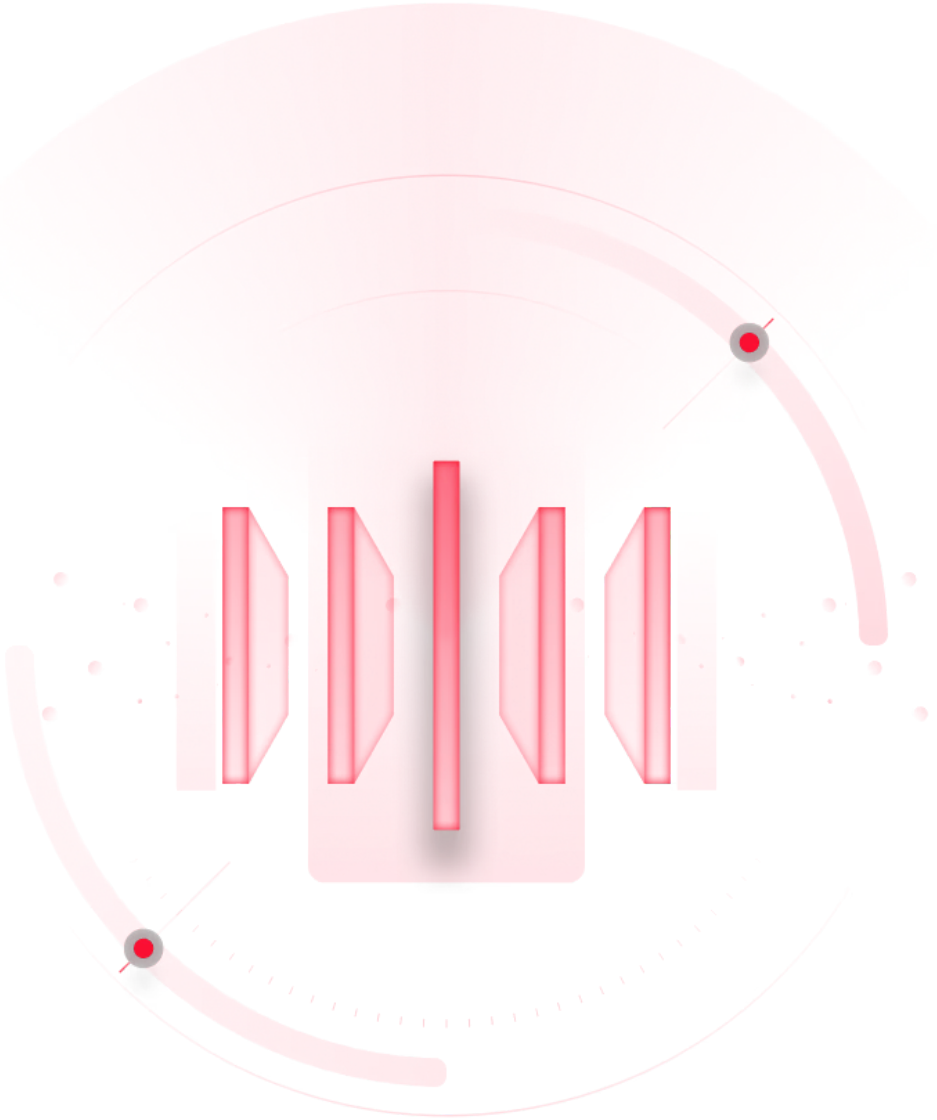
Alert

Near Real Time Automated Alerting

04

Expose

Customer/Researcher Raw Data Access



05

REPORT

Highly Contextualized Intelligence Reporting

//

//

HOW WE

Do It

RedSense is committed to providing companies with relevant threat intelligence, rich in context and insights, ready for immediate action to prevent and remediate cyber threats

Zero Integration

Network Telemetry

RedSense Active Telemetry capabilities require no integration from customer environments and monitoring can turn on in a matter of hours.

ADVERSARY

INFRASTRUCTURE & ACCESSESS

RedSense Proprietary Adversary Collections facilitate near-real time and LEFT OF BOOM mitigation opportunities.

SCALABLE

AUTOMATED ALERTING

Whether a direct customer or an organization responsible for supporting a larger portfolio, RedSense Automated Alerting scales coverage to seamlessly integrate into your security ecosystem.

FULL RAW

DATA ACCESS

The 'RedSense Advantage' offering provides sophisticated customers with full raw data access and independent research capabilities.

WHITE GLOVE

SERVICES

The 'RedSense-as-a-Service' offering provides understaffed/under-resourced organizations with high fidelity alerting and white glove services

//

//

WHY WE

DO IT

The company was founded by a group of threat intelligence experts and practitioners who repeatedly found companies falling drastically short of their cyber threat intelligence (CTI) goals. Too often they witnessed security organizations with lean budgets and staffing, overwhelmed by a flood of threat intel that was outdated, irrelevant to their companies, poorly correlated, and lacking sufficient context to be of use.

//

//

Who We

ARE FOR

RedSense is purpose built by industry leaders for threat intelligence teams everywhere who share a common purpose: to strengthen their detection and response capabilities by leveraging the best threat intelligence.

Understand

Threat Actors

Knowing the latest motivations, tactics, techniques, and procedures (TTPs) of cyber criminals allows organizations to develop and implement proactive security measures. And since threat actors are constantly evolving, it's important you stay agile and adaptive.

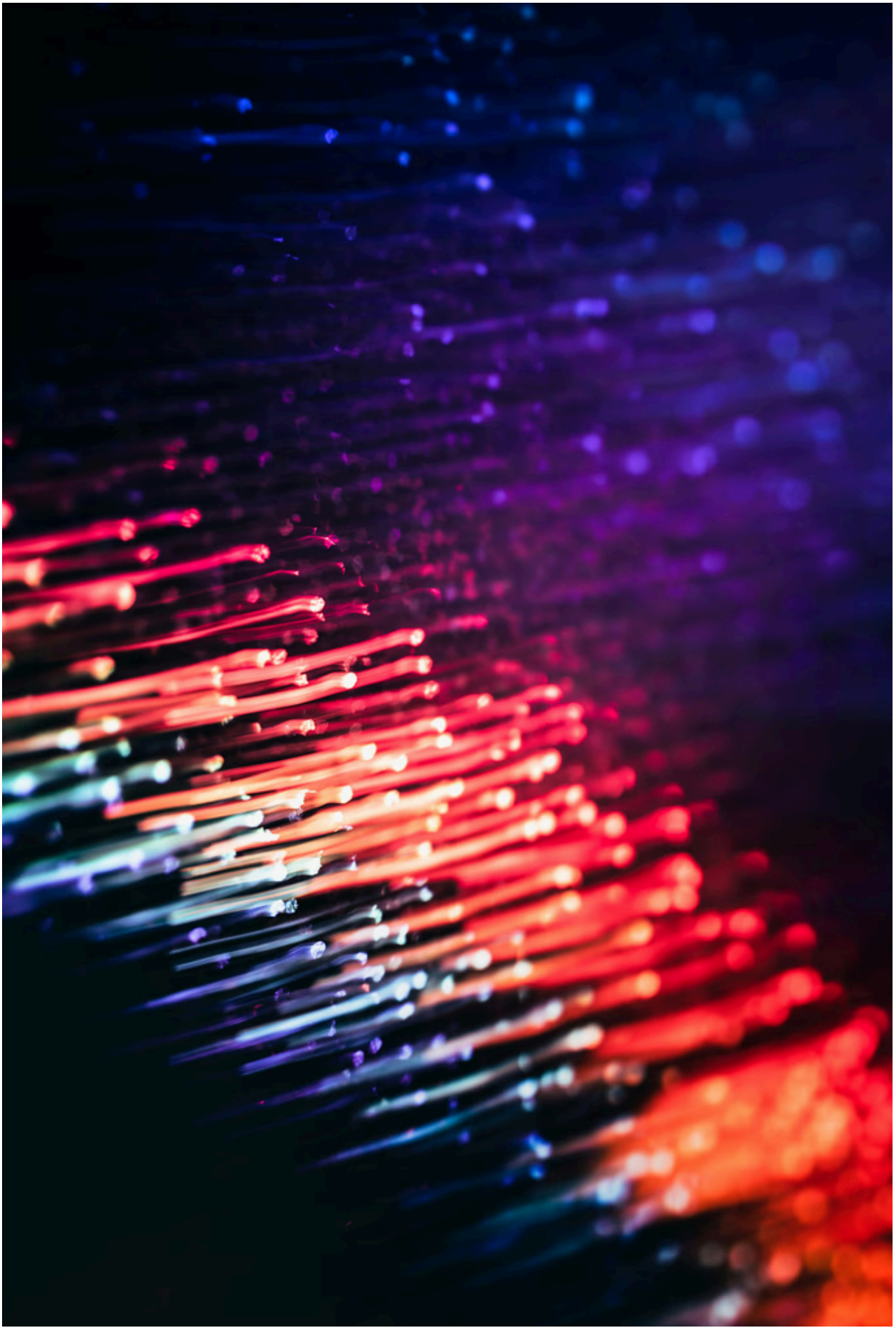

APOTIK
KK
HOTEL
CHINA TOWN
HOTEL

01

See Attack

Campaigns Coming

Successful cybersecurity is not static. Being prepared for emerging cyber threat campaigns, organizations can anticipate potential threats and ensure their defensive posture is up-to-date and ready for the latest damaging threats.



02

Map Attack

Infrastructures

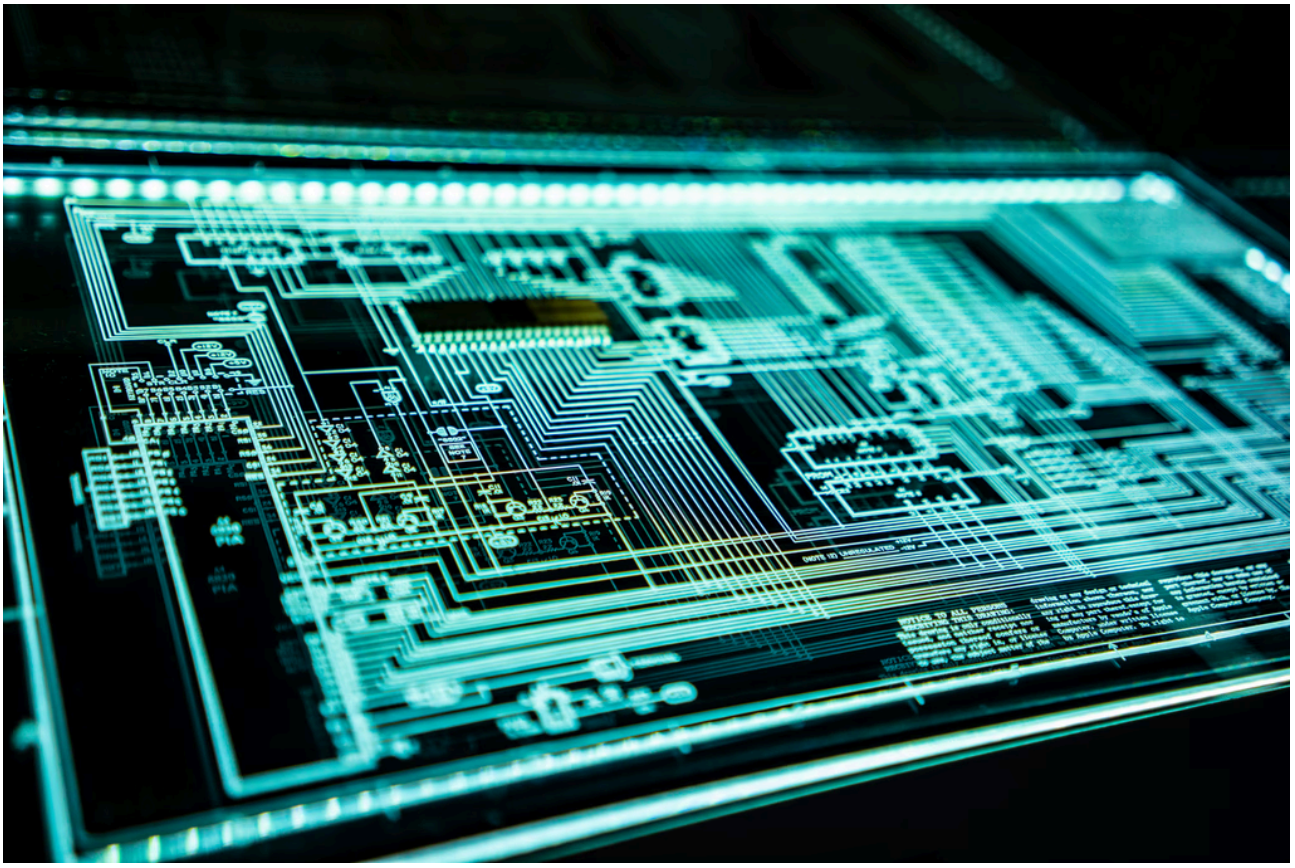
Insight into adversaries' attack infrastructures lets organizations proactively defend and detect threats by recognizing network patterns, domains, IP addresses. Security teams can update detection mechanisms and provide more effective incident response.

03

Detect Compromised

Systems

Threat actors can often evade endpoint protection! Imagine finding those systems based on external observation and proprietary intelligence, providing an additional layer of protection against the most sophisticated attacks.

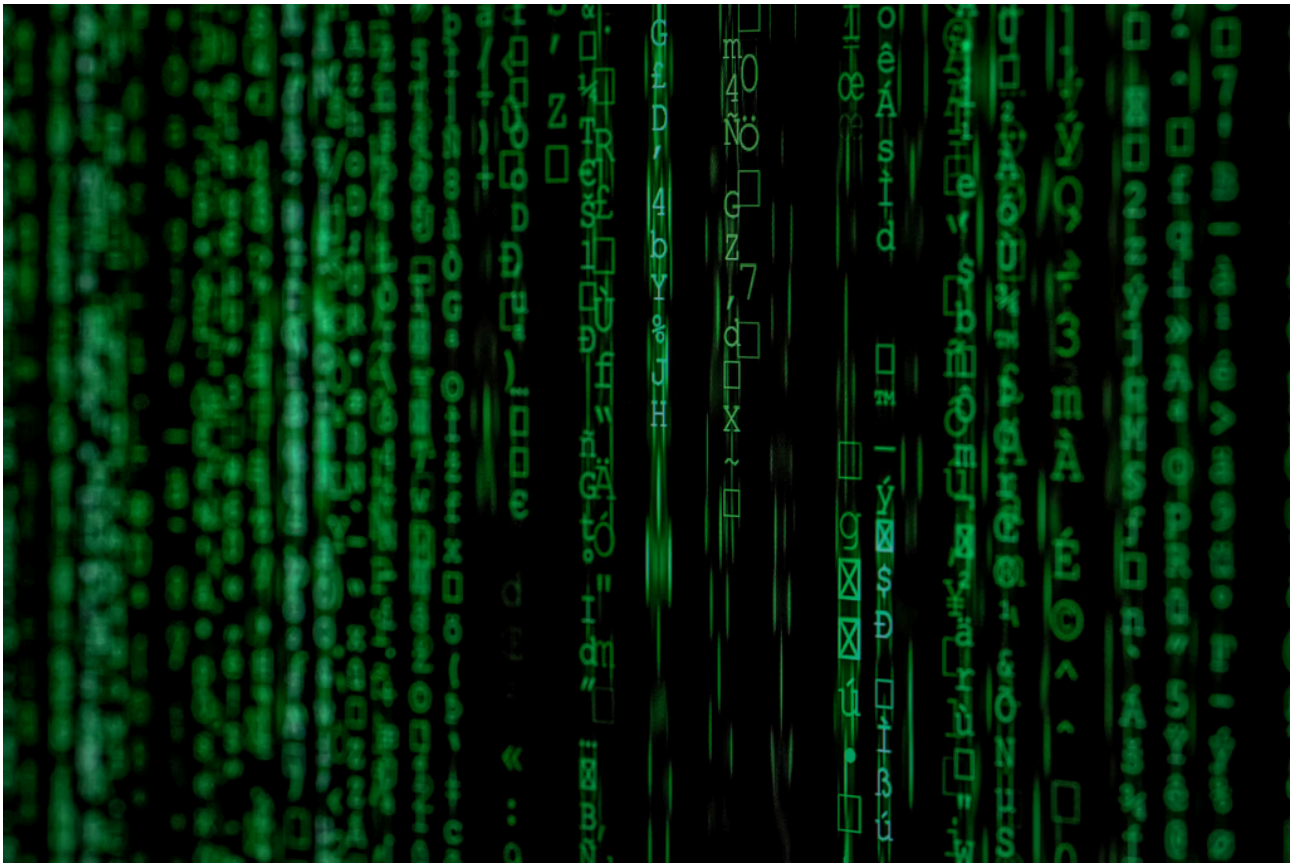


04

Monitor for

Malicious Traffic

External traffic analysis is a powerful weapon against cyber attacks. Without the need for additional security devices, deep network flow analysis can detect internal compromise, as well as potentially compromised customers and partners.



05

Block Use of

Stolen Credentials

The vast majority of breaches involve stolen credentials. It is best to find out about those compromised IDs and password before they are leveraged to hurt you. That way you can change them or shut them down and proactively prevent costly damage.

06

//

//

$100M

saved in potential incident claims and losses for a mulit- billion dollar insurance customer

Dozens

of Ransomware attacks mitigated and prevented before they could inflict damage

10B+

Compromised credentials processed and alerted on for our customers and partners in 2024 alone

Hundreds

of IRs and RFIs processed every quarter - helping our customers prioritize and respond with better accuracy

1M

Internet devices actively monitored daily by RedSense Network Telemetry

:: WORK WITH US ::

- **GET**
- **_**
- **Started**
- **_**
- **NOW**
-

Enter your email below and we will be in touch.

- **GET**
- **_**
- **Started**
- **_**
- **NOW**
-

:: WORK WITH US ::
