

POLARITY

Enterprise Search Platform



Polarity was founded by former intelligence officers and incident responders to bring the first commercial memory-augmentation platform to market. Why perform simple searches or lookups when the power of modern computers and Polarity can automatically bring the results to you? The human brain is great at pattern recognition but not so great at recall.

We set out to empower our users with the capabilities of a machine. Some of the world's largest financial institutions jumped on board as early customers when Polarity was in closed beta and now we are expanding within the market. Polarity was named one of the top 10 most innovative startups of 2016 by MIT Sloan's CIO Symposium. We hope you share our vision of a world with less search and better decisions, and decide to join our team or user community.

Founders



Paul Battista
CEO and Founder

Everything from penetration tests on Wall Street to information security briefings at the White House



Edmund Dorsey
Founder and CTO

Data analytics, visualization, and software engineering for financial services, medical imaging and big data processing



Joseph Rivela
Founder and Chief Strategist

Customer development, security strategy, policy, compliance, incident response, PCI, and current NYC ISSA President

Investors and Advisers



Hank Thomas
Board Member, Investor

20+ years of experience in cybersecurity, military intelligence, management consulting, and business.



Tom Noonan
General Partner,
TechOperators

Former Chairman, President and Chief Executive Officer of Internet Security Systems



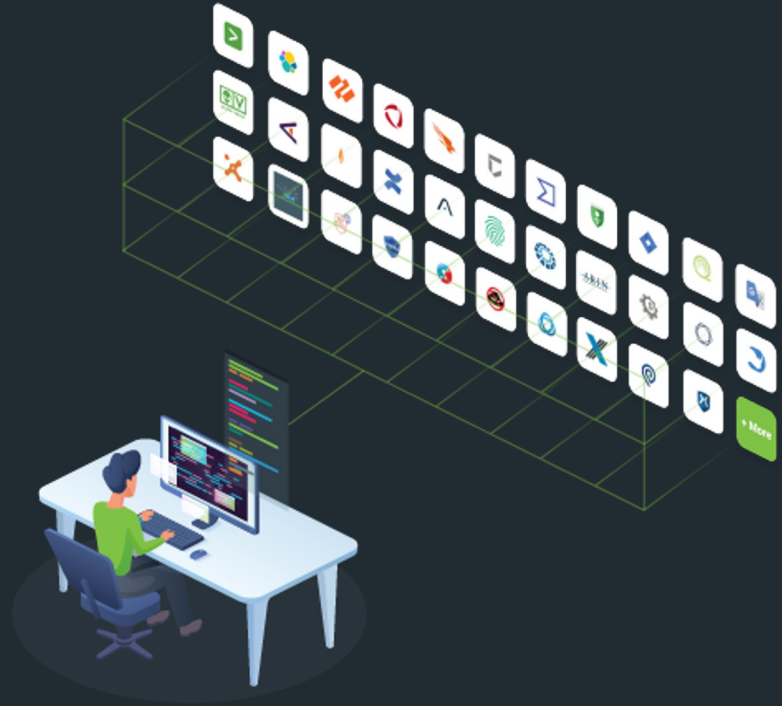
Ron Gula
Board Member, Investor

Co-founder and former CEO of Tenable Network Security

What is Polarity?

Polarity is a Federated Search,
Automated Research, & Context
Enrichment Platform

Polarity supercharges Operations
and Analysis by bringing data
from every available data source
into one **unified view**.

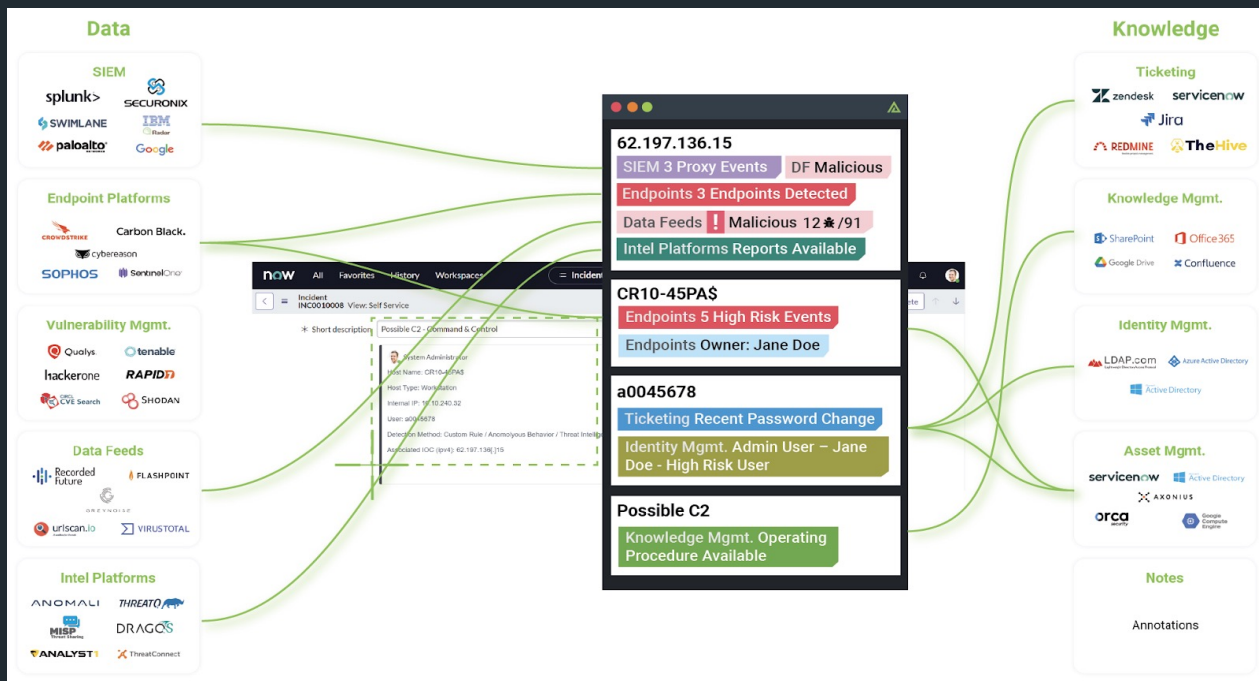


How does Polarity work?

Knowledge and data is spread across distributed systems.

Polarity fuses them together in one unified view.

Polarity engages knowledge and data where it resides – avoiding the creation of another data lake.



Polarity – Highlight Mode Automated Search

Enabling Operations at 10x Speed

- Polarity “real-time” automated search passively suggest the availability of additional context information to a user in relation to information on their screen.
- Polarity Highlight will color boxes directly over your active application, highlighting the entity that Polarity can deliver context information about.

With our Highlight Mode you just hover on the indicator and results will populate in the overlay window.

The screenshot displays the Polarity Highlight Mode interface. The main window shows a network traffic capture (bad.pcapng) with columns for Time, Source, Destination, Protocol, Length, and Info. The traffic is color-coded by destination IP: 192.168.55.133 (green), 173.194.76.95 (blue), 173.194.43.42 (green), 74.125.226.180 (blue), 192.168.55.2 (orange), 108.162.232.200 (blue), and 108.162.232.205 (blue). A green arrow points from the text 'With our Highlight Mode you just hover on the indicator and results will populate in the overlay window.' to the '108.162.232.205' IP address in the traffic list.

An overlay window titled 'Search entities in Polarity' is open, showing search results for the IP address '192.168.55.133'. The overlay includes a search bar, a 'Focus' button, and a list of search results. The results are categorized by 'Server Assets' and include items like 'Hard drive failing', 'Hosts Credit Card Data', 'Split Split Web Server', 'IPDB Confidence of Abuse: 0%', 'IPDB Associated Domain: null', 'IPDB No reports', 'MTIMScore: 10 (benign)', and 'SLACK Message Channels'. The 'SLACK Search Results' section is also visible.

The bottom of the screenshot shows the details of the selected packet (Frame 1):

```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF...
> Ethernet II, Src: VMware_82:ee:03 (00:0c:29:82:ee:03), Dst: VMware_fb:b5:0e (00:50:56:fb:b5:0e)
> Internet Protocol Version 4, Src: 192.168.55.133, Dst: 74.125.226.234
> Transmission Control Protocol, Src Port: 62081, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

Polarity Core Benefits



Immediate knowledge delivery for informed decision making

Enable team members to
work with speed and
thoroughness



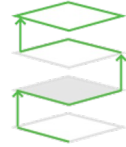
Fuse all your disparate data into one unified view

Full data visibility and
complete asset awareness



Uplevel your team

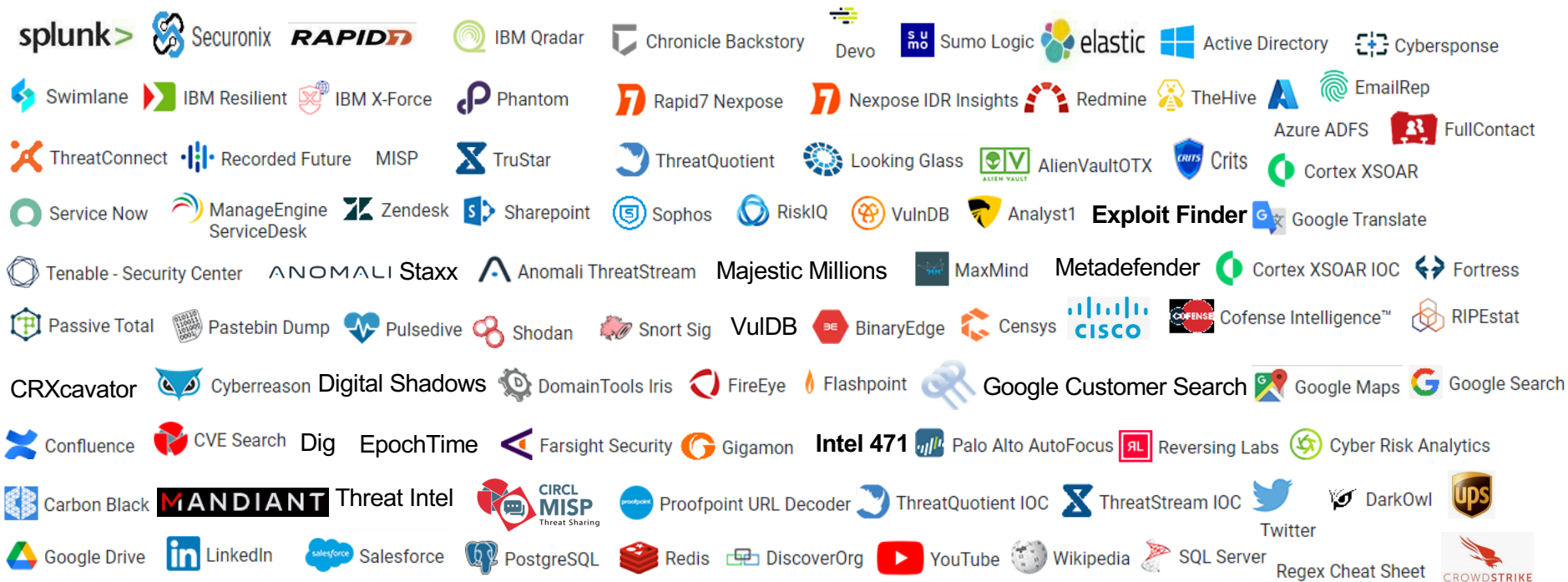
Improve team
communication and
automating knowledge
transfer for team member
onboarding



Gain insights from Telemetry

Understand what tools
deliver value, make
informed spending
decisions, and remove
process deficiencies

Polarity Integrations include:



IT Operations |
Help Desk

Malware
Analytics

Network
Engineering

Network Web App
Security

Open Source |
Github

Orchestration |
SOAR

Pen Testing

Security and IR

SOC | SIEM

HR | Legal | EDR

Threat Hunting |
DLP

Threat
Intelligence

Vulnerability
Management

Workflow
Management

Core Benefit - Telemetry and Analytics



Prominent Use Cases



Incident Response

Security Operations

Threat Hunting

Threat Intelligence

National Security

CRM / Legal Discovery

**DLP Protection
Response**

**Insider Threat
Investigations**

**Help Desk/IT/Network
/Operations**

Core Use Case

Incident Response



Key Pain Points

- Lack of information sharing across teams
- Blind spots lead to mistakes
- Teams are stretched thin - too many tasks

Solutions

- Enabling speed and thoroughness
- Upleveling analyst teams

Core Use Case

Threat Intelligence



Key Pain Points

- Lack of information sharing across teams
- Blind spots lead to mistakes
- Difficult to collect information and get it into platforms - reverse process

Solutions

- Enabling automatic collaboration
- Complete data visibility
- Enable collection from anywhere

Core Use Case

Threat Hunting



Key Pain Points

- Time searching
- Ability to mitigate potential risk
- Fear of missing the adversary that's there coupled with the diversity of places you need to search
- Threat landscape is too vast and there is too little time dedicated for the research necessary to gain understanding

Solutions

- Delivering knowledge to enable analysis - tools don't hunt, people do.
- Complete data visibility
- Working with any tools analysts use in the hunt
- Upleveling the analyst

Core Use Case

Security Operations



Key Pain Points

- Overwhelmed with events
- Alert fatigue
- Choosing between speed and thoroughness
- Tool/dashboard/vendor fatigue
- Time to onboard new team members (more tools = longer onboarding)
- Finding and retaining talent

Solutions

- One unified view
- Enabling both speed and thoroughness
- Speeding up response time
- Upleveling the analyst
- Knowledge retention (even with employee turnover)

Core Use Case

National Security



Key Pain Points

- Choosing between speed and thoroughness
- Teams stretched thin - there's too many tasks and not enough people
- Tool/dashboard/vendor fatigue
- Time to onboard new team members (more tools = longer onboarding)



Solutions

- The right person, the right data, the right time
- Patching blind spots
- Maximize investment with automatic dissemination

Core Use Case

HR/Legal Findings



Key Pain Points

- Sources located in multiple locations leads to incomplete analysis of disparate data
- Too much time needed for informed decision making

Solutions

- Comprehensive view of knowledge and data
- Speeding up time to informed decisions





Core Use Case

DLP - Data Protection Response



Key Pain Points

- Team members don't know if data is confidential to view or send
- Team members don't always have access to confidential data
- There are different repositories of confidential information

Solutions

- Complete knowledge and data visibility
- Team members enabled to make informed decisions

Core Use Case

Insider Threat Investigations



Key Pain Points

- Searching for context in siloed disparate systems
- Cumbersome review of
 - DLP or endpoint data
 - access logs for desktop/laptop, or server(AD, IAM, SSO, SAML, PAM etc)
 - user's logs to the IP repository (Git, BitBucket, Perforce, etc. code base, SharePoint or other)
- Difficult to correlate all that data in one view with known vulnerabilities, bad actors' IPs, threat feeds and organizational context from teammates

Solutions

- Fusing all indicators of compromise and anomalous behavior as well as organizational context in one unified view

Core Use Case

Help Desk/IT/Network Operations



Key Pain Points

- Finding the right data to answer customer questions
- Repeating what was discussed on previous calls
- Technical answers to issues and querying the JIRA, Knowledgebase
- Are their known solutions to their needs

Solutions

- Complete data and knowledge visibility
- Being able to review what was discussed on previous calls
- Awareness of known solutions

Respected and Recognized



”

Polarity enabled our incident response team to quickly draw on historic intelligence which furthered their ability to respond effectively to observed events

CIO, Leading Media and Internet Company

”

You guys continue to set the bar for what Customer Support should be

SOC Manager

Verizon Media

”

Polarity is a force- multiplier for our security team whether its threat hunting or another discipline. With Polarity in Highlight or On-demand mode we have confidence that all of our most valuable information is delivered to our analysts, cross referenced against multiple sources, and is acted upon by the right people at the right time.

Michael Fracness

Manager, Cyber Security
Advanced Threat

”

Our investment in Polarity led to an annual ROI of nearly 200% based on just its initial use cases. Since purchase, we continue to find ways to use Polarity to increase the speed and thoroughness of the team.

Cybersecurity Manager

Leading Financial Service Company

”

...really haven't stopped using it since you showed me it, great little tool.

Robert Gasior

CIRT Lead EMEA



Winner of two awards: Editors Choice Infosec Startup of the Year, and Best Product - Memory Augmentation

Cyber Defense Magazine



This is one of the few tools that I recommend outright based on a demo alone. The capability is awesome.

Andy Piazza



Information and Guides

[Polarity Admin Guide](#)

[Polarity Enterprise Guide](#)

[Polarity Developers Guide](#)

[Polarity Integrations on GitHub](#)

Questions?



POLARITY

POLARITY

Thank you