Cybersecurity Challenges

Business adoption of new technologies enhances workforce productivity, but also places a higher burden on the IT security teams that must defend growing attack surfaces. Many organizations have invested a great deal of time and money on point solutions that solve one problem at a time but fail to deliver comprehensive visibility and protection across these environments. Managing these myriad tools and the high volume of data they produce to find and stop attacks can overwhelm small teams with limited resources and specialized expertise. Sophisticated attackers are leveraging intelligence and automation to exploit these challenges.

Growing attack surface	Ineffective & inefficient point solutions	High volume of complex data	Lack of resources & expertise

ActZero MDR

ActZero supports organizations of all sizes with an outcome-focused Managed Detection and Response (MDR) platform that's powered by market-leading artificial intelligence and a team of expert threat hunters. ActZero's MDR offering delivers machine-speed detection and response across endpoints, networks and cloud backed by a global team of analysts to investigate and remediate 24/7. By deploying Crowdstrike endpoint detection and response technology, next generation anti-virus, plus advanced cloud and network analytics powered by Stellar XDR as well as proactive scanners, ActZero finds and stops the full spectrum of threats, from commodity malware to the latest ransomware attacks.

Stop advanced threats

18 proven ML detections in service

Multiple data sources + data types + analyst review

Superior alert quality

<10 alerts/month with only 15% FPs

7x more precise EP coverage than untuned leading EDRs

60,000x more precise XDR coverage than untuned leading XDRs

Machine speed defense

Automatic responses for ransomware

Automatic responses for Cloud Account Takeover

Who we are

- Well-funded, company with ~100 employees
- Dedicated to delivering measurable outcomes
- Gartner-recognized MDR provider
- Delivering services for 15+ years
- Offices in Menlo Park, Seattle, Toronto, Dublin, and Manila

What we do

- High-accuracy detection & response across endpoint, network and cloud - 24/7 SOC
- Ransomware protection; account takeover protection; and security maturity
- Partner with you to address the entire attack lifecycle to proactively improve your posture

Why ActZero

- Large data science team - our specialization is AI/ML-enabled detection & response
- Extremely low false positive rate (multi-level AI + SOC review), high confidence alerts/responses
- Tech stack of market leading technologies

ActZero in Action

Scalable Threat Coverage

- 24/7 SOC support
- Full visibility across endpoint, network, and cloud
- Supported with XDR technology
- Log Management
- Vulnerability Scanning
- Next Generation Antivirus
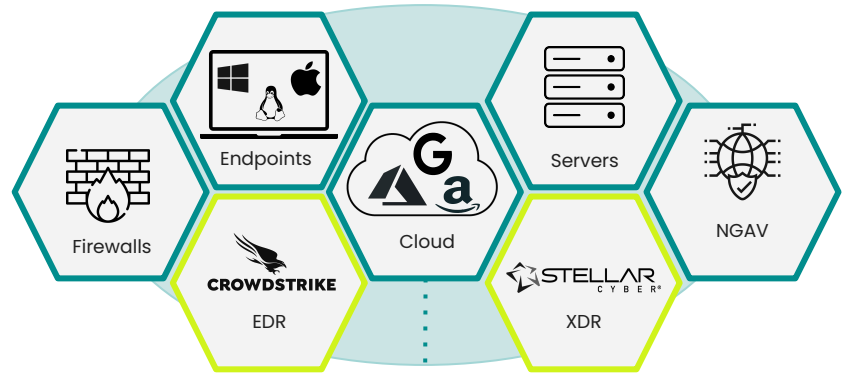
Tailored Maturity Improvement

- Customer Portal provides increased visibility and on-demand access to:
  - Security Hygiene reports
  - Prioritized patching & configuration
  - Security Maturity Model
  - Compliance posture management for HIPAA, CIS, NIST
- vCISO support (optional)
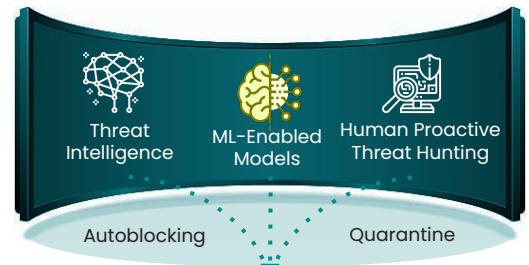
Superior Detection & Response

- Multiple threat intelligence sources
- Cross-correlated signal detections
- ML-enabled threat detection
- Human proactive and reactive threat hunting
- 24/7 Active Response
- Automated ransomware & ATO blocking
- Guided remediation
- Optional Advanced Incident Response
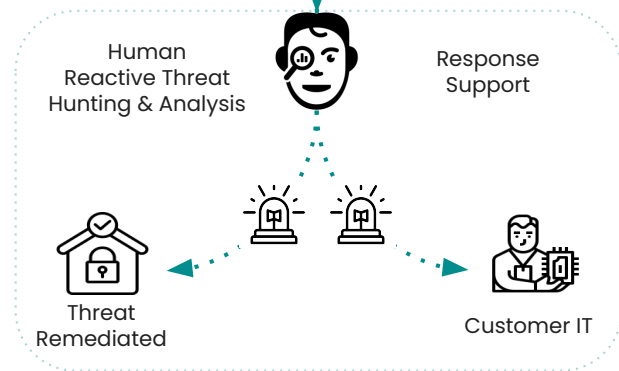
Customer Feedback

"In three months, we got more actionable alerts from ActZero than from our previous service provider over three years. Now, we're not flooded with bad alerts. When we get an alert, we know we need to look at it. The monthly report is phenomenal, the CIO is very pleased with the service. We're way more secure now than we were when we started."

–VP of IT, large regional hospital, US Southeast