Executive Overview

•Headquarters: Waterloo, Ontario -Canada
•Founded in 2001
•600+ Employees
•2 Security Operations Centers (Cork, Ireland and Waterloo, Ontario -Canada)
•Over 2,600 customers in 80+ countries

Product & Service Offerings

BREACH PREVENTION
Managed Detection & Response
•Network
•Endpoint
•Cloud
•Log

BREACH SERVICES
Digital Forensics & Incident Response
•On-Demand 24/7 Incident Response
•Emergency Incident Response

PRE-BREACH SERVICES
Managed Risk Programs
•Managed Vulnerability Service
•Managed Phishing and Security Awareness Training
•Penetration Testing
•Virtual CISO Services

Sales Engineer Take On Best Fit

One of the largest 'pure play' security providers in the market focused on breach prevention, detection & remediation. Full DFIR services can be purchased standalone/after a breach. Offer MDR services. Offerings around Crowdstrike & Microsoft Security and can bring SumoLogic as a SIEM service. Best consulting vCISO practices in the portfolio with some size and length of service minimums. Offer 24/7 SOC services include proactive Threat Hunters and their patented Atlas XDR platform which has a 15-minute mean time to contain (an incident). Finally they offer an agent called CYFIR that allows for some of the fastest investigation and response services on the market. They will work with smaller customers, but their ideal cusstomer is 100-500 with no IT team or 500-2,500 as an extension of their cyber team. They have identified niche opportunities with customers over 2,500 employees usually around their IR services.

-Rick Mischka, Cybersecurity FSE

Key Features & Differentiators

©2024 AVANT Communications. All rights reserved.

•Full Threat Visibility & Investigation eSentire's multi-signal approach ingests high-fidelity data sources from the endpoint, network, log, cloud, insider threat, assets, and vulnerability data, enabling complete attack surface visibility.
•24/7 Threat Hunting & Disruption eSentire's SOC analysts and elite threat hunters rapidly investigate, contain, and close down threats when an automated response isn't possible.
•Atlas XDR Platform Patented AI and Machine Learningusinghigh fidelity detection and automated real-time threat disruption powered by unique intelligence from across our global customer community identifies and disrupts new and emerging threats.
•Rapid, Robust Response SOCanalysts and threat hunters disrupt, isolate, and stop advanced threats with a 15-minute mean time to contain.
•Original Threat Intelligence eSentire's Threat Response Unit (TRU) delivers original research, curates threat intelligence, and builds new detection models to stay ahead of attackers.

Top Industries Served

- Manufacturing
- Financial Services
- Information Technology
- Law

Ideal Customer Profile

- Has no team & needs one: Needs an extension of the team
  - Looking for a complete cyber solution, looking to hire "the team" as a Service
  - Manager or Director of IT
  - Influencers: Manager, Engineer, Architect
  - Less than 500 employees
  - •1-2 people in security
  - •"One man show"
- Needs an extension of the team: Hiring threat hunting and response expertise to expand capabilities, augment 24/7 SOC as a Service
  - VP or CISO, IT, Cyber
  - Influencers: Manager, Engineer, Architect
  - 500 -2,500 employees
  - •Understaffed
  - •Requires off-hours support
  - •Lacks threat hunting/response
- Has a team needs –Niche Expertise: Outsource capabilities to focus their team on higher priority initiatives, may be secondary SOC, driven by compliance requirements
  - CISO, CIO, CRO, CEO
  - Influencers: Manager, Engineer, Architect, Director, CFO
  - 2,500-10,000+ employees
  - •Right-Sized
  - •Looking for compliment or back up to support technical expertise

Qualifying & Technical Questions

©2024 AVANT Communications. All rights reserved.

Qualifying Questions

1. Do you have a dedicated security team?
2. Do you have a team and a security policy and incident response plan in place?
3. How does your security process scale for larger, heavily regulated clients?
4. Where do you feel the existing program is falling short?
5. What have you done to ensure you are meeting industry regulations?
6. How do you think a breach can impact your organization?
7. If you were breached, how would this impact your brand reputation?
8. How long would it take you to diagnose a breach?
9. How are you currently monitoring your network?
10. Are you sure threats are not bypassing your controls?
11. How do you assess the security risks of partners, supply chain, and prospective acquisitions?
12. How do you address security due diligence questionnaires from potential clients?

Technical Questions

NETWORK

1. Total number of locations?
2. Total number of Knowledge Users?
3. What is the make/model of core switches?
4. Is the internet direct or backhauled? Speed?

ENDPOINT

1. Total Number of Workstations, Laptops, Servers?
2. Are you running Windows OS, Mac OS, Linux (RHEL / CentOS) specific versions?

LOG

1. Currently do you have a SEIM?
2. Do you have compliance requirements? If so, which ones?
3. Are compliance requirements driving your decision to have a SEIM?
4. For audit purposes do you have a data retention timeframe? If so, how long?

CLOUD

1. Are you using IaaS or SaaS?
2. What cloud service provider are you using? IE. AWS, Azure, Google, private
3. If known, how many total workloads do you have?

Elevator Pitch

eSentire is a managed detection and response (MDR) service that stops business disrupting events before they happen. We secure hybrid environments for both users and applications in network, endpoint, log, and cloud. Our elite team proactively hunts and responds

©2024 AVANT Communications. All rights reserved.

to threats, taking actionin real-time while protecting over $7 Trillion in assets. We partner with best-in-breed tools to deliver a holistic and robust platform that ingests, enriches, and normalizes data to hunt and stop threats immediately. eSentire is a 5x Gartner Leader in the Managed Detection and Response Services category.

Objections & Rebuttals

1. **We don't have the budget or leadership support for this investment.**
2. **My business' security and compliance requirements are always changing.**
3. **I already have several tools protecting me.**

1. Many clients have said the same thing, believing highly effective around-the-clock cybersecurity was far more than they could afford, thus not getting leadership support. They were surprised to learn how technology and resources built for the Fortune 500 could be implemented for them, too, and often for less than a full-time employee. Best of all, eSentire can assist with helping you present a business case and ROI for budget approval. Let's set up a quick 30-minute meeting to share how we can do that together. When are you available next week?
2. Of course they are, which is why you are in your position to ensure your company is always in compliance. Implementing security solutions for healthcare, finance, and municipalities is what I like about eSentire. eSentire is PCI DSS certified and holds ISO 27001 and SOC 2 Type II certifications. Their proactive adoption of these compliance mandates demonstrates their commitment to a deep understanding of the disciplined approach required to deliver security operations to highly regulated organizations around the globe. Let's set up a quick 30-minute call to share how they can meet your changing compliance needs. When are you available next week?
3. That is great to hear —all our clients do. Did you know that almost 40% have seven or more tools? Often, they don't have the complete visibility and response time necessary to stop and remediate a threat in all pillars of network, endpoint, log, and cloud. In fact, you can choose which pillar may need to be further strengthened and ensure you get the full robustness and benefits of the tools you have. Let's set up a quick 30-minute call to share how they can help you where you want it most. When are you available next week? Benefits • Absorb Complexity eSentire combines people, process, and technology to deliver turnkey 24/7 threat detection and response across multiple attack vectors (network, endpoint, cloud, log, etc.). • Enable proactive security Managed Risk Services proactively prevent threats by leveraging their unique, integrated threat intelligence and the MITRE ATT&CK framework. • Cost-EffectiveRealize ROI on overall security spend, reduce TCO of threat detection and response by ~50%, and reduce the need to find, train, and retain security talent.

©2024 AVANT Communications. All rights reserved.