VECTRA®

What's your ROI for cybersecurity?

IT security organizations have limited resources to address unlimited risks, threats and attackers. This means security products must be effective as well as operationally efficient. Does your security infrastructure drain manpower and resources or does it make your staff more productive and nimble?

The need for efficiency is especially true of modern cybersecurity. Sophisticated attacks require more time and skill to detect but resources are in short supply. To meet this challenge, Vectra® Networks automates the detection and analysis of sophisticated attacks while making security teams vastly more efficient and productive.

This overview summarizes the operational costs of security investigations and the savings that can be achieved using Vectra software.

Get more details in the white paper

Find out how much time, headcount and money you can save. Download the Vectra white paper, *How to improve ROI and operational efficiency for cybersecurity*, to see the operational cost savings and ROI in security environments.

A scarcity of resources

Today, the process of detecting targeted threats is manual and expensive, requiring an abundance of security skills, time and money.

Skill The demand for skilled security analysts and data scientists has risen sharply in response to the increasing frequency and sophistication of cyber attacks. This has made top talent increasingly hard to find and expensive.

Time Attacks must be detected quickly, before assets are stolen or damaged. Yet network intrusions often go undetected for the better part of a year. Targeted attacks are time-consuming to detect and investigations can take skilled security professionals anywhere from a few hours to several weeks.

Costs Network breaches can have a massive financial impact, but can also have direct costs for the security organization in the form of internal and external incident response and cleanup efforts.

Automation creates operational efficiency

Vectra software addresses the three critical shortages of skills, time and costs. It automates the process of threat detection and data science to identify threats that would be impossible to find through traditional, manual methods of investigation.

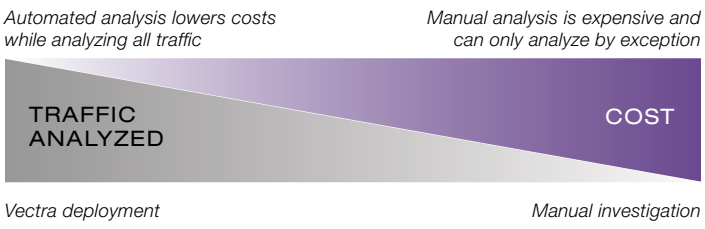
The Vectra value

Vectra is security software that thinks. By automating the process of threat detection and data science, Vectra identifies cyber attacks that would be impossible to find through manual investigation, while simultaneously lifting the time and resource burden from security teams.

While monitoring all local and remote network traffic, Vectra consolidates and automates the detection of active threats that evade perimeter security defenses. Dozens to hundreds of underlying events and metadata samples are automatically consolidated to provide a final diagnosis.

In addition to detecting hidden signs of a threat, Vectra correlates the multiple phases of an attack to specific hosts that are under attack. The ability to condense massive amounts of data down to a few specific hosts is most critical to the rapid containment of a threat.

Vectra is instrumental in proactively detecting targeted and opportunistic attacks before intellectual property, personally identifiable information and other critical data are lost or damaged.



Move faster and reduce costs

The cost of investigating and responding to incidents depends on the number of events, how long they take to resolve, and the experts involved. Vectra customers have reported 75-90% reductions in the time spent investigating security incidents. And they have IT generalists do the analysis instead of higher-paid security experts.

Vectra automatically identifies hosts at the heart of a threat and greatly accelerate the time to containment. The result is that security teams spend less time analyzing and can go straight to remediation. Customers who use Vectra can easily see an 80% savings in the cost of incident response.

By proactively detecting threats and network breaches before data is lost or stolen, security teams have fewer reasons to hire external incident response teams. With rates that are typically hundreds of dollars per hour, it's a significant savings.

What could you save?

With Vectra, organizations can leverage the expert knowledge of our security research team and automate threat detection to ensure that all traffic is inspected, less time is spent on time-consuming manual work, and active threats are mitigated rapidly.

Find out how much time, headcount and money you can potentially save. Download the Vectra white paper, *How to improve ROI and operational efficiency for cybersecurity*, to see the operational cost savings and ROI for security environments.

Get the Vectra Value Calculator — It's free!

The *Vectra Value Calculator* lets you estimate the cost savings with Vectra in your own network. Click here to request your calculator or talk with a Vectra representative.

VECTRA®

Email info@vectranetworks.com **Phone** +1 408-326-2020 www.vectranetworks.com