

DIY is DOA

With so many security products and solutions on the market, you may be thinking about building out your own in-house security operation. After all, how hard could it be? Explore why do-it-yourself (DIY) should be an idea that's dead on arrival (DOA) in your organization when considering the process, people, technology and budget that is needed to be successful.



Estimated costs for a DIY security program for a mid-sized organization:



People
(4 full-time employees at an average \$127K annual salary)

\$508K

Robert Half Technology via Gartner, 2019



SIEM
(estimated at 25% of average total security spend)

\$160K

Challenges to Achieving SIEM Optimization, Ponemon 2017



Additional forensic and workflow tools (SOAR, UBEA, AI/ML applications, etc.)

\$100K*

*Approximately \$25K per security employee



Cloud workload security

\$90K



NGFW and/or IDS/IPS systems

\$75K



Endpoint protection (NGAV+EDR)

\$75K



Vulnerability management

\$50K



Security and phishing awareness training

\$25K



Threat intelligence

\$25K



Regular penetration testing

\$25K



Email security

\$10K

* Estimates based on organizations with 500-1000 employees

THE REALITY

What are the minimum costs to run an effective security program and how do they compare to the average annual security spend for small to medium-sized business (SMB)?



\$1.14M
TOTAL ESTIMATED COSTS

\$650K
AVERAGE SMB SECURITY BUDGET

\$490K (43%)
GAP IN COST

THE CONSEQUENCES

Let's assume you have the budget, resources and stamina to stand up a DIY security program. How effective is your posture going to be in the long run? A DIY approach requires a never-ending investment in people and technology while maintaining the agility necessary to keep up with emerging threats.

Rethinking DIY? You are not alone. Apart from Fortune 500 companies and major nation states (and even this debatable), the vast majority of organizations do not have the resources to navigate today's threat landscape on their own. Thankfully, Managed Detection and Response (MDR) has emerged as a viable solution.

eSentire has been enabling businesses to accelerate their security programs at a fraction of the cost of a DIY approach since 2001.

650+
GLOBAL CLIENTS

97%
CLIENT RETENTION RATE

IN 48 COUNTRIES

99% of eSentire clients report an overall improvement in their security posture

65% of organizations cite limited internal resources as the #1 business driver for choosing eSentire Managed Detection and Response



35 AVERAGE SECONDS TO BEGINNING TRIAGE

20 MINUTES AVERAGE TIME TO ISOLATION AND CONTAINMENT



We now have faster detection of dangerous network activity without all of the false alerts.

— Steve Halvorson, Operations Manager, Preferred Credit



We have peace of mind knowing someone is watching our back during after-business hours with speed to alert, block and remediate threats.

— Gary Smith, IT Manager, Torys LLP

As cybersecurity grows in complexity, DIY security is like performing your own brain surgery. Find out how eSentire MDR can keep your organization secure.

[LEARN MORE](#)