REDUCE COMPLEXITY: THE INFOGRAPHIC

CREATED BY K LOGIX

One of the top challenges CISOs face is reducing complexity within their security program so they may instead focus on business alignment and strategic advancements while continuing to reduce risk. Reducing complexity most often means the combination of an under-resourced team and too many security products.

Furthermore, as businesses transform, the complexity will continue to increase and security will be continually tasked with keeping pace with changes within the business.

TOO MANY SECURITY PRODUCTS

An abundance of underutilized security products hinders productivity and may inhibit strategic focus. On average, CISOs believe 80% or more of their products are underutilized. Managing too many products is a drag on resources, from both a budgetary and time aspect. With consolidation as one of CISOs and security leaders' top priorities, they must focus on reducing the number of products in their environment to free up money to spend on other important areas, as well as give their team time back.

In the article about K logix's Security Investment Assessment, we discuss how this service provides an evaluation and analysis of our customers' security products in order to provide them with the ability to consolidate and operationalize.

CISOs should leverage a service such as K logix's Security Investment Assessment to reduce redundancy, eliminate waste, increase the value of investments, and in turn improve retention.

TEAMS SPREAD THIN

Today, security teams are spread thin. With one million or more unfilled cybersecurity roles, CISOs and security leaders often struggle to find qualified candidates who possess a balance of business and technical expertise and acumen.

Not only are many security teams small, but budget often plays a factor in the ability to expand, or meet salary demands of potential candidates. It also leads to higher employee turnover compared to other industries, with the allure of more money and perks moving people to different organizations. Security teams must be nimble and wear many hats in order to strategically protect the organization and make a positive impact on the business.

As noted in our infographic, teams are dealing with a plethora of tasks including things such as SOC alerts, complex security architectures, and IoT, to name a few. Many CISOs we speak with say their teams' tasks vary daily based on what alerts, new threats, and requests from the business come in.

CLOSING THE COMPLEXITY GAP

We recommend CISOs to partner with organizations to help evaluate their security products and alleviate the time their teams spend on managing underutilized or not fully operationalized products. Before investing in new technology products, they should assess what they currently have.

Security should also be factored into all business decisions. By doing so, security avoids adding complexity to business decisions such as moving to the cloud. If security is brought in after the fact, they are often viewed as roadblocks and impeding progress.

Automation and orchestration are ranked as one of CISOs top goals in 2019. Not only do both of these reduce complexity, but they help transform the security program to keep pace with the changing business.

Integration and collaboration enable security programs to reduce cost. For example, an open, connected, cloud-based security platform brings security products together and closes the gaps that point products leave in your defenses.

If you would like a poster-sized version of the infographic we created, please let us know and we will happily ship it to you.

To learn more about reducing complexity, visit:

www.klogixsecurity.com

THE CHALLENGE:

Under-Resourced Team + Too Many Security Products

leads to

INCREASED COMPLEXITY

TOO MANY PRODUCTS

Enterprises use as many as **40** different security products from **80** vendors[1]

77% report they have too many point products to track and manage[2]

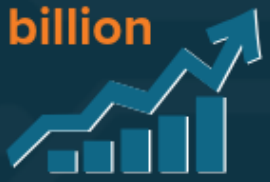
Yet, **45%** of CISOs are focused on acquiring new tools & solutions[2]

TEAMS ARE SPREAD THIN

55% handle more than 10,000 SOC alerts per day[1]

68% believe it is essential to reduce complexity within their security architecture[3]

The number of connected devices in use is expected to grow to **125 billion** by 2030[4]



CLOSING THE COMPLEXITY GAP

Assess the products you have before investing in more

Security must be factored into all business decisions

Automation and orchestration

Integration and collaboration

K logix

Research by: Katie Haug
Graphic created by: Marcela Lima

Sources:

1. "Break Through Cybersecurity Complexity With New Rules..." Security Intelligence, 28 Jan. 2019
2. "Simple Is The Goal: Reducing Complexity In Security." Forbes, 10 June 2019
3. Ponemon Institute Research. "The Cost & Consequences of Security Complexity Study." MobileIron
4. "The Security Risks Presented by Complex Networks." Fortinet, 1 May 2018