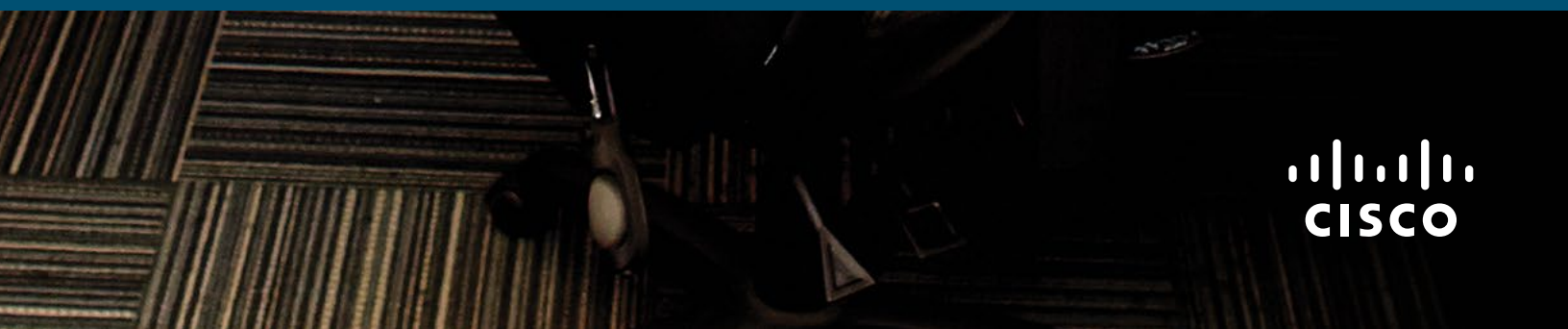
The likelihood of a breach increases every day.

# Can my security architecture keep up?



cisco

## Even in well-managed companies, the typical security architecture is complex, inefficient, and not entirely effective.

The pace of change continues to increase. The continued evolution and change in threat landscape coupled with an ever-increasing attack surface is difficult to stay on top of and manage.

### Multi-vendor approach takes existing security complex and increases it.

**46% of companies have more than 11 security vendors—some as many as 50.**

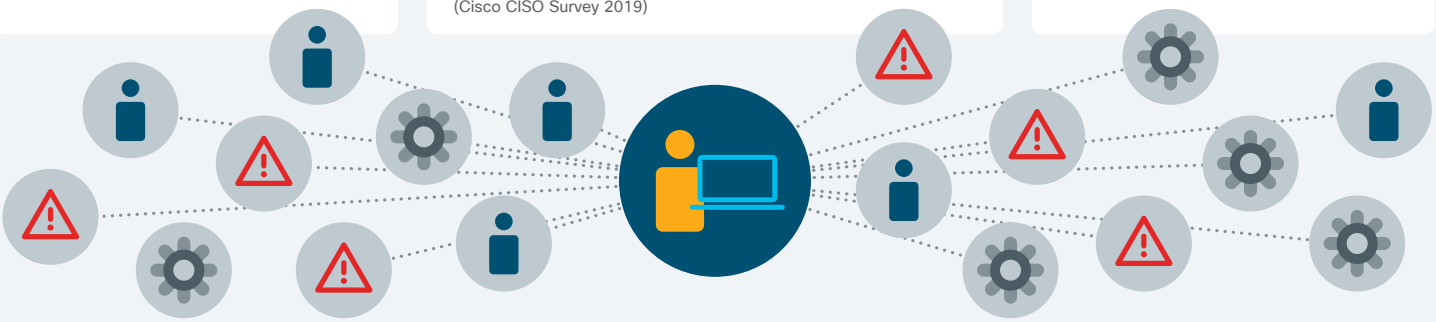
(Cisco 2018 Annual Cybersecurity Report)
"Complexity is the enemy of security"
(Forrester CISO survey)

**Overwhelming number of duplicate alerts compounds the issue**

79% of (CISO) respondents said it was somewhat or very challenging to orchestrate alerts from multiple vendor products

(Cisco CISO Survey 2019)

**Manual configuration and monitoring of disparate security products creates additional inefficiencies.**



### The weakest link in cyber security is still the end user.

> We need to protect the enterprise from their actions as "81% of breaches leverage either stolen or weak passwords.
>
> Verizon Data Breach Report, 2017

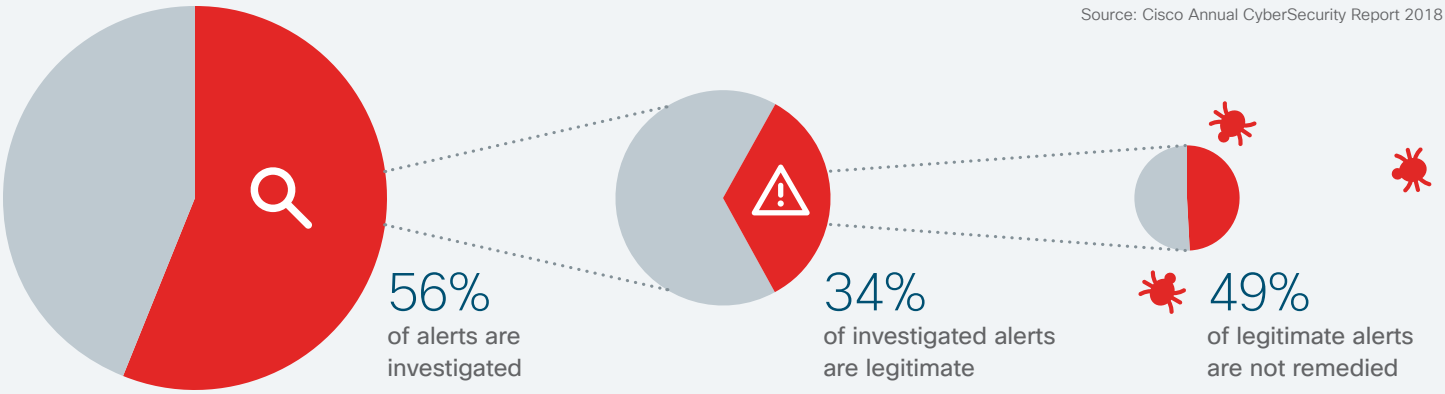
**The bad guys are not hacking into the network—they're just logging in.**

### And there are not enough qualified people to manage it all.

> There will be 3.5 million unfilled cyber security positions by 2021.
>
> Cybersecurity Ventures, *Cybersecurity Jobs Report*, 2018-2021

**We do not have enough time to investigate all the alerts we get and yet we are so swamped we cannot remediate all the legitimate ones we discover.**

Source: Cisco Annual CyberSecurity Report 2018



**What does all this lead to? Increased time to detect and remediate a breach.**

**197 days** Industry average detection time for a breach

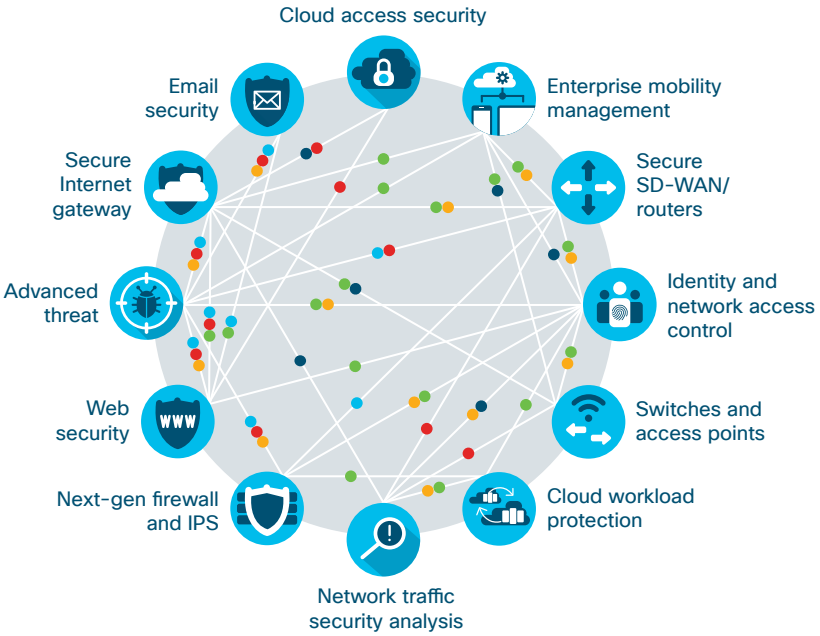
**69 days** Industry average time to contain a breach

**$3.86M** **Average cost of a data breach**

Source: Ponemon 2018 Cost of a Data Breach Study

## Maximize your protection with an integrated architecture. The pieces must work and interact together.

**What it looks like:** Sharing threat information and intelligence data




**What you get:**

| | | |
|---|---|---|
| Shared threat intel and enforcement | = | Increased threat prevention |
| Higher event visibility | = | Decreased time to detect |
| Increased context awareness | = | Decreased time to investigate |
| Enabling automated policy | = | Decreased time to remediate |

## Adopt a threat-centric and trust-centric approach for continuous breach defense.

Today's organizations must manage a delicate balancing act: they need to block threats from bad actors while simultaneously allowing valid users to access critical services and tools.

**Threat-centric**
Dynamically detect, block, and respond to threats in an automated fashion, based on threat intelligence.

**Trust-centric**
Continuously verify identity and device trust across the software-defined landscape.

**See once, block everywhere**
See anywhere in the world, block everywhere you are.

**Multi-factor authentication**
Make absolutely sure the person logging in is who they say they are.

## Cisco is uniquely positioned to provide effective and efficient breach defense.

**Integrated products**

Cisco Security Products work together for increased protection and decreased complexity

**World-class intelligence and visibility**

Cisco Talos Security Intelligence and Research Group is made up of over 300 industry-leading global threat intelligence experts. With Cisco Talos, you get access to the latest threat intelligence

**Incident response capabilities**

Cisco's Incident Response Team of elite security experts provides immediate response remotely, and can be on site within 4 hours

# Next steps

Set up a meeting to discuss in more detail how we can help you achieve your security goals, to:

- Reduce complexity
- Increase efficiency
- Minimize time to detect and respond

## Cisco has a process to get you from where you are today to where you want to be

### As is
Existing

Lacks the ability to prevent, detect, and respond to threats across the full network diameter (endpoint to cloud)

Gamut of security tools with multiple consoles (OPEX intensive)—and yet still vulnerable

### Phase 1
Prevention

Leverages efficient prevention methods to reduce overall risk exposure and maintain brand reputation

### Phase 2
Detection

Reduces risk exposure and costly expenses that result brand damage associated with a breach by securing the largest malware/ransomware threat vectors

### Phase 3
Response

Reduces cost and increases employee productivity through a consolidated management console that accelerates forensic investigations across the network diameter

### Desired state

Comprehensive incident prevention, detection, and response plan in place with prescriptive procedures on handling a breach effectively and efficiently