The likelihood of a breach increases every day. Can my security architecture keep up?
Today’s security landscape is too complex, too fragmented, and too ineffective.

Too many vendors leads to too much noise and too little protection.

46% of companies have more than 11 security vendors, and they are all getting breached.
Source: Cisco 2018 Annual Cybersecurity Report.

The overwhelming number of alerts compounds the issue: 77% of mid-market businesses found it somewhat or very challenging to orchestrate alerts from multiple vendor products.
Source: Cisco 2019 CISO Benchmark Study

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

The lack of cybersecurity talent makes the problem worse:

There will be 3.5 million unfilled cybersecurity positions by 2021.”
Source: Cybersecurity Jobs Report 2018-2021, Cybersecurity Ventures

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

Only 56% of alerts are investigated.
Source: Cisco 2018 Annual Cybersecurity Report

Of those, 10% are not remediated.

And who knows what’s in the other 44%?
Source: Cisco Small and Mighty security report

The average cost of a breach for 71% of mid-market businesses is over $100K.

Source: Cisco 2018 Annual Cybersecurity Report

The weakest link in cybersecurity is still the end user.

We need to protect the enterprise from their actions, as 81% of breaches leverage either stolen or weak passwords.
Source: 2017 Verizon Data Breach Investigations Report (DBIR)
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:
- Reduces noise
- Easier for teams to manage
- Reduces the number of gaps in the network bad actors can take advantage of
- One overall view of security through Cisco Threat Response

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

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.

Multifactor authentication
Make absolutely sure the person logging in is who they say they are.

Cisco and our Partner Ecosystem are uniquely positioned to provide effective and efficient breach defense.

Integrated products
World-class intelligence and visibility
Incident response capabilities
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 and our Partner Ecosystem are the best strategic partner to deliver on the journey to increase your security effectiveness.

**As is**
Existing network
Lacks the ability to prevent, detect, and respond to today’s threats effectively.
Too many tools and too much complexity create too many security gaps.

**Phase 1**
Prevention
Get visibility into who and what is on the network to minimize the threat to your network.

**Phase 2**
Detection
Limit risk to costly expenses associated with a breach by securing the largest malware threat vectors.

**Phase 3**
Response
Accelerate forensics investigations and remediation through a consolidated management console across the network diameter.

**Desired state**
A singular console to accelerate forensic investigations
A global threat information database, providing a platform for information sharing and unified protection
A comprehensive incident response plan with prescriptive procedures on handling a breach efficiently

Partner call to action: Learn more

cdw.com/cisco