The digital environment becomes more complex every day.

# Does my security architecture have to do the same just to keep up?

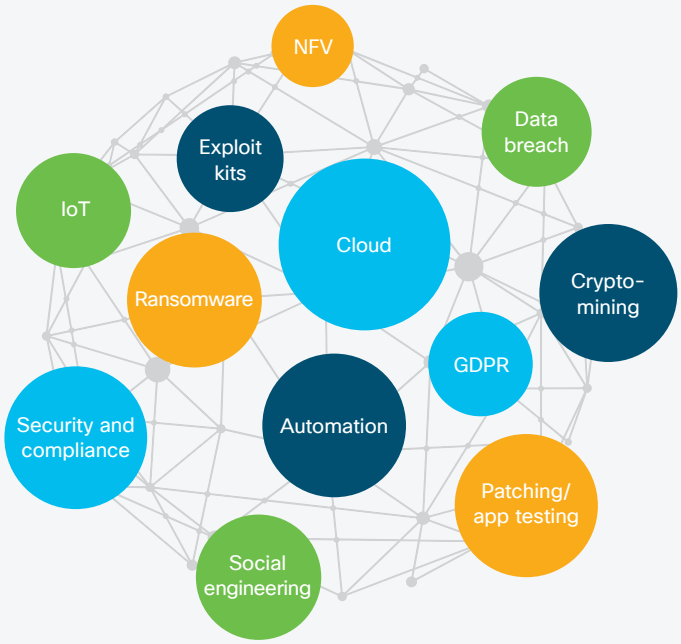
Anazeem Information Technology

www.anazeem.com

cisco Partner Gold Certified

# Even in well-managed companies, the typical security and network architecture is complex, costly, and limiting of security goals.

**Increasing pace of change:**
Continued evolution and change in the threat landscape, coupled with an ever-increasing attack surface, is difficult to stay on top of and manage.




**Complexity:**
A multivendor approach takes existing security complexity and increases it.



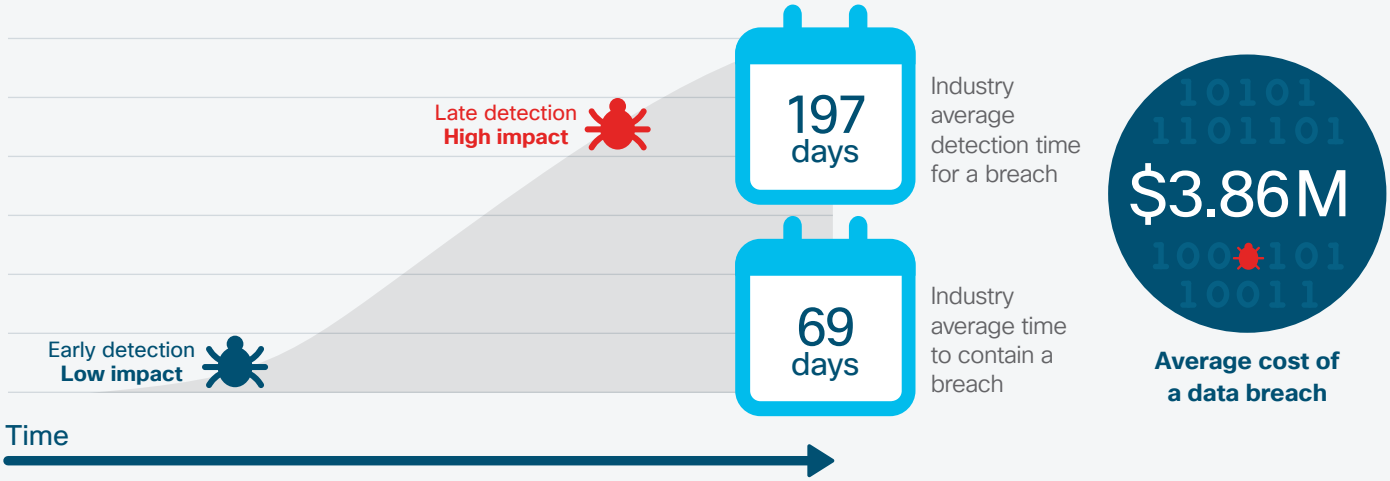
**Inefficiency:** A manually managed network, with lots of opportunities for errors and mistakes, opens up additional new security problems.

**Security operations centers are understaffed**

**Overwhelmed with alerts from disparate security products**

**Unable to keep pace with current threats**

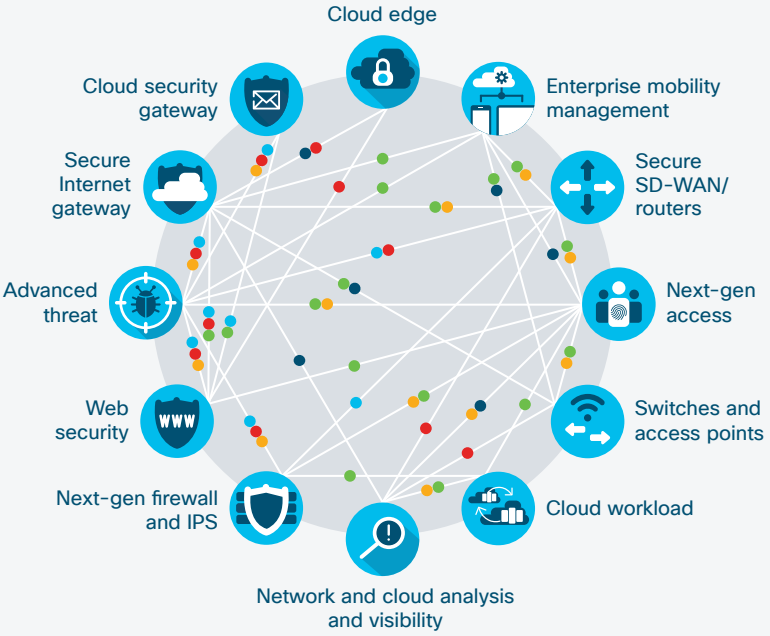
**Difficulty of detection and response:** Use of mobility and cloud leads to an expanded attack surface, increasing the time to detect and remediate attacks.




Source: Ponemon 2018 Cost of a Data Breach Study

## Maximizing your protection requires an integrated architecture. The pieces must work together.

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

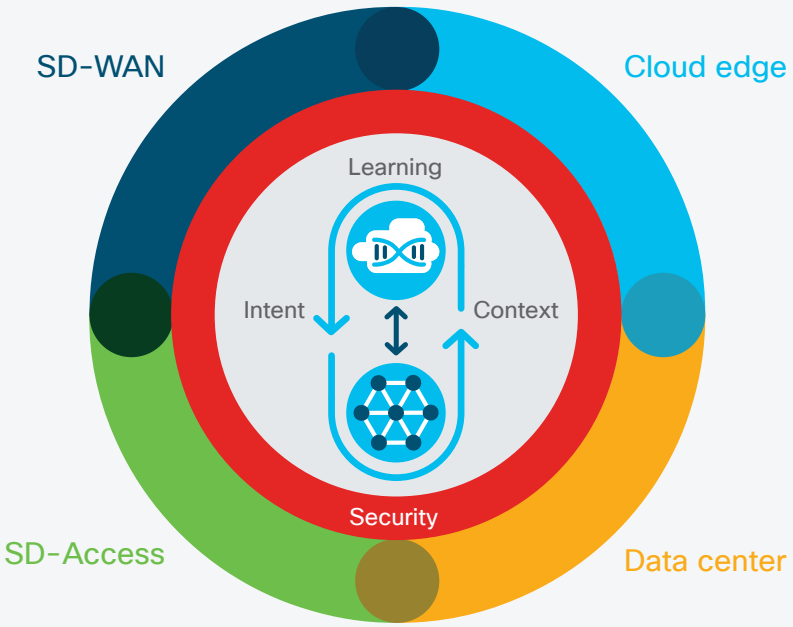



**What you get:**
"See once, block everywhere"

| | | |
|---|---|---|
| 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 |

## Aligning the integrated security architecture with an intent-based network creates measurable benefits.

- **Reduce complexity:**
  Embed security into SDN control points to break down silos.
- **Create efficiency:**
  Combine cybersecurity with intent-based networking to introduce automation and orchestration capabilities (lower risk and quicker response).
- **Accelerate forensic investigations:**
  Leverage integrated assurance and threat response platforms to ingest security telemetry.
- **Secure data access:**
  Adopt a "trusted access" strategy to ensure that all data and resources are accessed securely, regardless of whether they are public or private, to help meet compliance standards.



## Cisco and our Partner Ecosystem are uniquely positioned to provide an integrated security architecture.

**Automation reduces the burden.**

**Alerts are relevant and prescriptive.**

**Security and threat intel work together.**

# Next steps

Set up a meeting to discuss in more detail and learn 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 partners for the journey to increase your security effectiveness.

### As is
Existing network

Multi-vendor environment with complex operations and silos of information creating pockets of visibility

### Phase 1
Integrated architecture

Aggregating intent and delivering security with domain policy through an integrated architecture via domain SDN control points

### Phase 2
Trusted access

Establishing trust through a framework that verifies user identity, device security, and secure access to both public and private apps

### Phase 3
Integrated assurance and threat protection

Ingesting security telemetry from the network and presenting it visually, leading to faster threat detection and containment

### Phase 4
Dynamic security protection

Constantly learning, sharing threat information, and tying actionable responses to behavior for auto-containment/quarantine

Anazeem Information Technology

www.anazeem.com

Cisco Partner Gold Certified



C07-743232-00 01/20