Reactive security protocols are a thing of the past. Take control of your security operations to proactively secure your business.

What is security leadership up against?

- **Current security tools struggle to detect and investigate sophisticated threat actors like BlackTech, Volt Typhoon or Wizard Spyder.**
- **Sophisticated threats like ransomware require detection and response that goes above and beyond.**
- **Security leadership and their teams are being asked to do more with less and better ROI.**

As attack volumes, frequency, and sophistication increase, SOC teams are becoming increasingly overwhelmed.

- **83%** of IT and security pros say their security alert fatigue is getting worse.
- **37%** say their alert fatigue is getting worse.

**Better experiences:**

- **See more, respond faster and alleviate analyst burnout with a better SOC experience.**
- **Alert fatigue is getting worse, but a better SOC experience can be achieved.**

**Breach Protection** gets you there by:

1. **Detecting threats sooner**
2. **Prioritizing incidents by potential impact**
3. **Conducting investigations quickly**
4. **Minimizing exposure**
5. **Accelerating response times**

**What is security leadership up against?**

- **Ransomware attacks are getting more costly.** The average cost of a ransomware attack, not including the cost of the ransom, is $4.45M.

**Why is security leadership up against?**

- **83%** of security leaders have experienced more than one data breach.
- **37%** say their alert fatigue is getting worse.

Disparate detection signals and complex investigations contribute to alert fatigue, which is causing high analyst turnover.

**Better ROI:**

- **Get more out of your existing security resources with automated responses and guided investigations, built to optimize SOC productivity.**

**Detecting threats sooner**

- **Minimize exposure**
- **Prioritize incidents by potential impact**
- **Minimize business risks**
- **Conduct investigations quickly**
- **Gain a full understanding of attacks**
- **Accelerate response times**
- **Stop attacks before they cause damage**

**Breach Protection** gets you there by:

- **See more, respond faster, and alleviate analyst burnout.**
- **We see billions of authentication requests, we see the phishing attacks, we see the bad web pages, we track every process that makes a connection from the endpoint so your SecOps teams know what's going on—and can stop threats, like ransomware, in their tracks.**
- **Delivered with the Cisco Security Cloud, users gain an end-to-end platform view, giving them the visibility and power to pair human intuition with AI and automation.**

**Breach Protection is bolstered by:**

- **Threat researchers**
- **500 security events observed daily**
- **550B security events observed daily**
- **AI algorithms**

**With Cisco Breach Protection Suite, security teams can stop threats such as ransomware, phishing, malware, and insider threats across their endpoints, email, network, and cloud environments.**

**Extended Detection and Response (XDR)**

- **Threat detection and response that goes above and beyond.**
- **A better SOC experience makes for a more secure business.**

A better SOC experience makes for a more secure business.