You can’t defend against threats you don’t address.

With 44% of security alerts never being investigated, organizations need simple and more effective solutions.

Disconnected and disparate systems can cause compatibility issues and add a layer of complexity to manage.

55% use between 6 and 50+ security vendors
65% use between 6 and 50+ security products

44% of alerts are NEVER investigated
54% of legitimate alerts are not remediated

80% of breaches lasted more than an hour
30% of systems

49% managed public scrutiny of a security breach

Impact of security breach is tangible
22% lost customers
23% lost opportunity
29% lost revenue

Majority of breaches impacted 30% of systems

Constraints
Organizational issues create environments that breed complexity.
Top 4 Constraints:
1. Budget
2. Compatibility
3. Certification
4. Talent

Impact
Complexity opens gaps in defenses, giving bad actors unconstrained time to operate.

Perception
Confidence and trust in tools and infrastructure must be verified.

71% believe their tools are effective at detecting unknown threats
58% believe their infrastructure is up-to-date
74% believe their tools are effective against known threats

Download the Cisco 2017 Annual Cybersecurity Report:
www.cisco.com/go/acr2017

A simple, integrated, and automated defense will give you the tools and visibility to combat the ever-expanding threat landscape.

With 44% of security alerts never being investigated, organizations need simple and more effective solutions.