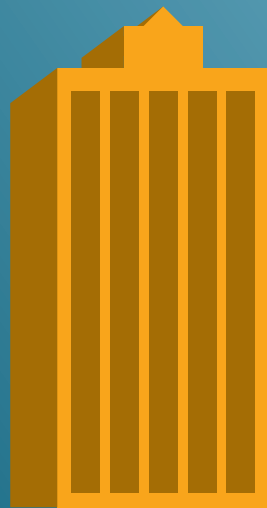




# The need for an integrated security management platform

**Fran Howarth**  
Senior analyst, security

*“It’s not if, but when and how often”*



**81%**

**Large  
organisations**



**60%**

**Small and medium  
organisations**

*Three-fold increase  
over previous year*

*Source: PwC/Infosec Europe 2014, Symantec*

A red banner with the words "STORE CLOSING!" in large, white, bold, sans-serif capital letters.A yellow sign with the text "LAST 10 DAYS!" in blue, bold, sans-serif capital letters. The number "10" is enclosed in a dark blue square.A white banner with the text "GOING OUT OF BUSINESS" in black, bold, sans-serif capital letters. The word "FURNITURE" is partially visible at the bottom right.A white sign with the words "WE QUIT" written in large, red, hand-drawn capital letters. To the left of the text, there are handwritten notes: "1/2 off Albums" and "1/2 off Frames".A grey sign with the text "Building for Lease" in red, bold, sans-serif capital letters.

## Smaller firms vital for the economy



- Percent of total number of businesses
- Contribution to employment (% total)
- Annual turnover (% total)

Source: UK Department for Business, Innovation & Skills



Source: Ponemon Institute

A unified security management platform:

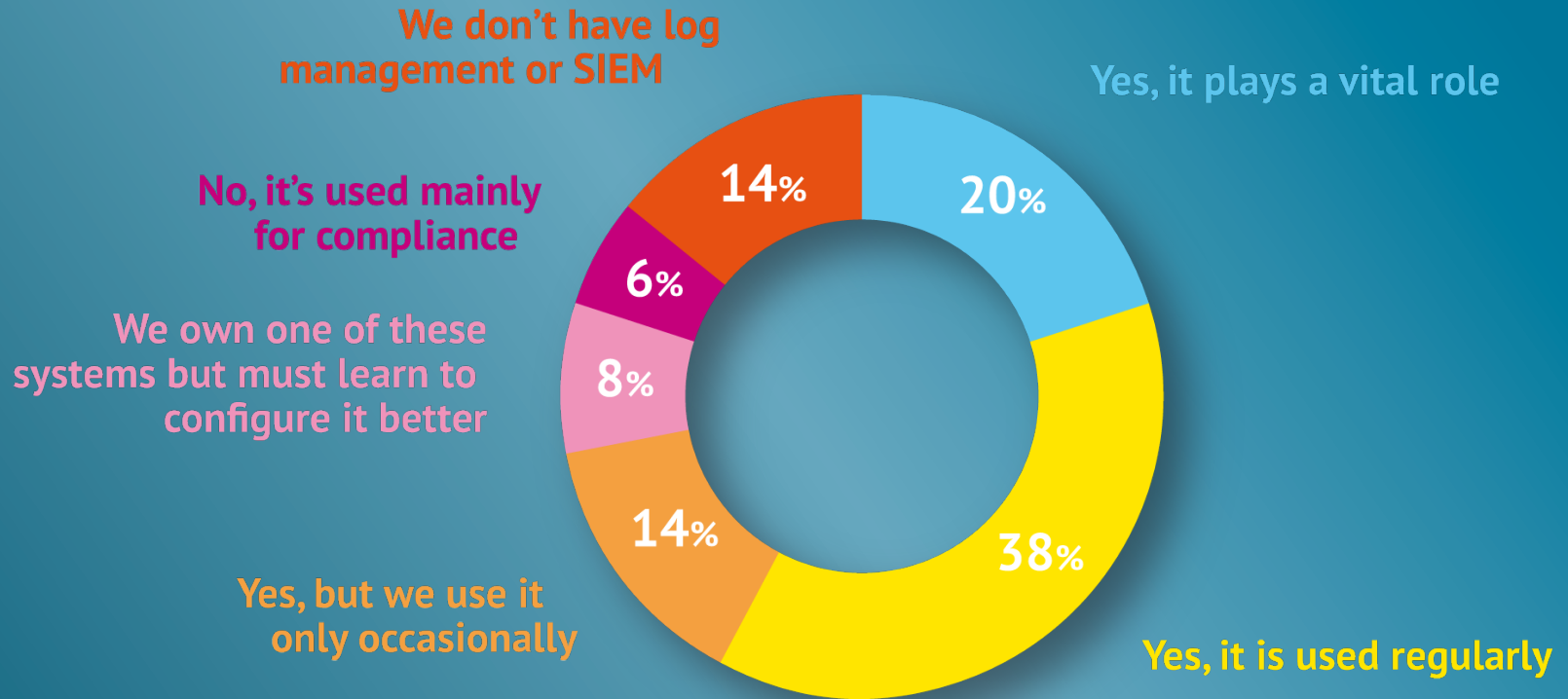
- Asset discovery
- Vulnerability and threat management
- Threat identification and management
- Behavioural monitoring
- Security intelligence
- Centralised management





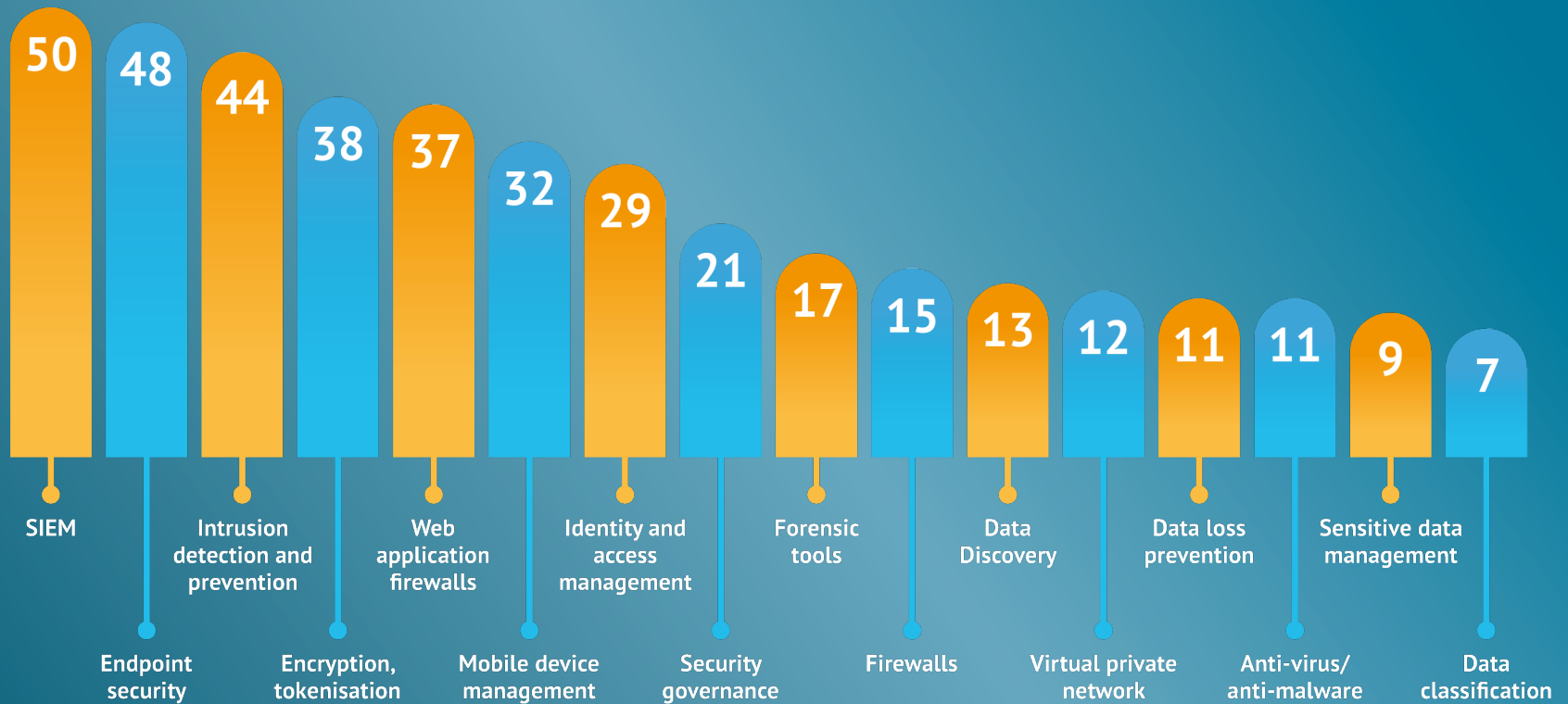


# Threat identification: the role of threat intelligence



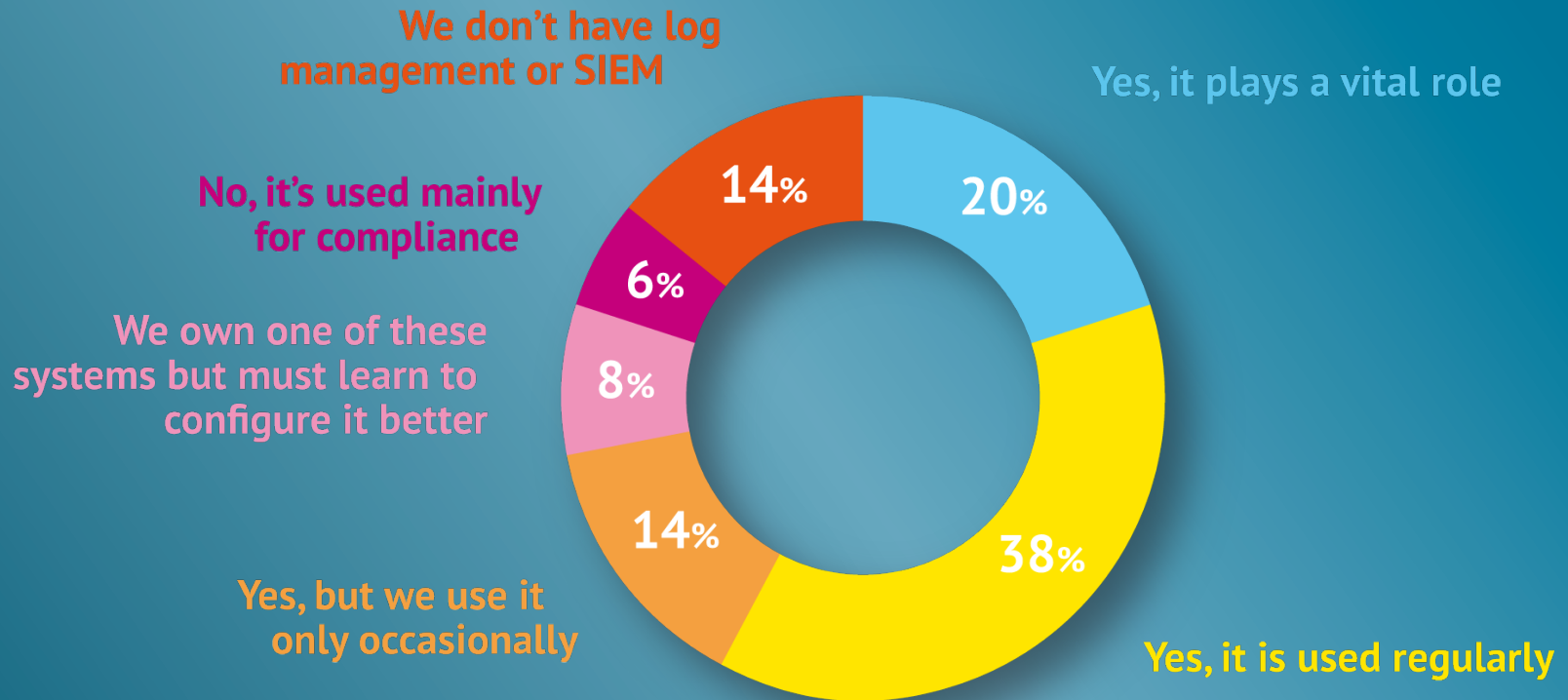
Source: InformationWeek





Source: Ponemon Institute

# Use of SIEM for security intelligence



Source: InformationWeek

- Integrate tools into a single operating console or dashboard
- Maintain a continually updated software inventory
- Use continuous vulnerability monitoring
- Complete a hardware inventory
- Use network mapping
- Incorporate log aggregation and correlation
- Take threat intelligence feeds for threat identification and prioritisation

*Source: SANS Institute*

# Expected improvements for incident response

More automation/SIEM integration  
for reporting and analysis

68%

Improved visibility into threats and  
associated vulnerabilities as they apply to

59%

Improved remediation and  
follow-up processes

53%

Improved ability to scope impacted  
systems and pinpoint source

42%

Better response time

42%

Source: SANS Institute

- Correlation of data from throughout network
- Anomaly detection
- Comprehensive visibility
- Advanced threat protection
- Risk prioritisation
- Alerting and monitoring
- Customise according to business needs
- Demonstrate adherence to policies and controls
- Protect sensitive data
- Limit exposure to breach disclosure
- Reduce risk to business partners and customers
- Reduce costs