2017 FORRESTER SOC SURVEY

91% of survey respondents have experienced at least one

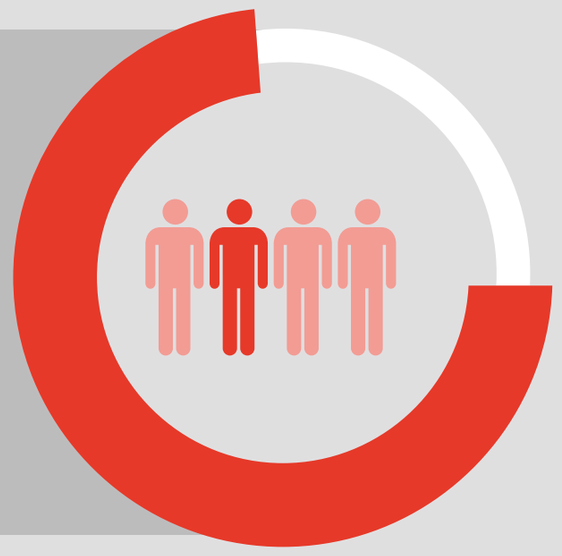
ATTACK OR DATA BREACH

that put their organization at risk in the past year.

73% of respondents agreed that though they are interested in acquiring deeper visibility into endpoint behavior, they

LACK STAFF EXPERTISE

to respond to detected events.



66% of respondents agree that their current visibility into endpoint behavior is lacking in

DEPTH & BREADTH

required to detect zero-day malware or targeted threats.

71% survey respondents are using **5 OR MORE** technologies in their SOC...

1/3 survey respondents are using **8 OR MORE** technologies.

> "What I'd like to do is reduce the overall risk footprint, thus being able to reduce the number of tools. There's a lot of work that we're doing to try to reduce overlap of tools."
>
> **- CISO of a global energy company**

Organizations are looking for the right tools to help them

PREVENT, DETECT & RESPOND

to endpoint attacks, and discover and reduce network

KEY RECOMMENDATIONS

1. Look for an **INTEGRATED** endpoint prevention, detection, and remediation
2. Expand detection **BEYOND** static IOCs
3. Build **SOC SKILLS** through automation

ENDGAME is the single centrally managed endpoint platform that stops targeted attacks and all of their technologies and techniques, before damage and loss occurs, with the people you already have.

REQUEST A DEMO

endgame.com/demo