The SIEM of Tomorrow

How SIEMs Are Evolving to Power the Modern SOC

Michelle Abraham
Research Director,
Security and Trust, IDC

Table of Contents

CLICK BELOW TO NAVIGATE TO EACH SECTION IN THIS DOCUMENT.

In This InfoBrief

The SIEM has moved beyond a place to simply store and analyze logs. It has evolved to become a modern threat detection, investigation, and response platform that acts as a centralized hub for the SOC, unifies security workflows, provides contextual security visibility, and delivers correlated and threat intelligence–enriched alerts.

The research comes from several IDC surveys.

SIEM
Security information and event management

SOC
Security operations center

SOCs Are Dealing with a Lack of Visibility and Too Many Alerts

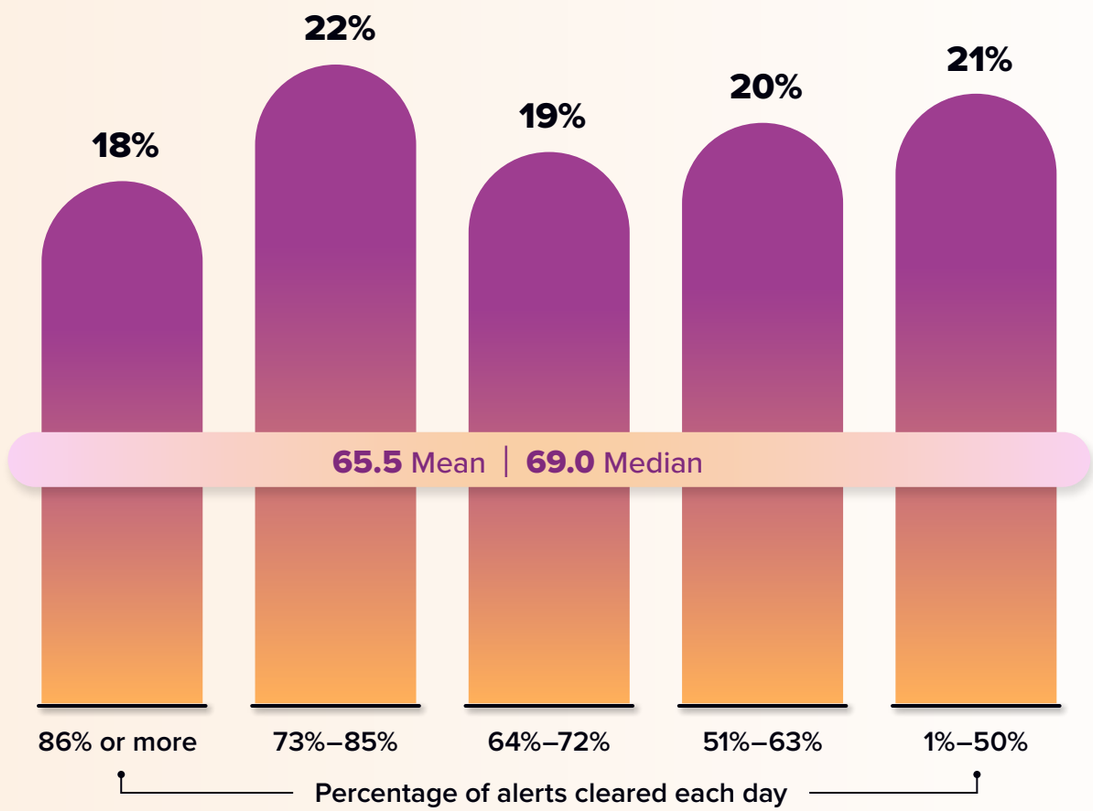
On a daily average,
organizations with a SIEM

clear only **65%** of alerts,

leaving **35%** uninvestigated.

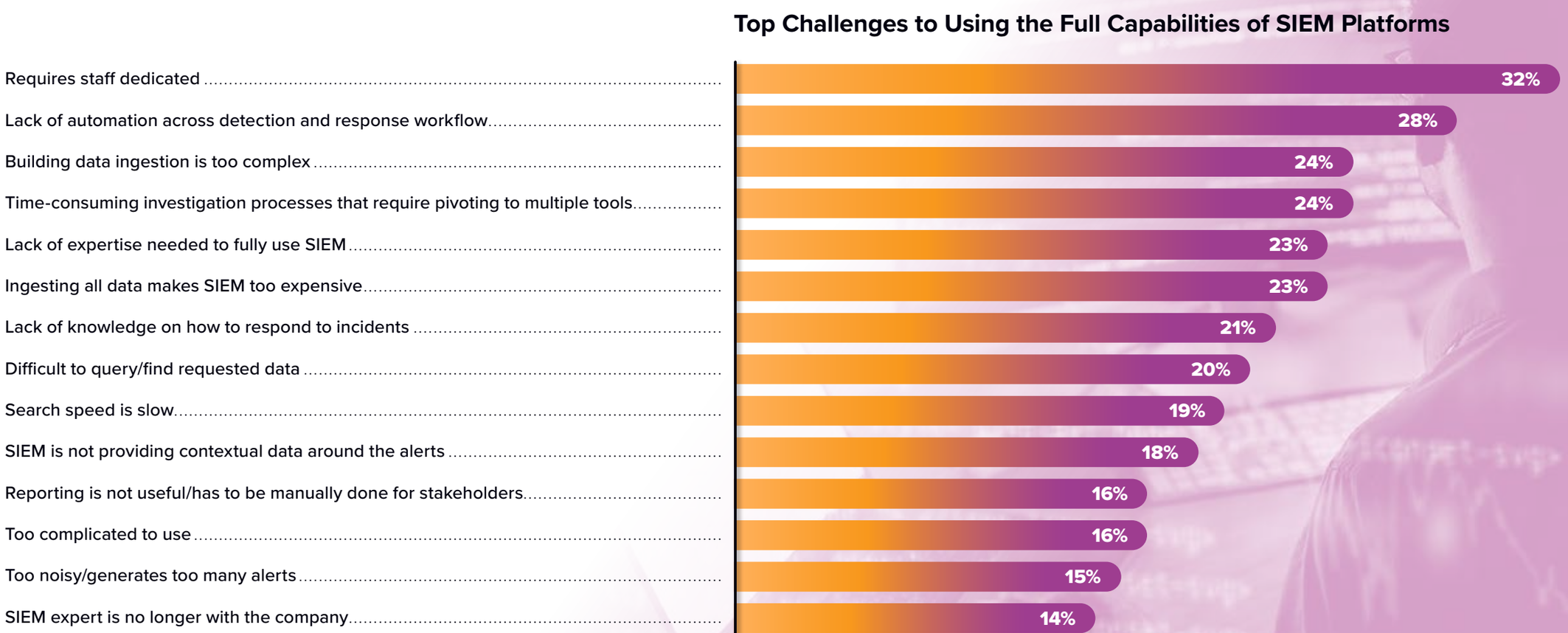
SOC teams find it
impossible to get to all alerts
with the resources they have today.

Percentage of Organizations Clearing Alerts Each Day



n = 259; Source: IDC's *U.S. Security Operations Center Survey*, December 2022

Traditional SIEMs Are Still Challenging, According to Users and Managers



n = 1,004; Source: IDC's *Worldwide Views on SIEM Survey 2024,* January 2024

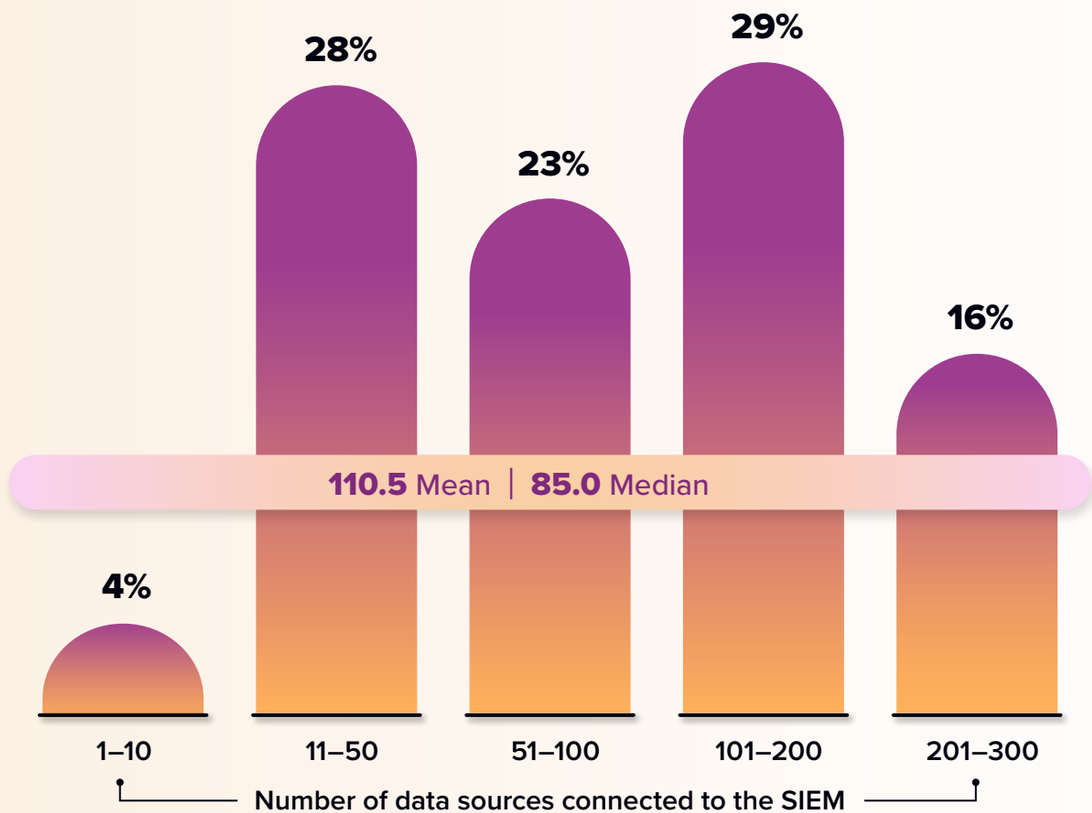
Practitioners Want to Bring In Data from Many Sources

Modern SIEM platforms can efficiently process data, analyze data where it lives, and correlate the data, presenting the SOC analyst with the information gathered.

Ensuring that the SOC is able to **centralize all the data in a SIEM brings down the risk of failing to detect a threat** because data was in silos.

On average, organizations have over 100 sources of data connected to their SIEM. Oftentimes, when allowed, they want to bring in more because the SIEM is the starting point for security investigations. As seen from the challenges presented previously, managing data is still an issue for SOC teams.

Organizations Have SIEMs Connected to Multiple Data Sources



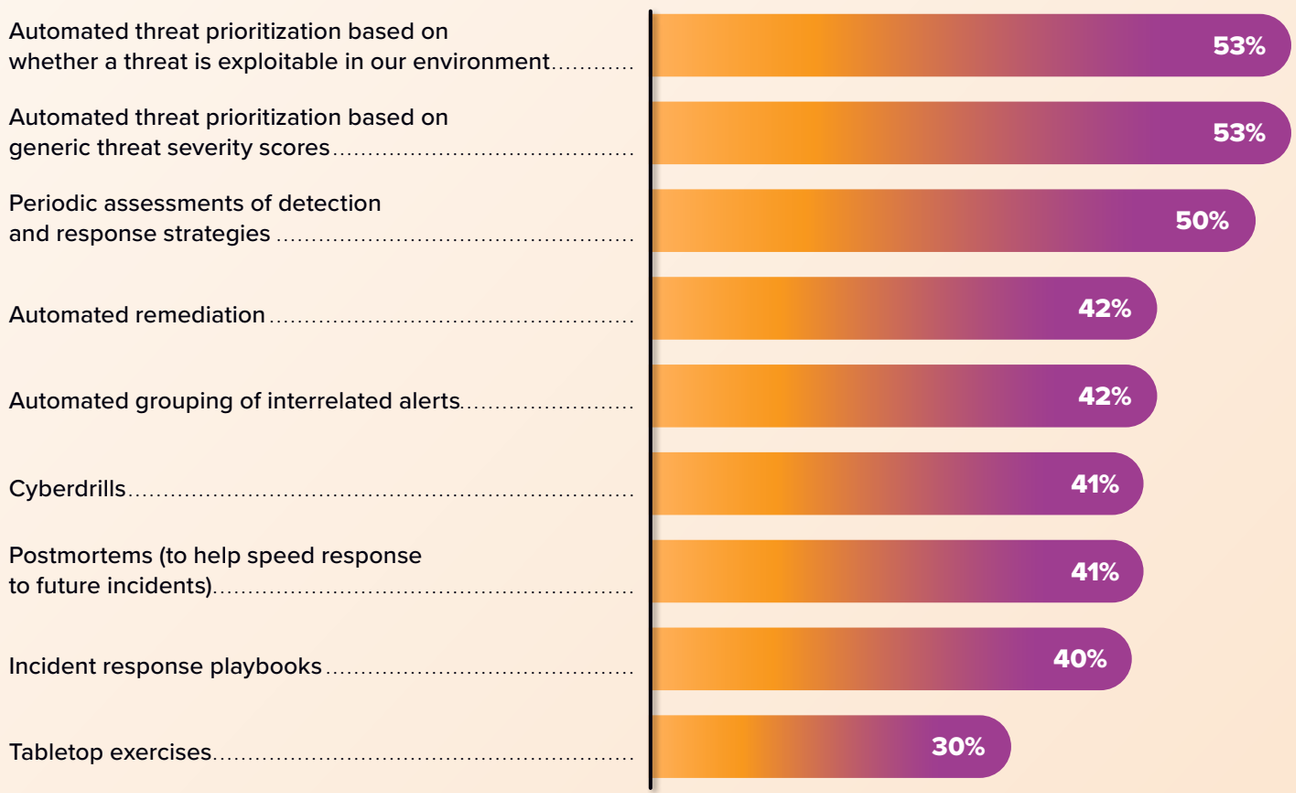
n = 1,004; Source: IDC's *Worldwide Views on SIEM Survey 2024,* January 2024

There Is a Desire to Unify Detection, Investigation, and Response with Automation

Practitioners want a modern SIEM that can unify detection, investigation, and response because it will:

- Take into account severity and exploitability when prioritizing alerts
- Enrich the alerts with threat intelligence
- Help with alert fatigue and the amount of time per investigation

Practices Organizations Want for Speed Detection and Response



n = 258; Source: IDC's *North American Cybersecurity Capabilities Assessment Framework (CCAF) Survey,* August 2023

Today's SOC Teams Prefer These Features

A detection engine that can keep up with the pace of today's threats

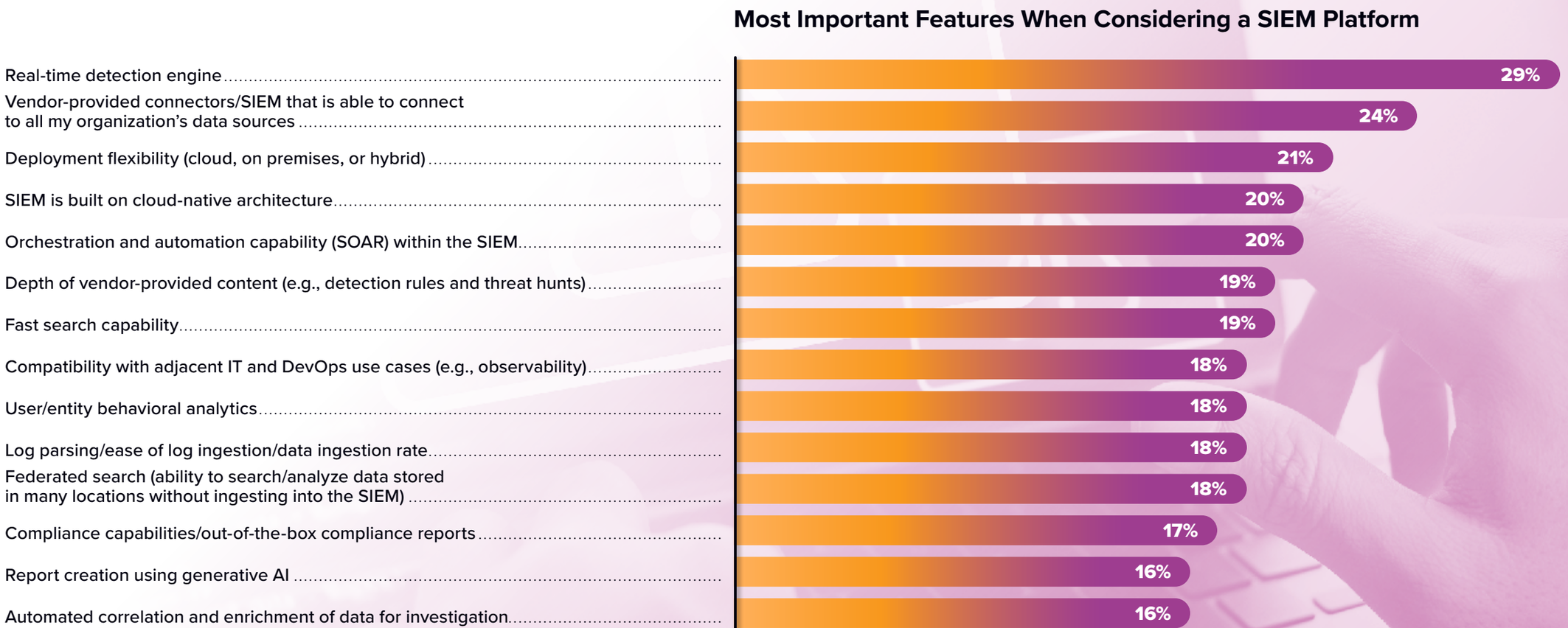
Connection to all the data sources the organization wants to use from the vendor

Deployment flexibility

User and entity behavioral analytics to find stealthy threats that trend over time

Automation built into the platform, eliminating the need to swivel into something else

Today's SOC Teams Prefer These Features (continued)



n = 1,004; Source: IDC's *Worldwide Views on SIEM Survey 2024,* January 2024

Essential Guidance

Choose a SIEM that allows you to:

Ingest the data you need for visibility across your environment, eliminating any gaps that allow threat actors to go undetected.

Automate, automate, automate.

There are too many alerts to manage, **so automation should prioritize which are most critical.**

Look for built-in automation capabilities that work seamlessly in the SIEM.

Many alerts may be auto-dispositioned through correlation with other alerts.

Essential Guidance (continued)

Look for solutions that unify detection, investigation, and response workflows to reduce swivel time in other platforms.

A modern SIEM doesn't stop at data and log analysis. It includes capabilities across detection engineering, data federation, manual task automation, threat intelligence, user and entity behavior analytics, detection engineering, investigations that align to industry-standard frameworks, and case management — all built in.

The combination of these capabilities within one common user interface will unify detection, investigation, and response workflows to reduce mean time to detect, reduce mean time to resolve, streamline processes, and provide better protection for organizations.

About the IDC Analyst

Michelle Abraham
Research Director,
Security and Trust, IDC

Michelle Abraham is the research director in IDC's Security and Trust Group responsible for the Security Information and Event Management (SIEM) & Vulnerability Management practice. Michelle's core research coverage includes SIEM platforms, attack surface management, breach and attack simulation, cybersecurity asset management, and device and application vulnerability management alongside related topics.

More about Michelle Abraham

Message from the Sponsor

Learn more about how Splunk Enterprise Security is powering the SOC of the future at splunk.com/es.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

idc.com @idc @idc

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.