NETWITNESS

From Rapid Response To Proactive Planning

Highlights from “The Pandemic-Driven Evolution of Security Operations” Report

The worldwide health crisis that kicked off 2020 has had a profound impact on everyone, everywhere—and security operations teams are no exception. You can see clear evidence of the impact in a survey of security industry leaders around the globe conducted in mid-2020 by Omdia in partnership with RSA. Read on to learn about the pivot to remote work that security operations teams quickly made in response to the pandemic, and about the longer-term changes they expect to see in 2021 and beyond.

An Unprecedented Move To Remote Work

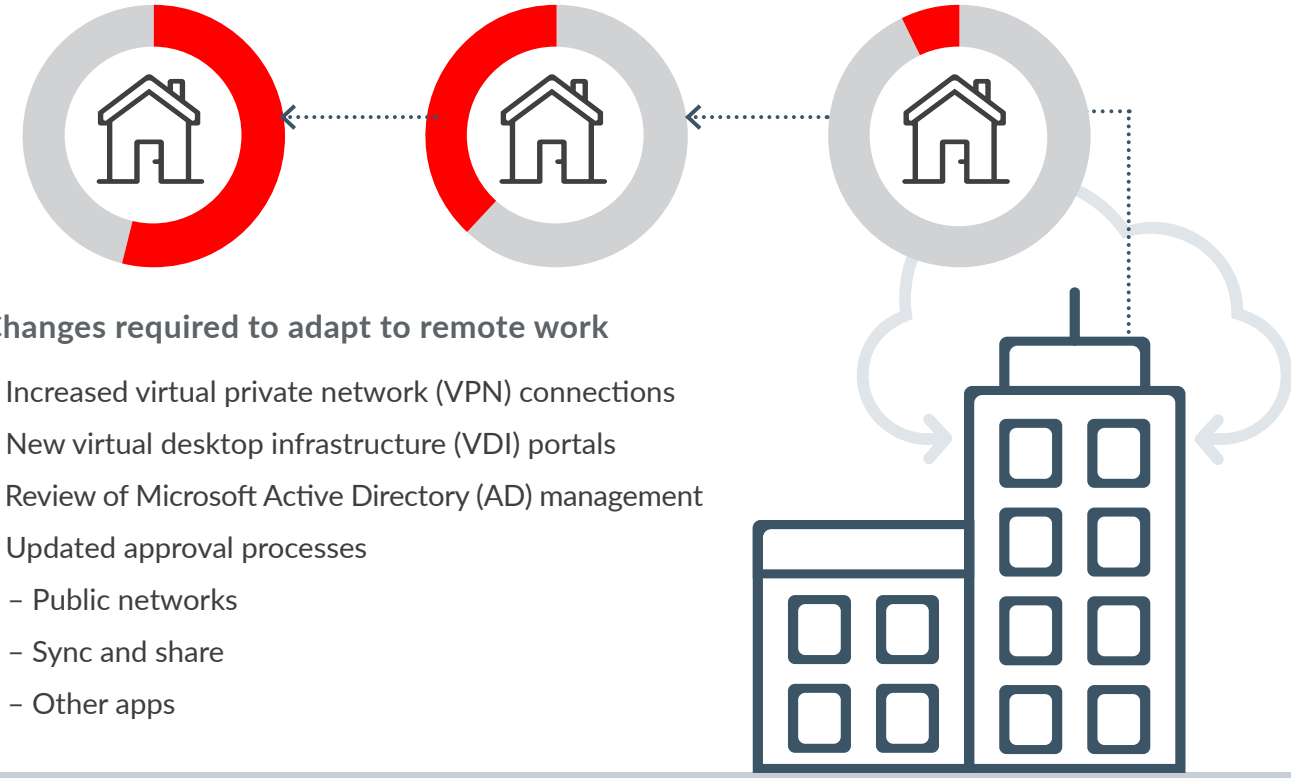
When vast numbers of people began working from home to reduce health risks, security operations had to adapt quickly to securing applications and systems far beyond the traditional perimeter. Even more challenging, they had to do it while working remotely themselves.

Percentage of organizations shifting security workforce to remote work

54%
Shifted a large proportion to remote work

38%
Shifted a moderate proportion to remote work

7%
Shifted a small proportion to remote work



Changes required to adapt to remote work

- Increased virtual private network (VPN) connections
- New virtual desktop infrastructure (VDI) portals
- Review of Microsoft Active Directory (AD) management
- Updated approval processes
  - Public networks
  - Sync and share
  - Other apps

"Although we were averse to the cloud and remote working beforehand, we shifted everybody. It happened very quickly with little warning." CISO-LEVEL STUDY PARTICIPANT

Top Challenges of Security Operations Teams Working Remotely

The new reality of having some proportion of security operations teams working from home has presented a variety of challenges for organizations. Respondents were asked to rank the challenges they faced.

Top 3 challenges ranked by respondents

60%
Ranked carrying out SOC responsibilities with staff working remotely

54%
Ranked enforcing security standards for the resources work-from-home users adopted

50%
Ranked the risk of new unmanaged devices accessing the organization's resources

The technology wish list

To address these and other challenges of remote work, security operations teams would like to have more of the following technologies:

- Machine learning (ML)
- Artificial intelligence (AI)
- UEBA
- Security information and event management (SIEM)

"The nature of incidents has changed—we've had to launch a proactive campaign highlighting phishing attacks embedded in emails about the pandemic." FINANCIAL SERVICES SECTOR CISO

What's Next for Security Operations

Survey respondents were asked about their views of various scenarios affecting security operations in the next 6-12 months—and the next 13-24 months. Most scenarios were cited for the 6- to 12-month period rather than the longer term.

Top scenarios expected to affect security operations in 6-12 months

60% Anticipated at least some employees would continue to connect remotely to work assets

60% Expected security operations to become more agile to adapt to changing priorities

53% Believed security initiatives would receive higher priority in the organization's overall strategy

Top scenarios expected to affect security operations in 13-24 months

43% Believed security initiatives would receive higher priority in the organization's overall strategy

43% Expected a relatively larger portion of budget to go to IT department

41% Expected a relatively larger portion of budget to go to cybersecurity department

41% Thought use of cloud or SaaS applications would accelerate faster

Most scenarios were cited for the 6- to 12-month period rather than the longer term, pointing up the need for proactive planning.

Organizational Strategy and Security Priorities: The Cloud

Increasing the security of technologies deployed in the cloud is a top priority to support organizational strategy. Cloud security was cited as a high priority in a post-pandemic world for two-thirds of organizations.

Importance of cloud security initiatives to organizational strategy

49%
Ranked enabling or increasing cloud cybersecurity as first or second most important

47%
Ranked shifting from preventative controls to detect-and-respond first or second most important

41%
Ranked shifting from VPN to direct-to-cloud access model first or second most important

Cybersecurity priorities for a post-pandemic world

- Two-thirds of respondents cited cloud security as a high priority
- More than half cited mobile security as a high priority
- 42% cited IoT security as a high priority

Cybersecurity was cited as a high priority in a post-pandemic world for two-thirds of organizations.

Take the Next Step

Want to dive deeper into the effects of the pandemic on security operations teams—and what they envision for the future? Read the complete report from Omdia and RSA: The Pandemic-Driven Evolution of Security Operations.

About NetWitness

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats. For more information, go to netwitness.com.

NETWITNESS
An RSA Business