Carbon Black.

10 ENDPOINT SECURITY PROBLEMS SOLVED BY THE CLOUD

Endpoint security is a challenge. There is too much complexity and cost, defenses aren't keeping up, and security staff is stretched thin. The cloud can help!

1 Keeping Up To Date

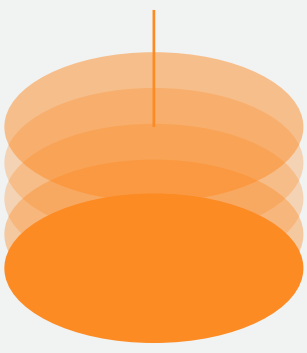
" [With traditional AV,] configuration settings were not intuitive, and we had updates fail and break a lot of things."

– **CHRIS ST. AMAND**
NETWORK SECURITY ENGINEER / PEOPLESBANK

CLOUD SIMPLIFIES AND AUTOMATES UPDATES.

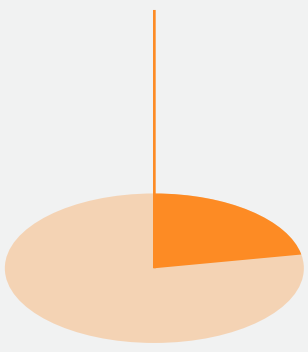
2 Integrating Security Products

49%



describe their endpoint detection and response (EDR) systems as not integrated or only partly integrated.[1]

4%



consider their security analytics to be fully integrated.[2]

CLOUD APIS AND PRE-BUILT INTEGRATIONS UNIFY PRODUCTS.

3 Managing Multiple Agents

" IT and security personnel are tasked with managing and maintaining multiple endpoint agents that often have fragmented security systems."

– **E-SECURITY PLANET** / MARCH 20173

CLOUD PLATFORMS HAVE A SINGLE CONSOLIDATED AGENT.

4 Securing Remote Workers

46% of organizations have operations in more than one country. Having remote workers can lead to inconsistent and out-of-date setups.[4]

CLOUD TREATS EVERY ENDPOINT THE SAME.

5 Slowing Down Endpoints

" [We were] trying to find a really comprehensive security solution without impacting the behavior of our endpoints and the usability of them. A lot of them tend to take up a lot of system resources."

– **TREVOR ALBRECHT**
TECHNICAL OPERATIONS ENGINEER / DRAFT KINGS

CLOUD PROCESSING KEEPS THE AGENT LIGHTWEIGHT.

6 Preventing New Attacks

60%

of security and IT personnel say their top challenge is finding new unknown threats for which their current security doesn't have signatures.[5]

CLOUD LEVERAGES BIG DATA AND SOPHISTICATED ANALYTICS TO PREDICT ATTACKS.

7 Identifying Problems

40% say they can improve visibility into network and endpoint behavior for quicker detection to prevent threats that have taken place on their endpoints.[6]

60% say determining the scope of a threat across multiple endpoints is difficult.[7]

CLOUD ANALYZES UNFILTERED ENDPOINT DATA TO GIVE YOU THE VISIBILITY YOU NEED.

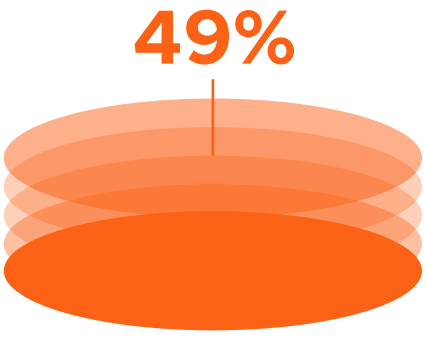
8 Responding Quickly to Threats

55% say it takes them three or more hours per endpoint to remediate, with most taking more than 24 hours.[8]

CLOUD ENABLES REAL-TIME INVESTIGATION AND REMEDIATION.

9 Getting the Help You Need

49%



say lack of staffing and a skills shortage are top inhibitors to effective response.[9]

CLOUD FACILITATES COLLABORATION AND EDUCATION.

10 Managing Infrastructure

" Between our traditional AV and all the other security tools my team has to manage, all the on-prem infrastructure becomes a nightmare—to maintain upgrades, to make sure you have enough storage and compute power."

– **RYAN MANNI**
SECURITY OPERATIONS MANAGER / HOLOGIC

CLOUD HAS NO INFRASTRUCTURE TO MANAGE.

www.CarbonBlack.com

87% Turning to the Cloud

of organizations report some of their SOC functions are handled in the cloud or plan to move them there in the next 24 months.[10]

1 **"The Show Must Go On!: The 2017 Incident Response Survey,"** June 2017, p.16, Table 3.
2 **"SANS 2016 Security Analytics Survey,"** December 2016, p. 1.
3 **"Endpoint Security: Preventing Threats on Devices Connected to Your Network,"**
4 **"Future SOC: SANS 2017 Security Operations Center Survey,"** May 2017, unpublished analysis
5 **"Exploits at the Endpoint: SANS 2016 Threat Landscape Survey,"** September 2016, p. 14, Figure 10.
6 **"2017 Threat Landscape Survey: Users on the Front Line,"** August 2017, p. 9, Figure 13.
7 **"Next-Gen Endpoint Risks and Protections: A SANS Survey,"** March 2017, p. 14, Figure 12.
8 **"Can We Say Next-Gen Yet?: State of Endpoint Security,"** p. 13, Figure 9.
9 **"The Show Must Go On!: The 2017 Incident Response Survey,"** p. 23, Table 4.
10 **"Future SOC: SANS 2017 Security Operations Center Survey,"** p. 4, Figure 3.