Interested in learning more about security?

SANS Institute InfoSec Reading Room

10 Endpoint Security Problems Solved by the Cloud

SANS surveys and testimonials from IT and security professionals indicate that endpoint security is a challenge. There is too much complexity and cost, defenses aren't keeping up, and security staff is stretched thin. This infographic explores how cloud can help address these issues.

10 Endpoint Security Problems Solved by the Cloud

Based on SANS surveys and testimonials from IT and security professionals, 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 2017[3]

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 Having remote workers can lead to inconsistent and out-of-date setups.[4]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.

Turning to the Cloud

87%

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]

SANS would like to thank its sponsor

Carbon Black.

[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.

SANS

Last Updated: July 16th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, GB	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Pen Test Berlin 2018	OnlineDE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced