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 Having remote workers can lead to inconsistent and out-of-date setups.[4]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: October 15th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Houston 2018	Houston, TXUS	Oct 29, 2018 - Nov 03, 2018	Live Event
SANS Gulf Region 2018	Dubai, AE	Nov 03, 2018 - Nov 15, 2018	Live Event
SANS Sydney 2018	Sydney, AU	Nov 05, 2018 - Nov 17, 2018	Live Event
SANS DFIRCON Miami 2018	Miami, FLUS	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS London November 2018	London, GB	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS Dallas Fall 2018	Dallas, TXUS	Nov 05, 2018 - Nov 10, 2018	Live Event
Pen Test HackFest Summit & Training 2018	Bethesda, MDUS	Nov 12, 2018 - Nov 19, 2018	Live Event
SANS Mumbai 2018	Mumbai, IN	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Rome 2018	Rome, IT	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Osaka 2018	Osaka, JP	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS San Diego Fall 2018	San Diego, CAUS	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS November Singapore 2018	Singapore, SG	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS ICS410 Perth 2018	Perth, AU	Nov 19, 2018 - Nov 23, 2018	Live Event
SANS Paris November 2018	Paris, FR	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS Stockholm 2018	Stockholm, SE	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS Austin 2018	Austin, TXUS	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS San Francisco Fall 2018	San Francisco, CAUS	Nov 26, 2018 - Dec 01, 2018	Live Event
European Security Awareness Summit 2018	London, GB	Nov 26, 2018 - Nov 29, 2018	Live Event
SANS Khobar 2018	Khobar, SA	Dec 01, 2018 - Dec 06, 2018	Live Event
SANS Dublin 2018	Dublin, IE	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Santa Monica 2018	Santa Monica, CAUS	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Nashville 2018	Nashville, TNUS	Dec 03, 2018 - Dec 08, 2018	Live Event
Tactical Detection & Data Analytics Summit & Training 2018	Scottsdale, AZUS	Dec 04, 2018 - Dec 11, 2018	Live Event
SANS Frankfurt 2018	Frankfurt, DE	Dec 10, 2018 - Dec 15, 2018	Live Event
SANS Cyber Defense Initiative 2018	Washington, DCUS	Dec 11, 2018 - Dec 18, 2018	Live Event
SANS Bangalore January 2019	Bangalore, IN	Jan 07, 2019 - Jan 19, 2019	Live Event
SANS Sonoma 2019	Santa Rosa, CAUS	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Amsterdam January 2019	Amsterdam, NL	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Threat Hunting London 2019	London, GB	Jan 14, 2019 - Jan 19, 2019	Live Event
Secure DevOps Summit & Training 2018	OnlineCOUS	Oct 22, 2018 - Oct 29, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced