Endpoints Everywhere

The rise in cloud-based endpoints not only challenges the standard remediation model, but introduces the need to secure those endpoints in a nontraditional setting.

42% of respondents report their endpoints have been breached, leaving 17% exposed to the latest endpoint breaches.

63% of respondents report remediation of a single endpoint takes an average of 24 hours or less.

Breaches and endpoint breaches involved 10–24 endpoints.

63% of attacks are detected by an antivirus.

49% of compromises were detected by automated SIEM alerts.

47% of organizations detected compromises only 10% of the time.

Key Findings

**Harden Your Endpoints**

Organizations must identify, install and configure effective solutions, as well as establish baseline readings. Top key success factors included:

45% ease of data collection

47% correlation of data into usable information

43% skilled operators

46% automation/tool interoperability

The latest SANS 2018 Survey on Endpoint Protection and Response offers key survey results and best practices to help you simplify and automate your endpoint protection, detection and response capabilities.

Successful Threat Vectors

The top threat vectors for exploited endpoints take advantage of the hapless user:

47% Web drive-by

32% Social engineer

32% Ransomware

Detection and Response

Aggressive threat actors are getting smarter, but not simpler.

47% of threats are detected by an antivirus.

32% of threats were detected by clouds.

32% of threats were detected by end-user defense.

It’s important that organizations detect threats more than 10% of the time.

Harden Your Endpoints

Organizations must identify and configure effective solutions, as well as establish baseline readings. The top key success factors included:

49% ease of data collection

47% correlation of data into usable information

46% skilled operators

43% automation/tool interoperability

The drive for anytime/anyplace/any device computing, including the growing use of employee-owned handhelds and smartphones, opens new windows of vulnerability, yet such devices are less frequently included in organizations’ management programs.

Many device types are connecting to networks: desktop computers, followed by employer-owned laptops, network devices and servers, mobile devices, even cloud-based systems, IoT devices, mobile and network devices, and wearables.