Cisco Leads Again in NSS Breach Detection Test

Cisco is a leader for the third year in a row in the 2016 NSS Labs Breach Detection Systems (BDS) test. Our solutions detected 100% of malware, exploits, and evasions and had the fastest time to detection.

Only Cisco has the breadth of technology to deliver an integrated security infrastructure that sees a threat once and blocks it everywhere. We draw on our unparalleled network presence, renowned global threat intelligence from Talos, and the industry's broadest and deepest security portfolio. Our architectural approach delivers solutions that are simple, open, and automated. They work together, seamlessly. In real time. We provide our customers with exceptional visibility and responsiveness so you can detect more threats and remediate them faster.

We also provide superior breach detection across **more platforms** than any other vendor. These include next-generation firewalls, next-generation IPS, unified threat management (UTM), switch and routing infrastructures, and email and web appliances. And we defend **more attack vectors**: network, data center, endpoint, mobile device, virtual machine, email, and the web. This integrated security architecture makes your networks harder to penetrate and, with automated responses, makes security simpler.

Get the latest report and learn how Cisco can help you stop more threats, faster.

Reducing Attackers' Time and Space to Operate

Defenders today must protect themselves against hackers who are increasingly sophisticated and professional. They understand the ever-expanding threat landscape and exploit any weakness they find. Ruthlessly. To undermine their impact, defenders must reduce the time and space those attackers have to operate. In our latest Midyear Cybersecurity Report, Cisco's time to detection (TTD) was found to be **13 hours**. The industry standard is about **100 hours or more**.

Cisco takes advantage of the fact that we see things more quickly and clearly than anyone else. We translate that visibility into intelligence that helps you stop more threats, faster. Our industry-leading threat intelligence team, Talos, blocks 19.7 billion threats a day, - more than 2.5 blocked threats a day for every person on earth. – and analyzes more data in more ways than anyone else. This threat intelligence produces a 360-degree view that is used across all Cisco security products for fast and effective security.

Figure 1. NSS Breach Detection Test Results for Cisco

Product				Breach Detection Rate		NSS-Tested Throughput	
Cisco Firepower 8120 with NGIPS v6.0 and Advanced Malware Protection				100.0%		1,000 Mbps	
False Positives	Drive-by Exploits	Social Exploits	HTTP Malware	SMTP Malware	Offline Infections	Evasions	Stability & Reliability
0.33%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	PASS

Cisco Leads Again in NSS Breach Detection Systems (BDS) Test

Figure 2. NSS Time to Detection Test Results

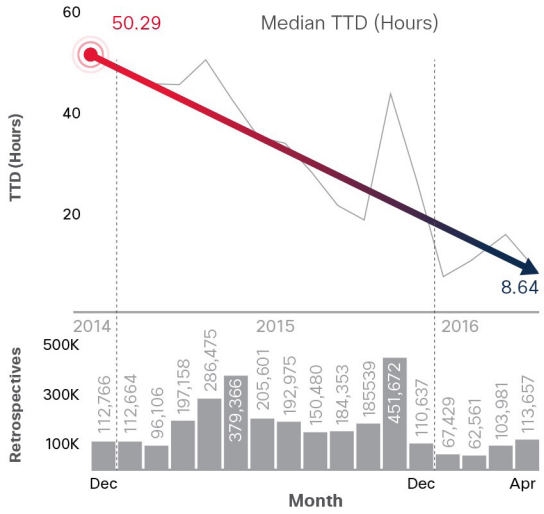
Detection Time Scoring									
Time to Detect	Product A	Cisco	Product B	Product C	Product D	Product E	Product F	Product G	Product H
<1min	44.40%	67.00%	0.60%	48.90%	46.20%	5.50%	7.30%	6.50%	3.60%
<3min	75.90%	91.80%	2.90%	88.70%	84.20%	31.30%	17.90%	17.10%	26.70%
<5min	86.60%	96.30%	6.50%	91.00%	88.40%	47.80%	27.60%	27.00%	66.20%
<10min	97.40%	96.60%	15.20%	95.60%	91.30%	85.00%	43.10%	42.50%	90.10%
<30min	97.90%	97.10%	85.80%	98.50%	93.10%	96.90%	76.40%	75.40%	94.00%
<60min	98.20%	97.90%	90.80%	98.70%	93.10%	98.20%	97.90%	89.20%	96.30%
<120min	98.50%	98.50%	90.80%	98.90%	94.30%	98.40%	98.50%	89.70%	96.60%
<240min	98.90%	99.20%	91.60%	99.00%	97.60%	98.90%	98.50%	89.70%	96.80%
<480min	99.00%	99.40%	95.80%	99.00%	98.70%	99.40%	98.90%	90.00%	99.70%
<720min	99.20%	99.70%	96.40%	99.40%	98.70%	99.50%	98.90%	90.10%	99.80%
<1080min	99.40%	99.80%	96.80%	99.40%	98.70%	99.80%	98.90%	90.10%	99.80%
<1440min	99.40%	100.00%	96.80%	99.40%	99.00%	100.00%	98.90%	90.10%	99.80%
Overall Detection Score	**99.40%**	**100.00%**	**96.80%**	**99.40%**	**99.00%**	**100.00%**	**98.90%**	**90.10%**	**99.80%**

= > 90%
= 80 - 89%
= 60 - 79%
= 40 - 59%
= < 40%

This chart shows the difference in effectiveness based on time to detection. Multiple products may end with same Overall Detection Score at the bottom. But the products with faster detection rates (that get to green numbers faster moving from top to bottom) are more effective because they give attackers less time and space in which to operate.

Figure 3. Cisco Midyear Cybersecurity Report Time to Detection

Source: Cisco Security Research



Read our blog and learn why time to detection may be an even better measure of effectiveness than a 100% detection rate.