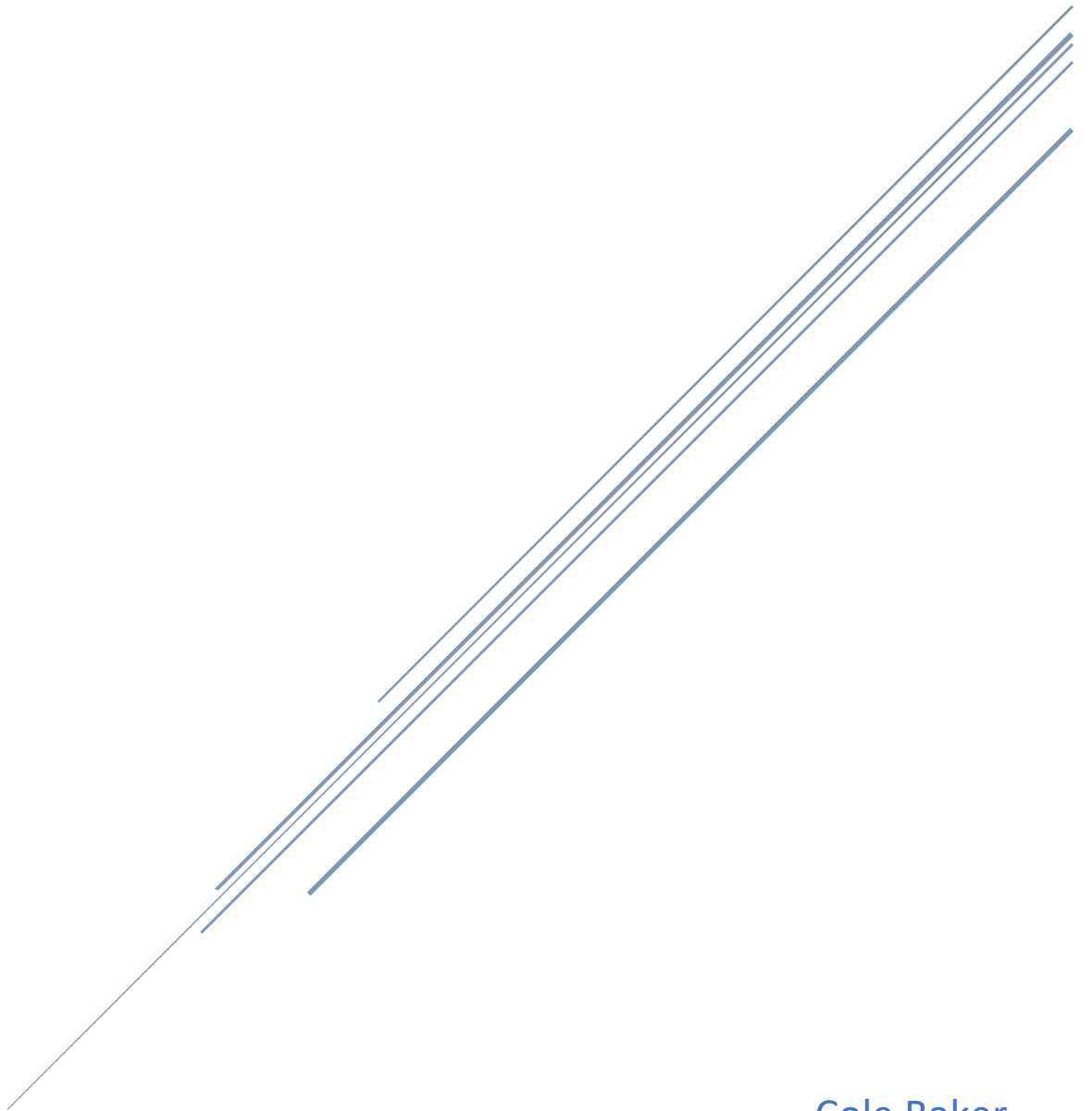


# COMPARING IPS SYSTEMS



Cole Baker

Table of Contents

Gartner Magic Quadrant Leaders ..... 2

    Cisco, Trend Micro, McAfee..... 2

    FireEye..... 2

References ..... 3

## Gartner Magic Quadrant Leaders

### Cisco, Trend Micro, McAfee

All three of the leader's intrusion detection systems have deep-packet inspection, bot and malware detection, inbound and outbound traffic monitoring systems, network attack monitors, SSL inspection, as well as many more features that they share.

However, McAfee has an advanced netflow analyser and ATD zero-day prevention system, which Trend Micro and Cisco doesn't have. Setting McAfee apart from the others, as well as its easy to deploy and has a high protection rate. Their netflow analyser works by using a 7 layers flow scanning system which monitors all of the network traffic at a deeper level than its competitors. (McAfee, n.d.) (Lippincott, 2018) (Cisco, n.d.) (Micro, n.d.) (Security, 2018) (Architect, 2018) (Lead, 2018)

### FireEye

FireEye which is a rising challenger in the Gartner Magic Quadrant. Their IPS share some of the same features that the leaders have, such as, deep-packet inspection, network traffic monitoring. What sets FireEye's IPS system apart from the leaders is that they use a method they call Multi-Vector Virtual Execution which reliably detects known and unknown threats, as well as reduces the number of false positives by up to 80%. (Grady, 2018)

## References

- Architect, S. (2018, December 27). *Advanced NG-IPS*. Retrieved from Gartner:  
<https://www.gartner.com/reviews/review/view/640471>
- Cisco. (n.d.). *Cisco IOS Intrusion Prevention System (IPS)*. Retrieved from Cisco:  
<https://www.cisco.com/c/en/us/products/security/ios-intrusion-prevention-system-ips/index.html>
- Grady, J. (2018). *Intrusion Prevention System*. Retrieved from FireEye:  
<https://www.fireeye.com/solutions/nx-network-security-products/intrusion-prevention-systems-ips.html>
- Lead, T. (2018, October 11). *Deep-Packet Inspection Feature That Detects And Prevents A Wide Range Of Network Attacks*. Retrieved from Gartner:  
<https://www.gartner.com/reviews/review/view/558891>
- Lippincott, E. (2018, January 17). *Trend Micro Named a Leader in 2018 Gartner Magic Quadrant for Intrusion Detection and Prevention Systems*. Retrieved from Trend Micro:  
<https://blog.trendmicro.com/trend-micro-named-leader-2018-gartner-magic-quadrant-intrusion-detection-prevention-systems-idps/>
- McAfee. (n.d.). *Data Sheet - IPS Platform*. Retrieved from McAfee:  
<https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-network-security-platform-series.pdf>
- Micro, T. (n.d.). *Intrusion Prevention*. Retrieved from Trend Micro:  
[https://www.trendmicro.com/en\\_ca/business/capabilities/intrusion-prevention.html](https://www.trendmicro.com/en_ca/business/capabilities/intrusion-prevention.html)
- Security, D. o. (2018, May 2). *Trend Micro TippingPoint NGIPS Review*. Retrieved from Gartner:  
<https://www.gartner.com/reviews/review/view/467734>