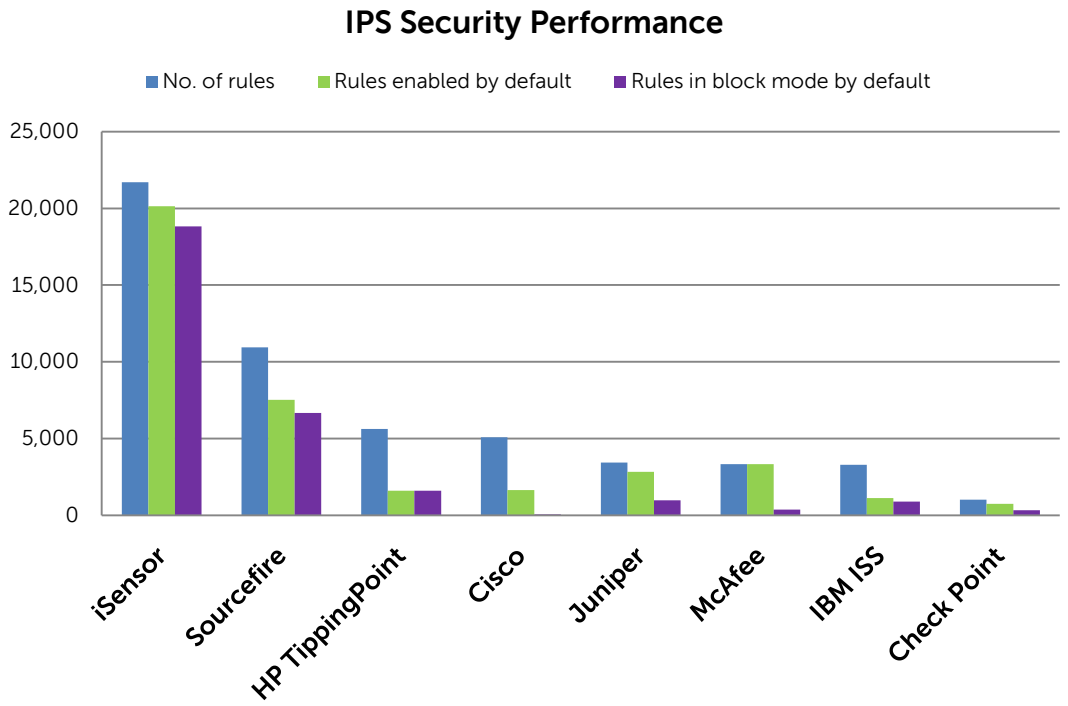
IPS Effectiveness

IPS with iSensor sees, identifies and blocks more malicious traffic than other IPS solutions

An Intrusion Prevention System (IPS) is a critical layer of defense that helps you protect your network from harmful traffic that has passed through or bypassed your firewall. It inspects Ethernet, IP and TCP layers which harbor attacks. Many IPS vendors differentiate their offerings with claims about high speed, low latency and maximum bandwidth supported. While packets processed per second is a valuable indicator of traffic volume and throughput, it is not a gauge for security effectiveness or the capacity to prevent cyber threats. The true measure of IPS security performance is the accuracy and effectiveness of identifying and blocking malicious traffic.

During a recent six-month period, Dell SecureWorks reviewed IPS security effectiveness across leading IPS devices we manage and monitor for customers. We collected live data in the real-time threat defense environment of our Security Operations Centers, which provides more accurate results than reports produced from synthetic data created in a controlled lab setting. Because we manage and monitor more Dell SecureWorks iSensor™ IPS devices, we normalized the findings specific to each vendor to produce a balanced view of each vendor's IPS security effectiveness. The results illustrated throughout this report verify that the Dell SecureWorks Intrusion Prevention Service with iSensor delivers better threat protection and significantly strengthens our customers' defensive posture.

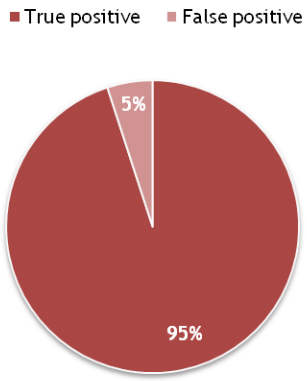


IPS with iSensor blocks harmful and malicious traffic with more high-fidelity rules enabled and set to block by default.

Effective intrusion prevention

IPS with iSensor delivers fast and effective attack protection by performing in-line deep packet inspection of inbound and outbound network traffic using multiple integrated defense technologies to protect critical assets from known and emerging attacks. With more than 20,000 unique rules developed by our Counter Threat Unit[SM] (CTU) security intelligence experts to counter real threats to our customers, IPS with iSensor outperforms leading IPS devices with:

- High-fidelity rules
- Periodic rule tuning and updates
- Real-time, intelligence-driven feedback loops
- Advanced analysis and blocking



95 percent of the events we escalate to customers are real security events that require attention.

High-fidelity rules

IPS devices pump out thousands of alerts daily, depending on how much traffic passes through your network. To prevent attacks and network compromise, rules are often written broadly and loosely. As a result, they tend to block and/or alert on legitimate business traffic. Rules must be written with high fidelity and enabled to block, not simply alert, in order to provide the best security.

Full context

The most effective high-fidelity rules are written to avoid false positives, and block attacks and policy violations without interrupting legitimate traffic. iSensor rules are written and managed based on the full context of vulnerabilities, exploits and malware behavior. This "big picture" approach helps minimize false positives, block attacks and policy violations without interrupting legitimate traffic, and mitigate damage if something malicious does enter your network.

Generally, IPS rules are written to block attacks against software vulnerabilities. These rules address root causes and protect against both current and future exploits.

Other rules are written specific to exploits. These rules produce fewer false positives but you need many of these rules to address the growing number and variations of exploits.

Rules can also be behavior based, to prevent data exfiltration and propagation. Creating these rules requires a deep understanding of how malware behaves following an infection. They provide additional visibility and help to block suspicious activity in outbound traffic. They also catch new vulnerabilities and exploits that have not yet been publicly disclosed.

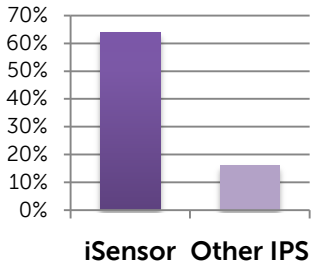
No single method of rule development is perfect. Effective threat prevention requires the big picture: rules based on vulnerabilities, exploits and malware behavior.

99.3 percent of iSensor rules are set to block and drop suspicious packets without interrupting traffic flow.

Block and drop

Identifying an attack without blocking it means your team will spend more time addressing the impact of a successful attack instead of reviewing reports enumerating the unsuccessful attacks. High-fidelity rules must block, not simply alert.

According to our research, only half the rules on leading IPS devices are enabled to block attacks; instead, they simply generate alerts while letting suspicious traffic pass through. On average, IPS with iSensor blocks four times more potentially malicious traffic than other IPS devices.



On average, IPS with iSensor blocks four times more potentially malicious traffic.

IPS with iSensor is configured and continually tuned by security experts to provide effective protection.

Rule tuning and updates

Rules for your business must be optimized, updated and measured for effectiveness. With other IPS deployments, tuning can be time-consuming and complicated. IPS with iSensor, however, is configured and continually tuned by security experts to provide effective protection.

Continual tuning and updates are imperative to ensure you are blocking the correct traffic as well as looking for the latest threats. According to industry surveys, only about 60 percent of rule updates are applied. Without the latest rule updates applied, IPS devices function at partial capacity and protection.

IPS with iSensor customers have the most up-to-date protection with:

- Daily audits of existing rule fidelity
- Rule updates deployed twice weekly
- Service Level Agreement (SLA) that guarantees protection against new, critical threats within 48 hours

99.9 percent of IPS with iSensor rule updates are deployed automatically, without customer impact or business interruption.

Our audit process enables us to continually fine-tune rules and ensure customers are protected with the latest countermeasures. Ultimately, our continual rule management and administration provides customer-specific protection with lower false positives and false negatives than other IPS devices.

Real-time, intelligence-driven feedback loop

Real-time intelligence and expert analysis underlie the accuracy and effectiveness of iSensor rules.

Dell SecureWorks is the only IPS provider that develops, fine-tunes and deploys rules based on a live feedback loop which we leverage across all our customers. The iSensor provides a live feed of information to our security experts, who monitor attacks and identify suspicious activity and emerging threats 24x7. As a result, in real-time we create and modify countermeasures quickly and effectively.

GIAC GCIA certified security analysts in our integrated Security Operations Centers work closely with our CTU security research group, sharing information about anomalous activity and threat intelligence 24x7x365. This tight integration provides an early warning system and comprehensive context in which to analyze emerging threats and vulnerabilities. It also enables rapid deployment of finely tuned rules and defenses to protect our customers against the latest threats.

We leverage intelligence and protections across our customer base. When we detect an incident impacting one of our customers, we identify the threat and notify the customer. Simultaneously, we use that information to protect our entire customer base from similar threats. We then build what we have learned into our technology to make it even more effective. This creates a continuously improving technology that adapts with the changing security landscape.

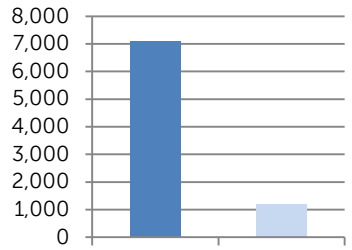
Rule updates from other leading IPS device vendors are less effective because they are not based on live transmission of activity occurring in your environment. At best, they are 24-hour delayed responses to malicious activity which may have already compromised your network.

Advanced analysis and blocking

IPS with iSensor provides real-time inspection of inbound and outbound network traffic using multiple, integrated defense technologies, including:

- Advanced statistical analysis
- Suspicious activity correlation
- Expert security analysis of patterns

IPS with iSensor protects our customers better by catching a wider array of attacks using high-fidelity IPS rules. On average, iSensor IPS identifies nearly six times the number of distinct attacks as other IPS solutions.



IPS with iSensor identifies nearly six times as many distinct attack types.

Advanced statistical analytics

We investigate, analyze and categorize significant events by criticality of risk, using advanced technologies and algorithms to mine and process IPS alerts across our entire customer base.

Suspicious activity correlation & expert security analysis

We filter, correlate and analyze billions of security events across our customers each and every day. We condense these events into meaningful security information that enables our expert security analysts to accurately assess risk in full context, in real time. Using advanced correlation and analysis techniques, we filter event noise down to positive and anomaly security events which our certified security analysts investigate and analyze further.

Advanced protection

We see attacks sooner and protect our customers faster and more effectively. On average, we analyze billions of security events across our customer base every day and analyze information from thousands of sources worldwide. We leverage that information to discover new attack techniques, vulnerabilities and threats as they emerge, and develop preventative countermeasures to protect our customers before damage occurs. We routinely uncover threats and provide timely countermeasures with the information collected across our customer base, as well as insight from the visibility and information exchange across many elite threat research circles, including:

- Anti-Phishing Working Group (APWG)
- CyberCop Network Network
- Cyber Security Forum Initiative (CSFI)
- Federal Trade Commission (FTC)
- Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Forum of Incident Response & Security Teams (FIRST)
- Infragard
- Internet Security Alliance (ISA)
- Internet Systems Consortium (ISC)
- Microsoft Active Protections Program (MAPP)
- National Cyber-Forensics & Training Alliance (NCFTA)
- North Atlantic Treaty Organization (NATO)
- SANS Institute
- Secret Service Electronic Crimes Task Force (USSS ECTF)
- U.S. Department of Defense
- U.S. Department of Energy
- Zero Day Initiative (ZDI)

As a Microsoft Advanced Protections Program partner, we are able to release defenses for vulnerabilities at the same time they are publicly disclosed. We receive vulnerability information from Microsoft in advance of its monthly and ad hoc security update releases. This allows us to analyze vulnerabilities that might impact our customers earlier. In turn, we develop and deploy countermeasures to protect our customers faster and sooner.

About Dell SecureWorks

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.