CONTINUOUS MONITORING OF ENDPOINTS: MYTHS AND REALITIES
“CONTINUOUS MONITORING”: UNDERSTAND THE OPTIONS

Continuous monitoring has been a popular topic in the IT community since the publication of two NIST (National Institute of Standards and Technology) reports in 2010 and 2011. But even cybersecurity experts sometimes fail to distinguish between two different styles of continuous monitoring. One of these is based on perpetual scanning, and the other is based on scanning performed at appropriate intervals.

In this document we review the differences between the two styles of continuous monitoring, and describe the strengths and weaknesses of each for endpoint security.

HOW THE EXPERTS DEFINE CONTINUOUS MONITORING

The website CIO.gov provides a concise definition of continuous monitoring:

Continuous monitoring is a risk management approach to cybersecurity that maintains an accurate picture of an agency’s security risk posture, provides visibility into assets, and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls, and implement prioritized remedies.²

NIST Special Publication 180-137 provides a similar definition, and adds an important clarification in a footnote:

“Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities and threats to support organizational risk management decisions. *The terms “continuous” and “ongoing” in this context mean that security controls and organizational risk are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organizational information. Data collection, no matter how frequent, is performed at discrete intervals.”³

It is clear from the definitions that these experts are not recommending perpetual scanning and reporting, but rather data collection performed at appropriate discrete intervals (i.e., frequently enough to maintain ongoing awareness).

In this paper we will call the two styles of continuous monitoring “always-on monitoring” and “real-time monitoring.” “Always-on monitoring” means that a data source (a network packet flow, a security device log, an endpoint) is being scanned without any pause. “Real-time monitoring” means that data is scanned at intervals using an automated tool. (Figure 1) Both contrast with “point-in-time” assessment, where scanning is only done in conjunction with a specific event such as an audit, a certification initiative, or a hunt for a newly identified attack.

---

2 CIO.gov, definition of continuous monitoring.
3 NIST SP-800-137, page 1.
Continuous Monitoring of Endpoints: Myths and Realities

THE BEST APPROACH DEPENDS ON THE DOMAIN

But which of these styles or continuous monitoring is best? The answer depends on the security domain.

There are some areas of cybersecurity where always-on monitoring is preferable. An intrusion prevention system (IPS) should scan all incoming traffic, because that is the only way to detect many network-based attacks. Data loss prevention (DLP) solutions need to inspect all outgoing traffic, because you don’t want to allow hackers to exfiltrate even one social security number or account number from your network.

But real-time monitoring is better in other cybersecurity domains. Setting antivirus programs to perpetually scan employees’ laptops would significantly degrade performance and anger users; scanning hard drives daily or weekly is usually sufficient. Endlessly scanning access control lists for compliance with corporate rules would be a waste of resources; weekly or even monthly testing is appropriate in that field.

In a given cybersecurity domain, the considerations for selecting the optimal approach include:

1. How big is the performance penalty of always-on monitoring?
2. How much advantage is conferred by updating security data constantly versus at longer intervals?
3. Which approach provides the most useful and complete information?
4. Which approach is more scalable?

THE CASE OF ENDPOINT SECURITY

Endpoint security is a critical area for IT groups today because most of the multi-million dollar cyberattacks in recent years have involved compromised endpoints. Endpoint monitoring can reveal indicators of compromise (IoCs) such as file signatures of malware, abnormal executing processes, registry key settings associated with known cyberattacks, and many other suspicious events and artifacts.
This data allows network and security administrators and analysts to:

- Detect advanced threats sooner
- Analyze cyber attacks, perform root cause analysis, and conduct forensic investigations

In fact, in many situations the *only* way to detect and understand advanced attacks is by collecting and analyzing IoCs on endpoints.

But how do the conditions of endpoint security affect the choice between always-on monitoring and real-time monitoring of endpoints, and which is the right approach for you?

**CONSIDERATION #1: PERFORMANCE PENALTY**

Always-on monitoring consumes significant resources on each endpoint. CPU capacity and memory are needed to read logs and scan for information related to open files, file systems, running processes, registry keys, network connections, installed software, and other system and application details. A single endpoint can contain 20,000 or more data points.

Also, always-on monitoring creates very high levels of network traffic by sending constant streams of data to central analysis locations.

This large “footprint” is likely to be an issue in organizations where:

- Endpoints include low-end systems that slow down because of the extra load of perpetual scanning
- Network capacity is limited, and extra network traffic affects application performance during peak periods
- Users have high expectations about reliable performance

**CONSIDERATION #2: TIME ADVANTAGE**

Always-on monitoring products scan perpetually, which by definition gives them a time advantage over real-time monitoring solutions, which typically collect data at intervals that range from once every few minutes to once a day.

However, the value of the time advantage depends on questions such as:

- The resources available to correlate and analyze endpoint data.
- How quickly it is necessary to react to threats.

---

4 As noted in the NIST SP 800-137 footnote cited above, *all* data collection is performed at discrete intervals. Always-on monitoring tools on endpoints don’t monitor every file, every process and every registry key at every instant. However, the scanning *process* is perpetually running.
Endpoint data almost always needs to be correlated to provide actionable results. With a few exceptions, a single IOC indicates only some probability of attack, and most IOCs are “false positives.” It is not until multiple related IOCs are found on the same systems, or across systems, that the presence of an attack can be validated. Most enterprises are so flooded with threat data that, even with a staff of dedicated analysts and incident responders, it takes several hours (or longer) to comb through alerts and correlate IOCs.

In effect, the value of more frequent data collection depends on the staff the organization has available to analyze the data. If the average alert sits in a queue for 12 hours before being analyzed, there isn’t much advantage in collecting data every minute, or even every hour.

The time available to react depends on the type of threat. Some low-level attacks can do damage within minutes. However, the most advanced attacks typically linger on the network for days, weeks or months. For example, the $81 million assault on the central Bank of Bangladesh and the SWIFT financial network in February 2016 evolved over weeks as the attackers used a sophisticated Trojan to gain a foothold on the bank’s network, then explored the network, acquired credentials, compromised multiple systems, and monitored messages from the SWIFT network in preparation for their attack. In scenarios of this type, completeness of information (discussed below) is far more important than minutes or hours of time advantage.

Based on these parameters, the time advantage of always-on monitoring is a bigger factor when:

- A large staff is available to comb through large volumes of alerts and correlate endpoint data
- The organization is most concerned with threats that do significant damage within minutes or hours, as opposed to advanced persistent threats that evolve over days, weeks, or months

CONSIDERATION #3: COMPLETENESS OF INFORMATION

In theory, always-on monitoring tools and automated real-time monitoring tools might both collect the same information. In practice, however, always-on monitoring products typically collect fewer types of endpoint information, in order to prevent them from overwhelming networks with their traffic.

Examples of endpoint data collected by real-time monitoring tools but often not compiled by always-on monitoring products include:

- Command and control artifacts, such as evidence of remote sessions, signs of unusual network communications between machines, and information in index.dat files about recent web site visits.
- Open file metadata
- Deleted browser histories
- Windows registry artifacts

---

5 According to the Verizon 2016 Data Breach Investigations Report (DIBR), in 68% of breaches, data exfiltration took days, weeks or longer (as opposed to seconds, minutes or hours). For information on the attack on the Bangladesh Bank see: Bangladesh Bank Attackers Hacked SWIFT Software.
A complete data footprint on endpoints, collected at the kernel level, is essential for detecting and analyzing advanced attacks. It is particularly important to have comprehensive set of artifacts related to command and control activities, since these provide the best evidence (and sometimes the only definitive evidence) of multistage attacks where the threat actor explores the network, compromises systems, and stages data for exfiltration.

Complete information is an especially critical consideration when organizations have stringent regulatory and legal requirements, are subject to breach notification laws, or want detailed forensic analysis to understand the tactics, techniques and procedures (TTPs) of attackers.

**CONSIDERATION #4: DATA FOR TIMELINE ANALYSIS**

Most always-on monitoring products collect massive volumes of log data. The huge quantity of mostly irrelevant information makes it difficult for analysts to find the key data points needed to construct a timeline of an attacker’s activities.

Also, because of the volume of data, many always-on monitoring products limit the amount of information that can be stored and analyzed, sometimes to 30 days or less. This is a serious problem for analysts if the endpoints were compromised weeks or months before the investigation.

Finally, many always-on monitoring tools only provide access to activities that occurred after they were installed on the endpoint.

In contrast, some real-time monitoring tools are able to provide detailed visibility into malicious activities on endpoints without collecting huge volumes of log data. They do this by taking advantage of how operating systems function to find forensic artifacts and traces left behind by attackers. Because of this they:

- Collect less redundant and irrelevant data, enabling analysts to find key data points faster
- Store years of data, allowing analysts to create attack timelines that go back to the first probes.
- Can provide insight into events and activities on endpoints where no monitoring tool was installed at the time of compromise.

These differences make real-time monitoring solutions a better option for enterprises that need timeline analysis and in-depth forensics. They also make real-time monitoring the clear choice for security groups that need to perform post-incident forensic investigations on endpoints where an endpoint monitoring tool was not previously installed.

**CONSIDERATION #5: DATA PRIVACY**

Some always-on monitoring products do not allow enterprises to be selective about the data that is collected and sent to the central management system. This can cause them to inadvertently capture personally identifiable information that should not be accessible to administrators, and to violate national data privacy laws by sending protected information across borders. Most real-time monitoring systems avoid these issues because they provide granular control over what data is collected and transmitted.
CONSIDERATION #6: SCALABILITY

As enterprises grow and add more endpoints, monitoring solutions that involve frequent polling and generate large volumes of data traffic can create network bottlenecks and slow application performance. This often makes some always-on monitoring products less scalable than real-time monitoring products. Organizations with large number of endpoints or rapid growth should pay particular attention to this issue, and should consider measuring network traffic and modeling the impact of deploying the tools on more endpoints.

THE HYBRID OPTION

Of course, organizations are not restricted to only one style of continuous monitoring. In some circumstances it makes sense to use always-on monitoring with critical high-volume endpoints like transaction servers and file servers, while using a real-time monitoring tool for the vast majority of other systems. This hybrid approach can help enterprises detect threats faster on key endpoints, without overwhelming the network and the incident response staff.

NEXT STEPS

The primary considerations for deciding between always-on monitoring and real-time monitoring solutions in the endpoint security domain are summarized in Table 1.

<table>
<thead>
<tr>
<th>CONSIDERATION</th>
<th>ALWAYS-ON MONITORING</th>
<th>REAL-TIME MONITORING</th>
<th>FACTORS AFFECTING PERFORMANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERFORMANCE</td>
<td></td>
<td>✓ ADVANTAGE</td>
<td>Real-time monitoring better if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Endpoints include low-end systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Network bottlenecks affect performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Users expect consistent performance</td>
</tr>
<tr>
<td>TIME</td>
<td>✓ ADVANTAGE</td>
<td></td>
<td>Always-on monitoring better if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Endpoint data is analyzed frequently</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The organization is most concerned with threats that do damage in minutes or hours</td>
</tr>
<tr>
<td>COMPLETENESS OF INFORMATION</td>
<td>✓ ADVANTAGE</td>
<td></td>
<td>Real-time monitoring better if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• In-depth forensic analyses are needed</td>
</tr>
<tr>
<td>TIMELINE ANALYSIS</td>
<td>✓ ADVANTAGE</td>
<td></td>
<td>Real-time monitoring better if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Timeline analyses are important</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Need for forensic study of endpoints where monitoring tool was not installed</td>
</tr>
<tr>
<td>DATA PRIVACY</td>
<td>✓ ADVANTAGE</td>
<td></td>
<td>Real-time monitoring better if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Compliance with HIPAA, FSMA and national privacy laws is important</td>
</tr>
<tr>
<td>SCALABILITY</td>
<td>✓ ADVANTAGE</td>
<td></td>
<td>Real-time monitoring better if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Large or growing number of endpoints</td>
</tr>
</tbody>
</table>

Table 1: Considerations for evaluating endpoint monitoring solutions
Organizations considering endpoint security solutions should assess their environments to weigh the relative importance of these considerations. For example, organizations with the staff resources to analyze endpoint data frequently will benefit from the time advantage of always-on monitoring. On the other hand, organizations will be drawn towards solutions with real-time monitoring if they are concerned about the impact of poor network performance, and if they want more complete information for forensics and timeline analysis.

Organizations should validate their assessments with trials of the tools or with reference calls to other enterprises using the solutions. These exercises not only serve to verify the claims of vendors, they also uncover new ways to use endpoint data to identify and analyze threats.

About GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known—so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.

For more information about Guidance Software, please visit guidancesoftware.com, email us at experts@guid.com, or call us at (866) 229-9199.

About CyberEdge Group

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our expert consultants give our clients the edge they need to increase revenue, defeat the competition, and shorten sales cycles.

CyberEdge Group, LLC
1997 Annapolis Exhange Pkwy
Suite 300
Annapolis, MD 21401
800.327.8711
info@cyber-edge.com
www.cyber-edge.com

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of CyberEdge Group, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice.