SPECIAL REPORT

REDUCE RISK WITH REAL-TIME INTERACTIVE REMEDIATION OF NETWORK TRAFFIC

Many areas of business operations need to move from reacting to situations that have happened in the past, to identifying changes as they happen and take proactive actions in real time. The ability to make decisions in real time can help in many application and operational areas ranging from cybersecurity to fraud detection, network performance, DevOps, and more.

To accomplish the task of real-time decisioning requires visibility into events as they happen and the capability to enact changes on network data in real time based on the intelligence gained from live network data.

To accomplish the task of real-time decisioning requires visibility into events as they happen and the capability to enact changes on network data in real time based on the intelligence gained from live network data. With such capabilities, many operational areas would be able to identify problems in the making, while they are happening, and prevent or mitigate those problems before they have a significant impact on the business.

Who wouldn't want to shut off the latest malware attack—in real time? By monitoring and processing network traffic at layers 2-7 in real time, a wide variety of problematic network traffic and threats—operational and security—can be identified and remediated, while they are transiting the network, before they have a chance to do damage. In other words, the intent of malicious payloads on your network is revealed as soon as they infiltrate the network.

This may sound similar to other concepts (such as the Mitre ATT&CK framework and OODA loop), whereby real-time decisioning and analytics are used to observe and analyze live data, then to take action in real time.

Challenges Achieving Real-Time Decisioning

The problem is, most decision-making systems today are based on examining static data at rest. A network manager, security administrator, or a financial planner typically looks at logs, or trends gleaned from analysis of historical records to act on after something has already happened (for example, degradation of network performance, delivery of malware, exfiltration of company IP, or change in market conditions).

The recognition of the value of rapid decisioning and the relationship between the time it takes to act and the resulting degradation, damage, or financial loss is generally understood and has been quantified in business literature for many years (see Figure 1, below).

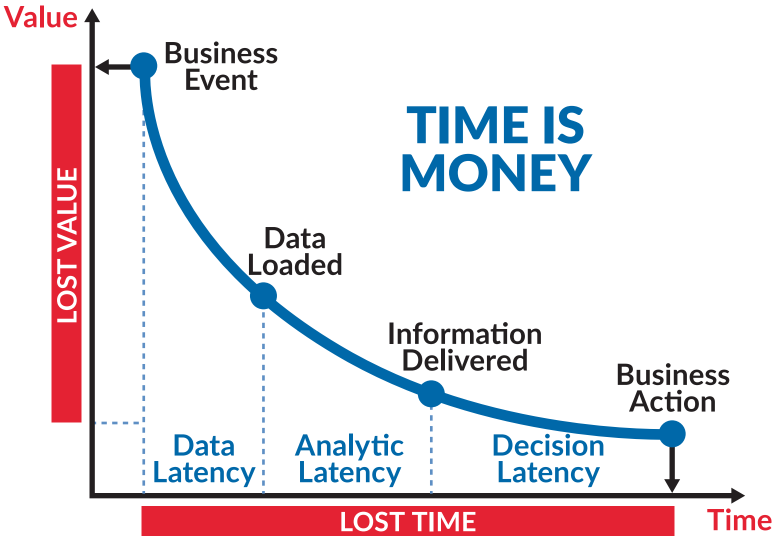


Figure 1
Source: Richard Hackathorn, DM Review, January 2004

You may be thinking, don't we already make decisions and take action on real-time network data today? Doesn't one of our tools already do this? You most likely have teams that use a variety of solutions (analytics, NPMD, IDS/IPS, SIEM, EDR, etc.) that rely on some sort of analysis of recent data. But are your teams able to access—and process—the most accurate intelligence they need to make decisions *in real time*?

Until recently, there has been no practical way to detect and react to events, anomalies, or attacks in near-real time. Instead, organizations have had to rely exclusively on previously stored data (in the form of logs, packet captures, EDR files, and other file-based data at rest) to make decisions. Regardless of the speed or throughput of those systems, the exposure to losses from this approach continues to worsen as the resulting damages from degradations or failures are now spread at near machine speeds (ref. Petya). Compounding matters, the bad actors are using increasingly sophisticated technical means to mask their activities and to prosecute their goals (ref. Methbot).

Therefore, the problem with relying solely on data at rest is that organizations cannot meet the demand to continuously monitor, identify, and mitigate issues in real time. To be proactive and take actions as events are happening requires information that is contained in data in motion, which is the stream of data moving through a network.

The problem with relying solely on data at rest is that organizations cannot meet the demand to continuously monitor, identify, and mitigate issues in real time.

This is easier said than done. To put the issue into perspective and understand the consequences, consider that the volume of data that must be examined is exploding. The annual data creation rate is expected to grow at a 29 percent CAGR through 2025.[i]

Organizations are overwhelmed by this data explosion—so much so that it can take weeks or months to identify problems after an incident occurs. That applies to network problems, abrupt financial market changes, and security breaches. For example, the mean time to identify a security breach is now 190 days, and the mean time to contain a breach after that is 57 days.[ii] The financial burden is huge: Globally, the average cost of a data breach is now $3.86 million.[iii]

Analyzing data in motion can dramatically change the picture. But extracting information from data in motion can be extremely difficult because of the quantity of data involved and the speed at which that data travels through a network. The issue is only going to get worse as more data is created in real time (nearly 30 percent of that data will be created in real time by 2025[iv]), and new networking technology, such as 400G Ethernet, is deployed. That will result in more data traveling through a network at faster data rates.

Existing approaches to deriving actionable information from data in motion often lack the capabilities and performance to be effective.

What organizations need today is the ability to detect and act on network threats and performance problems in *real time*. This concept is called *interactive remediation*.

A New Approach: Interactive Remediation

What organizations need today is the ability to detect and act on network threats and performance problems in *real time*. This concept is called *interactive remediation*. Interactive remediation hinges on the ability to create a closed-loop, dynamic exchange of real-time information between network traffic and analytic solutions.

A technology solution developed by MantisNet appears to accomplish this goal by allowing users to make continuous decisions based on wire-speed information and act immediately to isolate or remove malicious traffic or threats from the network.

Now, continuous, real-time remediation can be accomplished both on physical networks and in cloud/virtual instantiations. Leveraging advancements in software and processing capabilities, MantisNet is enabling true interactive remediation.

Business Benefits of Interactive Remediation

Using continuous, real-time monitoring and interactive remediation can enable organizations to make better, faster decisions that result in significant business and operational benefits.

For example, if real-time monitoring and advanced analytics solutions were used in security systems such as a next-gen firewalls to prevent a breach in the making, a company avoids the cost of the breach (which was noted above to be, on average, $3.86 million). Additionally, the company avoids the reputational damage, regulatory fines, and the cost of providing years-worth of credit monitoring services to the impacted users.

Some of these application areas are just beginning to emerge and are expected to grow rapidly in the near future. For example, the network automation market is estimated to grow from $3.7 billion in 2018 to $16.9 billion in 2022. Similarly, the market for IT operations and analysis tools is expected to grow from $5.4 billion in 2018 to $19.8 billion in 2022.

Incorporating continuous real-time monitoring and interactive remediation would provide enhanced capabilities to organizations that are simply not available today.

For example, organizations could:

- Reduce exposure to the costs of data breaches when used in cybersecurity applications.
- Improve authentication and stop fraud before it happens, preventing financial loss when used in fraud protection applications.
- Eliminate performance problems and outages, to keep the end-user experience, efficiency, utilization, and worker productivity high when used in network performance and monitoring applications.

Solutions that can continuously extract intelligence from data in motion and then use that information to take immediate actions are critical to any industry or market that depends on the reliability, availability, performance, and security of their networks.

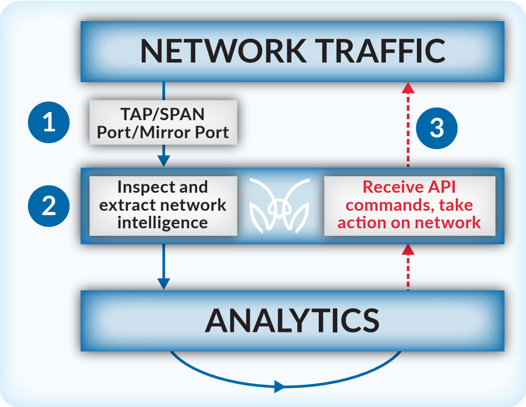
Solutions that can continuously extract intelligence from data in motion and then use that information to take immediate actions are critical to any industry or market that depends on the reliability, availability, performance, and security of their networks. These solutions enable organizations to improve situational awareness to better monitor, analyze, manage and protect their networks, enabling a more secure, reliable, scalable, and agile infrastructure.

The Three-Step Process of Interactive Remediation

Network operations and cybersecurity teams now have a method to enact changes in real time to live network data and remediate cybersecurity and performance issues as they happen.

The three-step process of interactive remediation as enabled by the MantisNet solution is (see Figure 2):

1. **Gain continuous visibility into network traffic for real-time processing.** Simply connect a network TAP, SPAN, or mirror port to replicate live network traffic into MantisNet solutions to inspect, filter, and process the traffic transiting on your network.
2. **Establish an access and enforcement control point to create a two-way, dynamic, and closed-loop process to analyze network traffic and take action in real time.** Using MantisNet solutions as your control and enforcement point, you can continuously monitor the data plane and filter traffic, to feed streaming analytics workflows or event-driven analytic tools, to further inspect and analyze the network traffic using real-time analytic processing.
3. **Take action on the network data based on real-time analysis.** Using machine-to-machine controls (RESTful APIs), the MantisNet access and enforcement control point receives instructions from the real-time analytic system to make real-time changes in the data plane to effect the desired actions. This closes the loop, providing the ability for the analytic processes to directly instruct the (MantisNet) control point to apply the desired action to specific network traffic flows via RESTful machine-to-machine controls (APIs).


NETWORK TRAFFIC
1
TAP/SPAN Port/Mirror Port
3
2
Inspect and extract network intelligence
Receive API commands, take action on network
ANALYTICS

1 Gain visibility into network traffic by using a TAP, SPAN, or mirror port

2 Establish a dynamic, two-way interface between the network and analytics. This is the control point for interactive remediation.

3 Remediate threats/take action on the network based on API commands from the analytic layer

Figure 2 MantisNet Interactive Remediation Three-Step Process
Source: MantisNet, 2019

For a more detailed technical explanation of the interactive remediation process, get the MantisNet guide, entitled "How to Implement Interactive Remediation."

Use Cases and Application Areas

Using interactive remediation, users can now make continuous, real-time decisions based on wire-speed information, and act immediately to remove threats from the network.

Using interactive remediation, users can now make continuous, real-time decisions based on wire-speed information, and act immediately to remove threats from the network.

The process harnesses the power of data in motion by programmatically extracting real-time metadata and putting it into standard, serialized formats. This intelligence can then be used as the fuel for powerful, open, machine-to-machine controls to dynamically monitor and manipulate the traffic of interest.

Deriving the metadata in real time from data in motion is the key element here. Streaming metadata is the fuel to power today's generation of cognitive and analytic decision processes and compute engines.

A few examples of interactive remediation in action will demonstrate the power of the approach.

Use case: Identifying suspicious DNS traffic in real time

With billions of websites on the Internet, separating the good from the bad is nearly impossible. However, by combining specific tools with streaming analytics, staff can better secure and harden a network into a real-time, dynamic, cybersecurity system that identifies potential attacks and blocks them during initial DNS exchanges—effectively stopping security breaches before they have the potential to reach users.

This technique takes enterprise web filtering a step further from standard cybersecurity systems software (IDS/IPS, NGFW, NGPB and SIEM). It also supports far more scalability and broader integration, with multiple analyst tools to better identify malicious sites on the fly, rather than leaving network security exposed to outdated databases or questionable data sources.

Use case: Account takeover (ATO) defense via SSL inspection

With automated credential stealing and account takeover tools, an attacker can send armies of bots to steal valuable information from thousands of victims and make hundreds of thousands of financial transactions. Where cyber criminals previously bought credentials and account information on the black market, they are now more likely to use sophisticated forms of exfiltration malware to automate the credential-stealing process to get access to vast amounts of even more valuable information. These tools give attackers the ability to collect and exploit thousands of stolen credentials using secure (encrypted) communication channels within a short amount of time.

To most effectively stop these attacks requires actionable real-time intelligence that can only be obtained from network data in motion. MantisNet solutions can be configured to monitor network traffic and initialization protocols continuously, as well as log-in attempts, to detect attacks in real time, as they occur. The MantisNet solution detects, identifies, and allows a company to stop credential/account takeover attacks in real time by detecting and identifying the unique "fingerprint" of the operations performed by the malware in the initial handshake exchange between the victim's system and the attacker's command and control server in real time, before stolen information can be exfiltrated in encrypted form.

Potential applications

There are many operational, security, and fraud detection applications for real-time decisioning and interactive remediation, including:

- Cybersecurity
- Fraud detection
- Authentication
- Data governance
- Compliance
- Event-driven architectures
- IDS/IPS, next-generation firewalls
- Network traffic analysis
- Next-generation packet brokers
- IoT gateways

For a more technical explanation of these use cases, see MantisNet's "How to Implement Interactive Remediation" guide.

At the Brink of Adopting Real-Time Decisioning for Interactive Remediation

The benefits of utilizing real-time, continuous network intelligence and advanced decisioning is compelling for any organization in any industry. In addition to the use cases cited above, real-time data-plane engineering and advanced decisioning can also be applied to NetFlow generation, load balancing, application delivery control, threat detection, authentication, and fraud identification applications.

Organizations have a decision to make—try to keep up using existing tools and technologies, or alter processes to better manage the growth and speed of data and adopt a real-time decisioning approach.

As stated earlier, the size and speed at which data is being created and traverses networks will only continue to increase. Without fundamentally changing how network data is inspected, analyzed, and managed, the inevitable result will be that network data will overwhelm already overtaxed resources and analysts' time, resulting in unacceptably long decision timeframes and the inability to effectively remediate operational and security issues. Organizations have a decision to make—try to keep up using existing tools and technologies, or alter processes to better manage the growth and speed of data and adopt a real-time decisioning approach.

Adopting solutions for real-time decisioning with interactive remediation is less invasive than you might think. The technology (for on-premises, virtualized, hybrid, or cloud-based environments) can be easily integrated into your current technology stack, business processes, and analytics, and the outcomes can greatly benefit your operational effectiveness and cyber-risk resilience.

For more information, to get our technical guide to implementing interactive remediation, and to evaluate a trial for real-time decisioning, visit https://www.mantisnet.com/start-your-trial.

i. "IDC: Expect 175 zettabytes of data worldwide by 2025," NetworkWorld, December 3, 2018

ii. 2018 Cost of a Data Breach Study, Ponemon Institute

iii. Ibid

iv. "By 2025, nearly 30 percent of data generated will be real-time, IDC says," ZDNet, November 27, 2018

v. "Network Automation Market worth 16.89 Billion USD by 2022," MarketsandMarkets Research

vi. "The IT operations market is projected to grow to USD 19.84 billion by 2022," PR Newswire, April 24, 2017

RTInsights is an independent, expert-driven web resource for senior business and IT enterprise professionals in vertical industries. We help our readers understand how they can transform their businesses to higher-value outcomes and new business models with IoT real-time analytics. We provide clarity and direction amid the often confusing array of approaches and vendor solutions. We provide our partners with a unique combination of services and deep domain expertise to improve their product marketing, lead generation, and thought leadership activity.

MantisNet develops Software Defined Network (SDN) and Network Function Virtualization (NFV) network solutions that transforms network traffic into an invaluable source of real-time intelligence. MantisNet enables real-time end-to-end visibility and control through data plane engineering, network monitoring, protocol analysis (from L2 to L7) and provides the capability for real-time interactive remediation of anomalies, threats, fraud, and malicious activities. MantisNet's solutions enable organizations to better monitor and control network traffic compared to traditional packet brokers, firewalls, event management and traffic engineering solutions.

MantisNet's real-time network intelligence, monitoring and remediation solutions can be found at MantisNet.com.

The information contained in this publication has been obtained from sources believed to be reliable. NACG LLC and RTInsights disclaim all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. The information expressed herein is subject to change without notice.