savvius™

WHITE PAPER

Network Security Analytics — A New Approach to Security Risk Management

This paper describes the advantages of a new set of risk management tools — Network Security Analytics. By focusing on network traffic and using advanced data science tools like statistical and pattern matching, Network Security Analytics promises to simplify complex and tedious security tasks. The results are better protection and efficiency, at a lower cost.

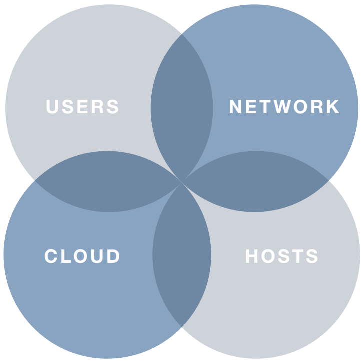
©SAVVIUS, INC. | 1340 TREAT BLVD, SUITE 500 | WALNUT CREEK, CA 94597 | 925.937.3200 | WWW.SAVVIUS.COM

Contents

Risk Management Challenge

Most enterprises find that they must manage security risk in four areas in order to protect the corporation:

- Users
- Internal Network
- Hosts (workstations, servers, smartphones)
- Cloud (or the external internet in general)



Traditional risk management starts with a threat assessment: who, what, where, when, and how could the asset or environment be compromised? This investigation results in a list of the vulnerabilities and an assessment of the damage potential. Finally, a mitigation strategy is developed to reduce the risk.

Such a static, defense-oriented approach to security is ill suited to today's rapidly evolving threat environment. Areas that were once thought to be safe, such as retail sales terminals, suddenly become attack gateways. Entirely new attack surfaces, with smartphones as a recent example, may emerge, undoing years of expensive defensive investments. This dynamic environment plays out against a backdrop of data volumes increasing dramatically.

Network Security Focus

While each of the four domains of risk analysis remains important, Network Security is widely considered the cornerstone of modern risk management strategy. There are at least two compelling reasons for this belief: first, the only way that an attacker or his malware tools can gain access to the enterprise's resources is by traversing the network. And second, the attacker has no opportunity to erase or modify the trail he leaves in the network information. Unlike logs retained by host systems or the behavior tracking of users, its nearly impossible for the attacker to erase his actions from network traffic that has been immediately collected and stored. As the saying goes "Packets never lie." None of the other domains offer this level of data integrity assurance.

The Challenge of Network Security

The incredible amounts of data that pass through the network and the limited time that any "security appliance," like a firewall or IDS, has to inspect the traffic poses a significant challenge. In addition, many security professionals, unskilled in dealing with network packet data or protocols, find key data difficult to find and understand because it's not presented in a simple and intelligible fashion.

Network Security Analytics to the Rescue

Security risk management is not the only department in the corporation dealing with large amounts of dynamic information. Customer, transaction, employee, machine, and supplier data are just a few examples. These departments use **data science** to address these problems, and "business intelligence" was born. The same tools applied to security are driving the emergence of "Network Security Analytics."

Network Security Analytics is a set of tools, technologies and methodologies broadly defined as applying the data science techniques of statistical analysis and pattern detection to network security risk management. Its promise is to replace the highly manual effort involved in defining and managing security risk with a more precisely targeted but automated way of achieving better protection with lower and less expensive manpower utilization.

There are four areas where Network Security Analytics improves on the traditional labor-intensive approach to network security:

- **Long-Term Visibility**
  Data science derives its power from analyzing large amounts of information in order to detect patterns or anomalies. Nowhere is there a richer data set to mine than network traffic.
- **Stateful Detection**
  Most current security appliances have only microseconds to inspect and evaluate traffic for malware. The network security analytics process can detect threats over minutes, days, weeks, or months.
- **Clear and Useful Guidance**
  The visualization and presentation tools of data science look to highlight what is most useful, not necessarily what is most abundant.
- **Persistent Threat Detection**
  Many corporate systems, long since penetrated, have “outpost malware” routinely communicating with the bad actors. Network Security Analytics provides a means to detect and remove these intrusions.

Each of these four areas merit greater detail:

Long-Term Visibility

Typical enterprise networks convey so much information — multiple gigabits per second — it has been considered only practical to store metadata. If full network traffic is captured, it is stored for short periods of time with traditional packet data storage systems. It is all-too-common for an attacker to delete or alter log files and other metadata in an attack that is not discovered for days, weeks, or even months. Long-term storage of appropriate packet data becomes an important enabler of informed response. Network Security Analytics storage systems can use screening algorithms to filter out “noise” traffic and enrich the stored information for mining. Like metadata storage, this approach offers the benefit of reduced physical storage requirements but still retains the ability to delve deeply into the full packet information.

Stateful Detection

Basic pattern recognition has always been a part of network security analysis. Antivirus (AV), intrusion detection systems (IDS) and even some firewalls have used constantly updated “signature” patterns to detect malware. The biggest problem with this detection strategy is that it is not “stateful” — it doesn’t maintain view behavior over time. Historically, attackers have taken advantage of this weakness to change, insert, or modify traffic and remain undetected. By contrast, Network Security Analytics maintains a higher level, historical view of the entire network traffic and can detect abnormal and malicious patterns that were previously invisible.

Clear and Useful Guidance

It is rare to find security personnel fully trained in the arcane details of many of the structures and protocols of modern internet traffic. Most existing tools demand considerable expertise to understand and analyze network traffic data. In contrast, Network Security Analytics automatically sifts through the gigabytes of network traffic and graphically presents usable, actionable information to the analyst.

Persistent Threat Detection

Existing real-time malware detection systems, with only a few milliseconds to detect a penetration, can perform only a small amount of analysis. As a consequence, attacks go undetected and succeed in planting a “backdoor” into the enterprise for later exploitation, simultaneously covering up any traces of their presence. However, the attacker cannot avoid leaving “footprints” in the network during his attack and, although the AV or IDS may not have had enough time to detect the attack, the trail is still in the historical record. Network Security Analytics engines have continuous processing systems which can examine the stored traffic at a more detailed level looking for signs that an undetected assault has taken place. In fact, any action that the attacker takes while using the network is likely to leave a trail and expose him to detection.

Summary

The historical, manual approach to risk management cannot contend with new and more complex threats to the enterprise. Business Intelligence has helped many corporations deal with vast quantities of customer, supplier, and employee data. Similar filtering and pattern matching science — Security Analytics — is being applied to security risk management. In particular, Network Security Analytics has the potential to dramatically improve threat detection, both immediate and persistent, while making it easier for the analyst to understand and respond to threats.

About Savvius, Inc.

Savvius is a leader in packet intelligence for network forensics. For over 25 years, Savvius has been providing networking and security professionals with software and hardware solutions that enable security investigations and resolve network performance issues. Savvius Omnipliance®, Savvius Omnipeek®, Savvius Vigil™, and Savvius Insight™ products deliver the expert analytics and deep visibility enterprise IT teams need. Through a global partner network, Savvius products are trusted at over 6,000 companies in 60 countries around the world.

Savvius was originally founded in 1990 as the AG Group before changing its name to WildPackets in 2000. Then, in 2015, WildPackets became Savvius to better reflect the company's core focus on network and security forensics.