White Paper
Fluency® Application Based Correlation

Introduction
FLUENCY IS COMPREHENSIVE VISIBILITY

Fluency® is vision for controlling a modern network. With innovative application awareness, auto-correlation and big data capacity, Fluency provides insight and understanding far beyond a single tool or dashboard application. Fluency reduces operating costs while allowing security to keep pace with modern networks.

Fluency technology:
- Provides comprehensive visibility into the network and how applications flow within it.
- Automatically correlates disparate security devices into a comprehensible view
- Shows network behavior and security events relate.
- Presents related information, providing a clear understanding to issues.

Network Visibility is a critical aspect to addressing today's threats. We know that the common network infrastructure does not work well in seeing network attacks, and your network cannot defend itself from what it cannot see. Fluency provides a fundamental shift to how your network detects and responds to threats by focusing on showing relative data. We know that attackers must use the lines of communication to your networks assets. The vision Fluency provides into this communication is an essential aspects to protecting your network.

Fluency technology achieves security comprehension by presenting relative information needed for the decision at hand, while providing access to significantly more information when needed. Fluency addresses information overload, not by dumbing down the data, but by better selecting relevant data. By providing the most comprehensive view of the network than any security or network product, Fluency technology makes staff more effective and productive.

Fluency is used by its customers to eliminate disparate views that are the result of single-brand driven solutions. Fluency believes that no single vendor has a complete solution, and that a technology must be implemented that leverages all corporate investments.

Our customers find that a view based on correlated application flow with security and network events provides the vision to manage, roadmap and operate their network in a business like manner. Prior to Fluency, our customers could only gauge their security by being compliant to the latest trends, or by how much time they spent reacting to issues.

After Fluency, our customers focus on measuring and road mapping their security. Response is a key element to staying secure, but response includes adjustments at the technical, architectural and policy levels. The ability to measure and roadmap to these larger issues ensures that best possible long term security performance.

This paper explores the challenges that organizations face without proper network vision and the results Fluency provides through application based correlation.

Challenges of the Modern Network

A NEW FOCUS ON INFORMATION AND MESSAGING

Businesses are discovering that simply putting antivirus on desktops and providing Internet to their employees is not enough. A business operates by efficiency and execution. Businesses of all sizes need the ability to see, measure and control how work flows within their network.

Today's work applications empower companies to execute. Companies have adapted to application connectivity through mobile support, BYOD integration and distributed/remote network connectivity. The flow of applications has become independent of the underlying network, and the traditional approaches conceived a couple of decades ago are no longer a fit for today's network and security needs.

Despite huge leaps in technology over the last two decades, log and event management has not changed from two basic camps: network flow analysis and security event management. Network flow technology was created in 1996 for network diagnostics, while event management in 1998 in order to handle alerts from multiple network segments. Though how they are used has changed, how they operate has changed little.

This gap between how the network is used today, and the technology being used to manage it has been growing to a point where many no longer see traditional security event information managers (SIEM) as being relevant. As networks continue to grow in size and complexity, the simple lists, dashboard gauges and charts add to the information overload and a lack of managerial control or any real insight. Security, which is now becoming more important to the board room, are provided no metrics or insight to execute as a business unit by traditional dashboard SIEMs.

Importance of Related Data

SOLVING INFORMATION OVERLOAD WITHOUT DUMBING DOWN THE DATA

Fluency is a network vision tool that correlates application flows, network logs and security events. It differs in that it maintains both a traditional transaction oriented view of events and a graph database that tracks and analyzes the relationships between events and attributes. This underlying technical difference means that the type of data Fluency produces is significantly different.

Fluency offers fast and complete vision into your network and your network logs. Fluency combines big data and event correlation making data access faster, while presenting related data leading to insight and vision.

Why is related data important? The old saying, “You can’t ask for what you don’t know.” is not exactly true. When you shop on Amazon, watch a movie on Netflix or go to iTunes, the system responds with related material that also might interest you. Related information is critical to good insight and decision making. Fluency is the only event management system that tracks event data, and computes the relationships between the data. The ability of presenting events in relationship to its attributes makes decision making faster and more insightful. In short, you and your people will make faster and better decisions.

On Netflix, a person can look at a movie they like and get a list of movies they might also like. This relationship is between movies you see as good. The opposite can also be true. In Fluency, looking at a badly acting system, the system shows other systems, signatures and files related to that bad actor.

It might seem a silly question, but why is faster and better decision making important. Why not just hire more people and use the systems that your company has today? Two things are working against that mindset.

- First, people are scarce. Not just good people, even average technical people are a scare commodity.
- Second, that there are more data sources and just more data being produced by your network. Technology built a decade ago just cannot handle the data loads of today. Those technologies are not changing, yesterdays solutions are just throwing more machines, processors and disks at the problem. And the breaking point where doing so no longer works is happening today.

The resource of good people are increasing in value. The number of unfilled technical positions continue to increase. Between tight budgets and the difficulty of finding good people, organizations have gaps in personnel, and rely heavily on their best people. Not providing fast and complete access to event and log data is not just costing money, but is stealing productivity from your most valuable people.

Case Study Summary: The Design Gap

A BUSINESS NETWORK IS NOT A HOME NETWORK

Its so easy to start a network these days. The moment you buy a home, the local provider drops a wireless cable modem, and your house has a network and you have Internet. Your phone can create a hot spot network on the fly. So, what is so hard about a network? It’s not only small companies, but fairly large ones too, that live of the instant network. “We have no servers, all we need is Internet access.”

Small Companies can benefit from good infrastructure.

The problem is that many growing companies have a network infrastructure that has grown organically through the networking knowledge of their people. On a recent engagement with an investment firm, we found many of the problems that medium sized companies have in their infrastructure. When the network started getting bigger, they had outsourced desktop support. The systems appeared to be running well, so what could be an issue?

- Issues with DNS
- Tracking the desktop
- Problems with Policy

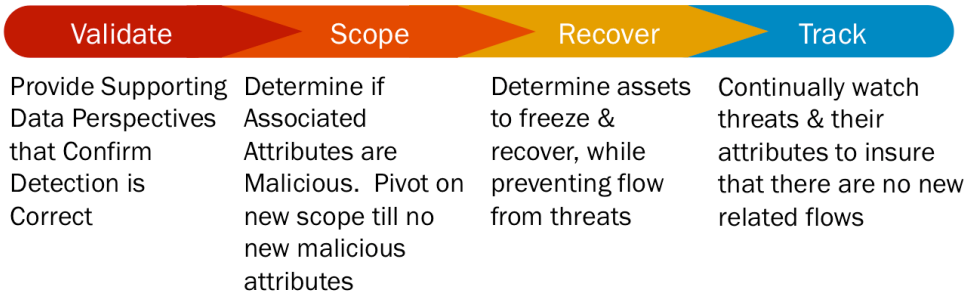
Focus was on devices and connectivity. As long as the device had antivirus, connectivity to the Internet and printers were good, then the network was considered complete.

Fluency was installed for peace of mind. And that is what they have now, but at first it was an eye opener.

Most people know how to connect their device to a network. But the judgement of individual people on what to install on their systems can have a large impact to security. Unwritten policies aim that common sense as its baseline. Without written policy and guidelines to its users, bad decisions can be made. Even with written policy, there needs to be a means to see and enforce direction.

During the initial profiling and assessment period of Fluency, it became apparent that the network had no true architecture. Fluency's profiling detected a desktop that was, among other issues, preforming automated communication not associated with the company. The issue was not just the need to clean the system, but also to address the network architecture and policy issues that were the cause of the issue and which hampered response.

The solution was driven by Fluency. Fluency addressed three critical elements that allowed the problem to be properly **understood**, **tracked** to closure and **mitigate** longterm risk.



Understanding the Problem

Fluency does not simply correlate data, its sensors listen to the network in order to track application flow. Every application communication is stored as a record, and any other network alerts associated with the flow are correlated to that flow. This approach is not a traditional SIEM approach, for traditional SIEMs focus on correlating only alerts. But most issues never generate alerts until they cause significant impact.

And so at the firm, it is this vision into application that showed a significant issue. Fluency profiled all network's behaviors, such as mail, phones systems and cloud services. The result was an outlier that communicated externally on an ongoing basis.

Fluency could subtract all the communications that were considered normal. Each communication outside of normal for the firm's business could be marked creating a complete scope of the issue.

Fluency also overcame the organic network that was created as the firm grew. How the system joined the network was not controlled and systems bypassed the local name server. Fluency's full packet capture was activated allowing for the connecting protocols to be reviewed in detail, providing the system name, network address and machine address code. Furthermore, policy issues and network management issues were documented.

Tracking the Problems

Business is about execution. The ability not only to see an issue, but to address it. Properly addressing issues is where organizations excel over others. This means that ability to measure a response and validate its closure. Fluency is further unique from SIEMs as it tags elements of the issues tracking them when they occur to ensure closure.

At the firm, this meant addressing the rogue processes (technical), how the systems connected to the network (technical) and developing a policy around BYOD (policy). Here Fluency tagged each element of these issues separately, and *provided metrics to the firm to measure the effectiveness of mitigations*. Measuring effectiveness is a key difference between Fluency and SIEM products. This requires detailed event logging, not just alert logs.

Tags are created in Fluency related to a metric related to a response decision. Here tags are created to track:

- unwanted communications from the system in question
- how the system connects to the network
- the name server (DNS) that the system uses
- the type of system based on asset list (BYOD v Corporate Asset)

Now each aspect of the three issues can be articulated in numbers, such as the amount and percentile, based on tags. The situation can be managed, and answers can be given:

- Have all the rogue communications stopped
- How many BYOD systems are on the network
- How many BYOD systems are mobile devices
- What are the names of BYOD systems
- Are all systems using the correct name server (DNS)

With Fluency tracking each communication with application tags, questions have definitive answers. The firm can now track the progress of the response.

Long Term Mitigation

Fluency's tracking is not a database query. Fluency tags and alerts on all incoming events in realtime. Its not reporting but tracking. And since the tagging is built into the system, the system can continue to monitor and produce metrics.

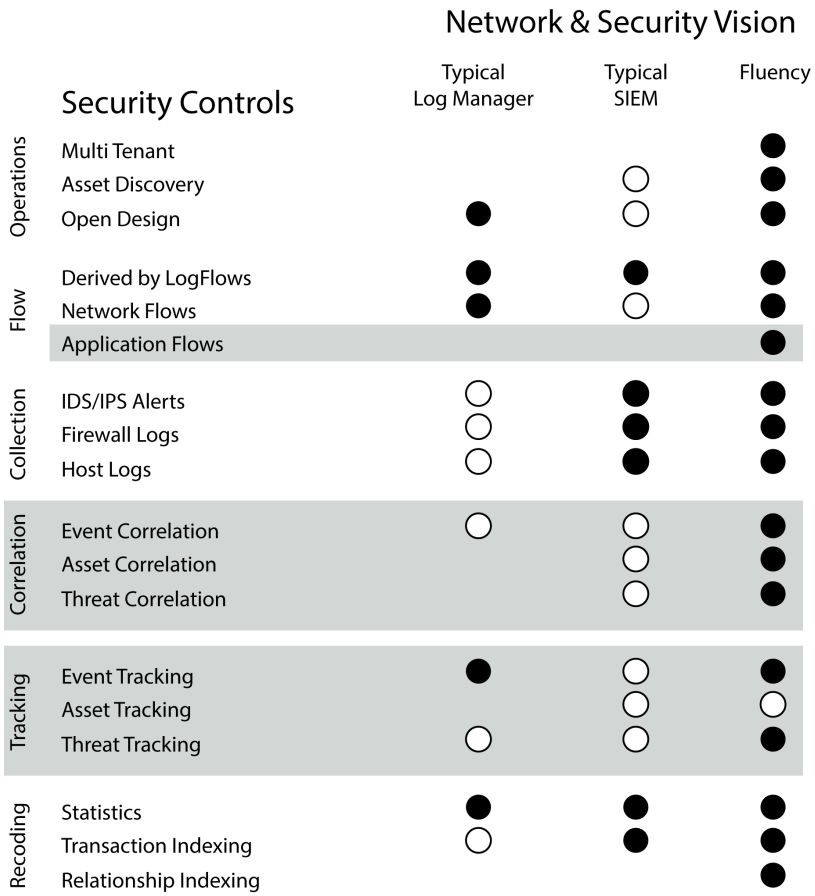
With Fluency, management can implement changes and measure the results of those changes. This is a different approach to security than checkbox compliance. The objectives of security managers can be focused on progress and business execution. The business day is quantified. Gone is a whack-a-mole approach of waiting for issues and then rushing to resolve them.

Fluency's provides metrics, which in turn allow management to execute a long term strategy. Management can now articulate more than "is it done", but how how much is done, and how effective is the change or response.

Results

When Fluency started with the firm, the firm had little insight into their network. Its corporate measurement for the network was asking, “is the network up?” and “am I getting mail?” Now the firm knows each system on the network, how they communicate and what is normal. The firm can now make changes to the network, and measure those changes. The firm now has vision into a valuable aspect of their daily operation.

Now, The firm knows what is happening on the network.



A Solid Home

A HOME, NOT A HEAP OF MATERIAL

Having all the parts does not mean you have a solution. Socrates said, “A disorderly mob is no more an army than a heap of building materials is a house.” The same can be said of your network. Having all the parts and checking all the boxes does not mean that the network is secure.

Placing all the data into a single location does not mean that you can leverage that data. A single console is not the real goal, it’s integrated data in order to get a holistic view of your network. From this view, you can make, execute and measure decisions.

At the same time, the amount of manpower to operate the solution needs to be minimal. Fluency is a deigned to reduce operational manpower. Correlation is automated based on the event parser. The datastore is dedicated, just like that of your contact list. You do not have a dedicated administrator to manage your contact list.

Fluency is engineered and built for leveraging data analytics. Its patented approach

Conclusion: Fluency's Business Approach to Security

Its not just networks that have changed. Companies have brought security to the boardroom. Managers with security responsibility must operate as managers, which means insightful decision making, a focus on execution and measuring results. Management relies on vision and Fluency provides that vision.

About Fluency

Fluency Corp, a recognized leader in security innovation, is transforming the way middle to large organizations manage the security of their network. Fluency is focused on improving the network and security operations of its customers. Fluency provides its customers with engineered solutions that are built to address business needs of network security and management. Fluency is privately owned. For more information about Fluency Corp, please visit www.fluencysecurity.com.