Active Network Defense: Real-time Network Situational Awareness and a Single Source of Integrated, Comprehensive Network Knowledge

This paper will present a case study of Lumeta's participation in an open standards group, The Trusted Computing Group and adoption and support of the Trusted Network Connect (TNC) standard. Open standards-based security integrations offer a single source of knowledge about the network; the ability to derive more value from best-in-class security tools already deployed; and a means to accommodate the rapid pace of change in today's dynamic and distributed enterprise network environments. This RFI response will discuss the benefits of open standards technologies for integration from Lumeta's perspective as a vendor, taking a close look at the TNC such standard technology. We'll also examine a working example of an IF-MAP implementation, showcasing the increased value active network discovery data contributes to integrated network security metadata.

Why Open Standards for Security Integration?

Network security solutions are often deployed to address a particular regulatory requirement or to in response to a known threat to the enterprise. For organizations with large and complex networks, the result is often a disjointed series of security point solutions. The security solutions may be best-in-class technologies, which address the original need but do not impart their full potential value to the enterprise.

In response to this, many IT organizations increasingly looked to proprietary security suites in recent years. While these may address some of the challenges in disjointed enterprise security architectures, they typically neglect significant portions of an organization's existing investment in security point solutions and further limit the future selection of best-in-class products.

As an organization evaluates proprietary or closed architectures against open standards, there are three factors that are particularly important to consider:

1. The exponential growth of IP-enabled devices in the enterprise means that IT organizations are supporting a wider variety of devices. As new devices connect to the enterprise network, they bring with them unique security issues, necessitating specific security solutions that may not integrate into closed, proprietary security models.
2. Today's networks are increasingly heterogeneous because of the drive for IT to support much more agile business technology needs. Open security architectures and standards-based security integrations allow for organizations to adapt to requirements for network change, without compromising security.
3. Comprehensive, open security integration allows organizations to drive more value from their existing security and IT operations investments, and to continue to select products that represent the true best-in-class solution for each specific area.

The Problem of Proprietary Approaches in a Growing, Heterogeneous IP Environment

Embedded security as a concept defies the proprietary model, as the heterogeneous nature of networks today requires security solutions that offer open architecture and standard interfaces to support components from a variety of vendors. This is particularly true at the large enterprise level, where it is easy to see that when a particular security solution is deployed, it may be protecting devices that are all of a certain type. However as the business changes, through an acquisition for example, it may become necessary to manage security across multiple vendors. In this kind of environment it is clear that proprietary integrated security solutions will inevitably leave part of the environment unmanaged or unsecured. To further the issue, after changes occur continued reliance on assessments through proprietary protocols could not possibly provide the most accurate information on which to make security decisions.

In contrast, an integrated security architecture built on open standards will accommodate new security information as best-in-breed products are deployed on the network as long. As long as those best-in-class selected point products have adopted the chose open-standards (or can at least share data in a manner compatible with it) configuration of those tools to enable event and information sharing will be a simple undertaking.

Supporting Exponential Growth of IP-enabled Devices

There is no doubt that every large enterprise network is facing a huge challenge in dealing with the exponential growth in IP-enabled devices. From newly Internet-connected devices that are already entrenched in operations; to non-traditional devices using IP to communicate for remote administration (such as physical security and HVAC machines); to consumer and mobile technology adoption being driven by the need to support an agile workforce: the need to secure the enterprise network is being intensely complicated by the need to support these new devices.

Adoption of an open, integrated security architecture built on vendor-neutral technology allows for active security assessment of every device that touches the enterprise. As new device types connect to the enterprise, and the open, fully integrate security solution will assess those devices and provide information about their state, and possible security gaps to the security architecture.

Derive More Value from Existing Solutions

By the time most organizations are considering adopting an integrated security architecture, they have already invested a significant amount in security tools. Vendor-neutral, open standards based approaches allow for organizations to further leverage the investments that have already been made, driving more value from the security function. Further,

In order for organizations to respond in real-time to changes in security posture, maintain compliance and ensure continuous network service availability, they require in-depth network and security awareness and coordinated defenses among deployed networking and security solutions.

A fully integrated security environment, communicating on open technologies that are widely adopted by security infrastructure vendors, has the advantage of becoming more intelligent overtime through it's ability to gather information unique to specific best-in-class security specialty solutions as well as from new security tools as they are integrated.

The State of Open Standards for IT Security Integration

We have established the number of IP-connected devices on the network continues to grow exponentially; networks are increasingly homogenous; and IT organizations are under pressure to derive more value from existing investments. Unfortunately, many of the integrated security solutions on the market are vendor-specific. Given these circumstances in enterprise IT it's apparent that vendor-neutral, standards based integrated security solutions will become the only sustainable way to embed security into the enterprise network.

As the growth of networks outpaces hiring and budget increases, IT security organizations are increasingly looking toward integration as a means to facilitate IT automation. An integrated solution which bases policy decisions on the best available information from all available security tools greatly improves the quality of the basis of that decision making, giving organizations confidence to full automate those processes, reducing man-hours spent on remediation and log analysis.

The concept of using integrated security architectures, based on open, vendor-neutral standards has matured significantly in recent years. Many of the core technologies and open standards are now widely deployed and time-tested business solutions.

Trusted Computing Group's TNC Architecture and the IF-MAP Protocol

About the Trusted Computing Group (TCG) and Trusted Network Connect (TNC)

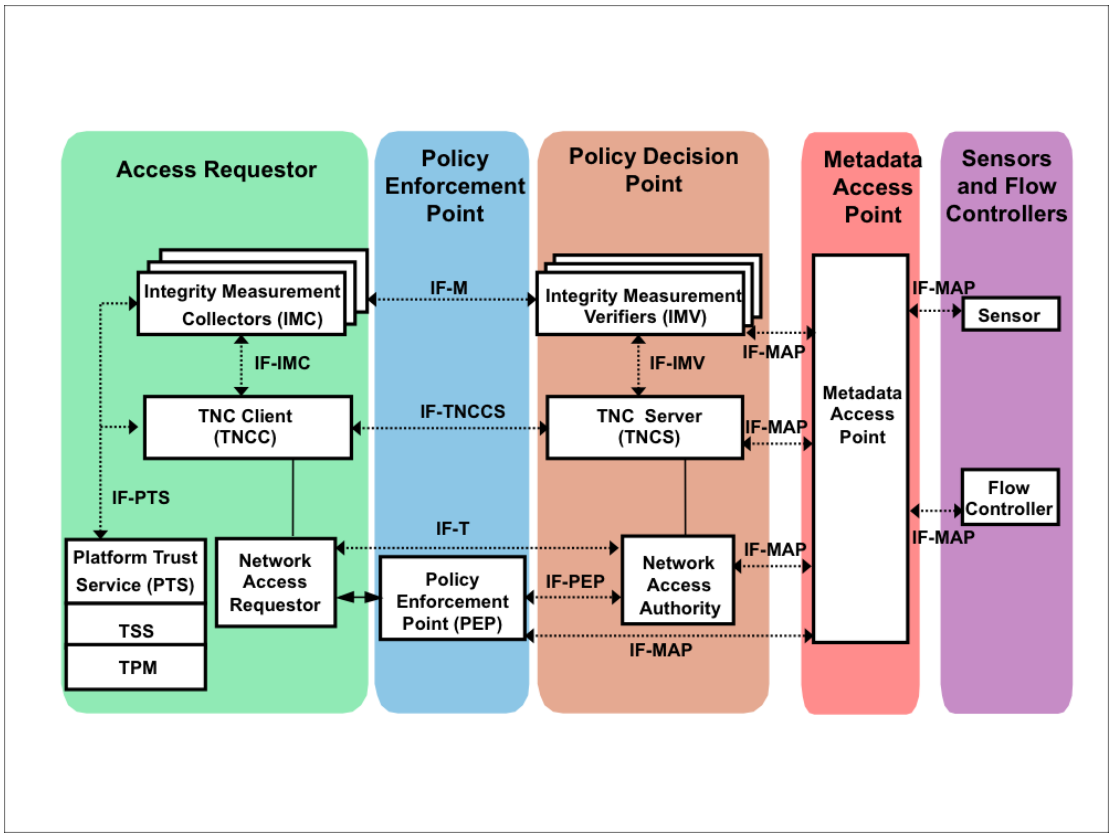
The Trusted Computing Group (TCG) is an international industry standards group, which develops open standards for trusted computing which are vendor-neutral and interoperable. The TCG is supported by hundreds of IT and security equipment manufacturers. TCG has approximately 100 members from across computing, including component vendors, software developers, systems vendors and network and infrastructure companies and a number of products support TCG specifications.

TCG has been perhaps best known for its development of the Trusted Platform Module (TPM), a hardware component specification designed to protect platform and user authentication information and unencrypted keys from software-based attacks. TPM chips are available from a number of vendors and sold today in almost one billion PCs and other systems.

In 2005, the Trusted Computing Group (TCG) introduced an open architecture for network security and policy enforcement called Trusted Network Connect (TNC). The TNC specification has evolved over recent years, expanding in 2009 to include the Interface for Metadata Access Points (IF-MAP), an open standard client/server protocol for sharing information about security events and objects.

For the sake of overview, the diagram below shows the complete TNC architecture. Each dotted line represents a standard protocol. In short the protocols serve the following purposes in this architecture:

- IF-M, IF-TNCCS, and IF-T offer standard protocols between the Access Requestor and the Policy Decision Point to ensure that a device from one vendor can be health checked by a Policy Decision Point from another vendor.
- IF-PEP provides a standard protocol to ensure compatibility with a variety of different Policy Enforcement Points.
- IF-IMC and IF-IMV are client and server security software packages.
- IF-PTS provides TPM support and integration for the hardware component discussed previously.
- IF-MAP to integration of data from network security products like intrusion detection and leakage detection.



The TNC architecture solves a problem in security coordination. Most enterprises have a wide variety of tools in operations that hold bits of network and security information about users or endpoints. These tools range from firewalls and authentication servers to continuous monitoring tools and malware detection. But in most enterprises, the information is collected in silos. There is often no single authority on the state of the network.

The issue is further complicated by the many different ways which network security data is structured. As the enterprise network continues to evolve, new data from non-network sources becomes relevant to network security, such as physical security devices like badge readers.

IF-MAP: A Common Interface for Network Metadata

Although an overview of TNC is provided for background, the focus of this paper is primarily on the Interface for Metadata Access Points (IF-MAP) protocol. IF-MAP, provides a common interface between the Metadata Access Point (MAP), the Policy Decision Point (PDP) and Policy Enforcement Point (PEP) as well as the various devices in the network that have information about the security events and objects ("sensors" in the above diagram).

The Metadata Access Point (MAP) server is meant to be that single authority on the state of all devices on network and IF-MAP is meant to be the means to communicate information to form that picture. IF-MAP servers, publishers and subscribers provide a standard means for policy decision-making and enforcement based on comprehensive information on the state of events and objects on the network.

The IF-MAP protocol defines a publish/subscribe/search mechanism, with a set of identifiers and data types. This enables devices in a security architecture to share data about network devices, policies, status, and behavior in real-time.

Active Network Discovery Contributes to Rich Network Metadata

As enterprises seek to automate facets of IT security policy enforcement, knowing what's on the network and ensuring that only devices which are known, managed, and clean are allowed to connect are critical parts of any security plan. The first step in implementing an integrated network security architecture is to assess and document the entire infrastructure including all resources, devices, and connections. The information gleaned from this type of assessment is information on which the majority of security tools will rely. An active network discovery baseline offers real-time situational awareness of large, complex geographically disperse networks. An active network discovery baseline provides a means to uncover all active IP space, automatically catalogue those address ranges that fall within the IP space provided initially (i.e. those ranges that are "known") vs. all newly-discovered IP space, which may contain active, but previously "unknown" IP devices. By taking this holistic approach to the baselining process, IT security managers can make accurate decisions based on the best information available as to the nature of individual networks/devices within any network.

Earlier in this paper we established the rapidly changing enterprise network environment, where consumer devices, mobile, and other non-traditional network devices connect to the enterprise with increasing frequency. Just as an active baseline is critical part of the initial implementation of security integrations, with the rapid pace of change in the enterprise, active network discovery also remains an important component of continuous monitoring well beyond the baselining process. Active network discovery by definition uses an active probe to locate everything that's on the network, (not just an IP range that is supplied for scanning) resulting in a comprehensive view of the entire routed infrastructure. This active probe can be used to ensure that Network Metadata is being complied on every connected device, and that unauthorized devices or connections are promptly indentified and managed.

Active network discovery provides the mean to scan IP ranges continuously and be empowered with a solution that will dynamically "learn" more about the environment, eliminating the inherent gap between the perceived network and the actual one. The simple idea being that: you can't secure what you can't manage, and you can't manage what you don't know about.

Lumeta and the Trusted Computing Group

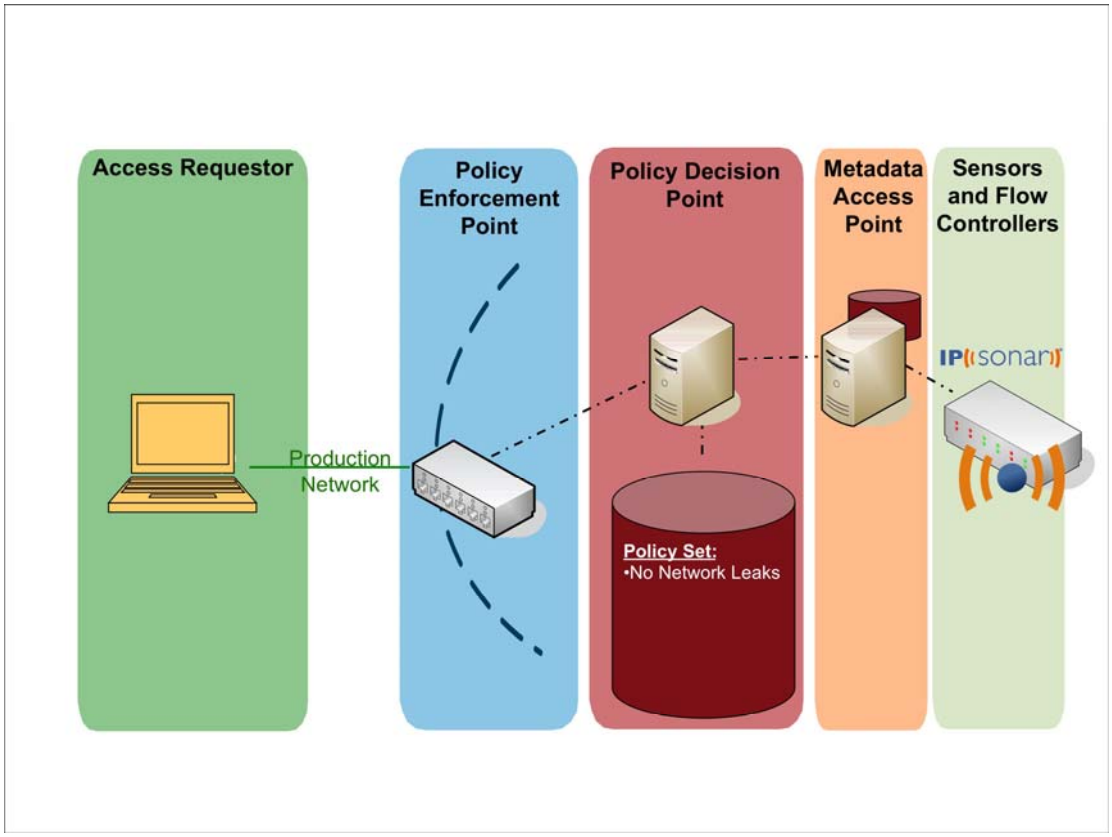
Recognizing the power of TCG's IF-MAP prototype to bring together security information and events across the security infrastructure, Lumeta joined the TCG in 2008 to support the development of and adopt the new IF-MAP standard. The dynamic data exchange among a variety of security and network applications which IF-MAP facilities is something that Lumeta has seen in many customer environments. As a long-standing proponent of open standards, Lumeta participates in the development of a standardized enterprise security information sharing technology as part of our commitment to future-proof and less complicated deployment of integrated network security architectures.

In 2009, Lumeta was among the first companies to announce availability of an IF-MAP client, for our active network discovery solution IPsonar. Lumeta continues to be an active contributing member of the Trusted Computing Group working to advance adoption and development of this standard.

IPsonar uses active network discovery and mapping capabilities to gain visibility into every asset and connection on a network, including those not currently under management. The data discovered by Lumeta IPsonar and shared through IF-MAP enables IT professionals to analyze the connectivity between assets and networks, uncover risk patterns, and automate the enforcement of network policies.

For example, of how the Lumeta IPsonar IF-MAP client works, we'll illustrate here how information detected by Lumeta IPsonar's patented network leak discovery capability can be acted upon in real-time in an operational network environment. Lumeta IPsonar's network leak discovery capability is a patented technology which is used to empirically determine the connectivity to and from the Internet or secure zones; verify that secure zones are properly protected; validate security of outsourced or managed connections; expose rogue or unauthorized connections; and finally, to perform continuous monitoring or post-admission policy validation via TNC.

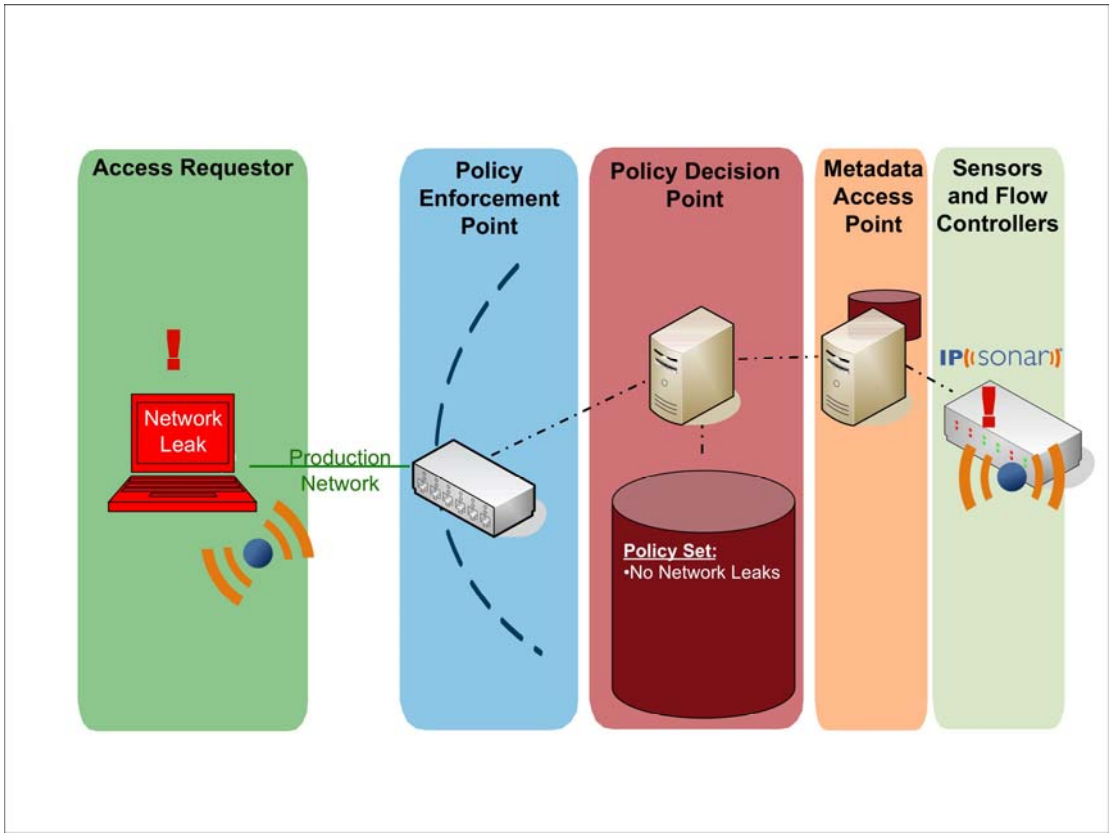
Lumeta IPsonar IF-MAP / TNC Deployment Automates Network Leak Prevention
In the diagram below, a pre-admission health check was conducted on the Access Requestor and after passing this test; the user was grated access to the production network. On that production network, there is a policy set at the PDP that states 'do not allow network leaks on the production network.' Lumeta IPsonar is depicted on the far right of this graphic as a "sensor." In this depiction, Lumeta IPsonar is continuously scanning the network with its network leak detection capability and has not detected any network leaks.



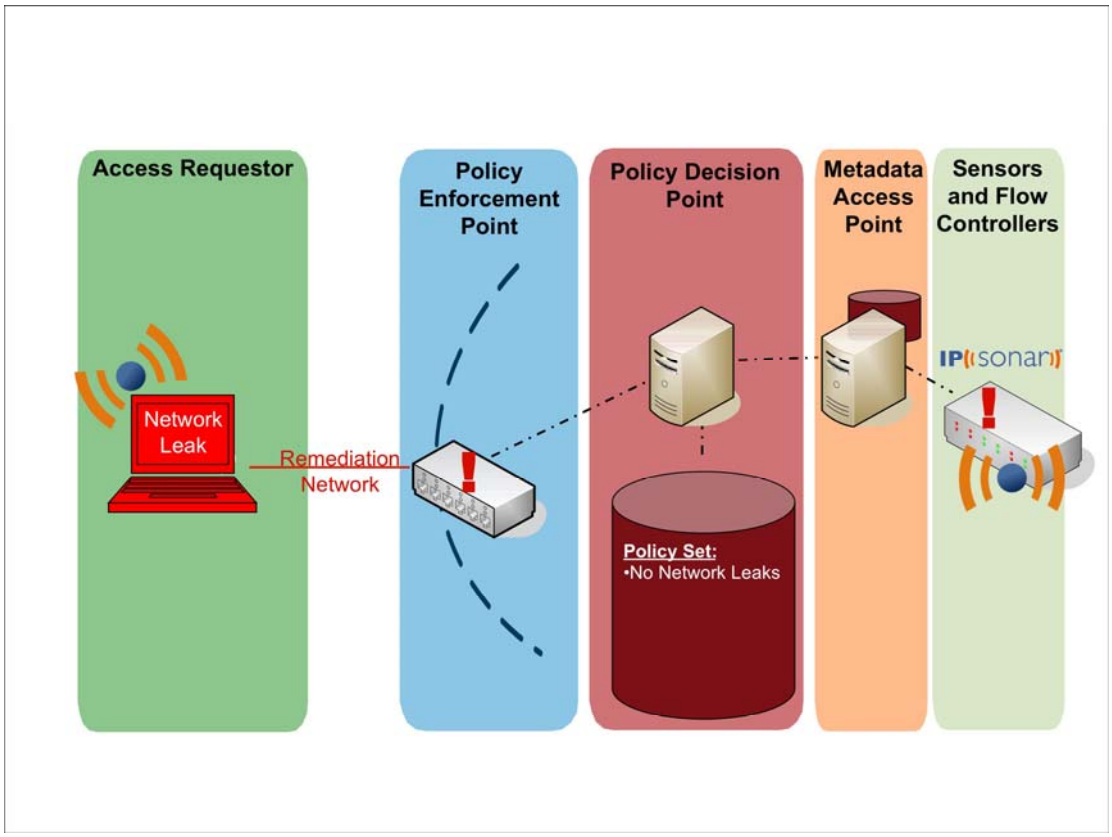
As we've discussed, enterprise networks are highly dynamic and events (both intentional and unintentional) can cause network configurations to change over time, falling out of step with security policy. For the sake of this example, let's say that after the user was successfully granted access to the production network, the user opens a PDF file that contains a Trojan, which causes the laptop to suddenly change the state of its external connections in a manner in violation with policy.

In an environment where the TNC architecture is deployed, and Lumeta IPsonar is deployed to provide active network discovery information about the network, IPsonar will discover the network leak as it continuously scans the entire connected network. IPsonar is unique in the market for its

ability to do this quickly and in such a lightweight manner that it can be continuously run during a network's key hours of operation. In the diagram below, IPsonar has detected that the device has a network leak.



Lumeta IPsonar then uses the powerful publish/subscribe/search mechanism of the IF-MAP protocol to publish information about the leaking device to the TNC MAP server. The TNC Policy Decision Point (PDP) recognizes that the information published to the TNC MAP server is in violation of the set policy and publishes that recognition to the Policy Enforcement Point (PEP). The TNC PEP server immediately takes action, as illustrated in the diagram below. The laptop which as been identified as having network leak (unwanted connectivity into or our of a network space) and in an automated real-time manner, that device has been placed in a remediation subnet.



In this case, the policy defined dictated that the devices be moved to a remediation network, effectively eliminating the exposure from the network leak because the remediation network would change the access granted to the user. This is just one enforcement action that is possible, there are endless possibilities but one alternative is for a user in violation of the policy to be denied access to any network resources.

It should be noted that this fairly complex action, from granting access to user in compliance, to a security event or change occurring to move that user out of compliance, thru to the detection of that policy violation and the limitation of that users network access for appropriate remediation would only take a matter of seconds. Further, other than the need to set up the integrated environment, and to define the policies in the architecture, the process itself of detecting the violation and changing the users access was completely automated. The automation of this type of integrated, dynamic security environment not only helps to keep costs down while deriving increased value from existing IT infrastructure, but it inherently makes security more effective by anticipating even the most savvy of bad actors.

The TNC architecture, leveraging the powerful IF-MAP protocol, has detected and remediated an unauthorized "backdoor" Internet connection that potentially would have bypassed network access controls in a different environment. IF-MAP enables integration of network intelligence from additional network and security systems to make access decision based on all available information in real-time.

Other Deployments and Use Cases

While we have focused on one simple use case and a simple (yet powerful) example of integration, using Lumeta Network Leak Discovery for policy enforcement, the power of the IF-MAP technology reaches well beyond this example. There are IF-MAP implementations where customers have for example integrated physical security information with network access control, uniting physical and logical security. This adds a common sense layer to security, for example automating policies to enforce that a user must physically be in a location to access a logical network connection point in that location. This not only increases network security by adding another check, but also can uniquely help to close in on insider threats. There are other implementations where IF-MAP is deployed in securing remote access functionality for a variety of types of systems. IF-MAP is also actively deployed in several client instances for integration of information about overlay networks, such as control systems.

Because of the simplicity of the IF-MAP technology, it scales exceedingly well and can handle disparate data types as it was built to support loosely structured, asynchronous data that is only related through publish/subscribe/search mechanism. The future of IF-MAP is as a scalable means for real-time security information sharing and control coordination on across distributed enterprise networks, reaching all the way through to the physical security world.

Conclusion

An enterprise's security posture can be impacted by a plethora of variables – lack of visibility into the network, unauthorized network connections, ineffective security controls, infrastructure modifications, unmanaged network devices – the list goes on and on. In an effort to combat such threats and obtain true network security, organizations typically implement a range of security and network management solutions from multiple vendors. While these point solutions can be effective in delivering one piece of the overall network security picture, the nature of today's evolving networks necessitate a comprehensive, integrated network defense solution where there is one single source for network metadata that is used to inform policy enforcement and risk mitigation.

The Trusted Computing Group's open standard for TNC IF-MAP technology provides a groundbreaking, working opportunity for vendor-neutral security integration in a standardized and scalable manner. The IF-MAP protocol technology is uniquely able to accommodate varied data sources and unstructured data relationships to compile that single source of network metadata.

For more than 10 years, Lumeta IPsonar has been on the forefront of active network discovery, focusing on providing unprecedented situational awareness on the world's largest networks. Uniting Lumeta IPsonar's powerful active discovery data with the information correlation and real-time automation that TNC IF-MAP offers, real-time security automation and seamless continuous access control are possible on even the largest most complex networks.

Together, the IPsonar and IF-MAP standardized technology provide the keys to active network defense on dynamic, complex networks to help organizations keep pace with the changing cybersecurity threat landscape while deriving more value from network security investments through correlation and automation.