

CONTINUOUS CYBER SITUATIONAL AWARENESS

Continuous monitoring of security controls and comprehensive cyber situational awareness are the building blocks of proactive hybrid cloud security

Executive Summary

Successful cyber security programs require complete cyber situational awareness. For enterprises that are embracing the cloud, this means having comprehensive visibility to assets and activities throughout hybrid cloud networks. Cyber situational awareness enables security and network professionals to predict and defeat cyber-attacks by recognizing threats originating outside an organization as well as vulnerabilities and threats emerging from within. The foundation of this awareness is continuous monitoring that produces visibility in real-time across the hybrid network and all of its connections and devices.

A comprehensive continuous monitoring program provides essential, near real-time security status-related information. It allows an organization to track the security state of a system on an ongoing basis and maintain the security authorization for the system over time. Maintaining the security state of information systems in highly dynamic environments that include cloud, virtual, physical, and software-defined network infrastructure, as well as endpoints and operational technology (OT) / Internet of Things (IoT) is particularly challenging.

To meet this challenge, organizations use a variety of threat and vulnerability monitoring tools. Although they may be effective at performing targeted tasks, such tools typically cannot provide complete visibility into the threat landscape. Security and network professionals therefore need a **continuous cyber situational awareness program that leverages investments in existing tools while introducing new approaches to network visibility and data analytics to achieve real-time, accurate, advanced threat detection and incident response for hybrid environments.**

This paper provides an overview of the concept of continuous monitoring, describes how to achieve continuous monitoring, shows why automation is critical to continuous monitoring and reporting, and summarizes the impact of the proliferation of new technologies on an organization's security and risk postures. The paper then discusses FireMon's approach to continuous monitoring through real-time network and cloud discovery, topology mapping, and leak discovery, and how it delivers vital, comprehensive visibility to security and network professionals.

Introduction

Comprehensive cyber situational awareness is foundational to effective hybrid network security.

Cyber situational awareness involves the collection, correlation and analysis of information to produce a common operational picture of the entire hybrid cloud environment, including:

- A comprehensive and broad visualization of the current IT infrastructure
- Real-time data needed to test the security controls protecting the IT environment
- Identification of critical and/or sensitive infrastructure components
- Detection of events or configurations linked to adversarial or anomalous conditions

Without a means to obtain holistic cyber situational awareness, security and network professionals largely rely on locally focused specialty products, such as intrusion detection systems (IDS), and manual data analysis from complex systems such as network management suites to gain a level of insight into the network infrastructure. But monitoring only specific parts of the network without visibility into the state of the network as a whole leaves inherent gaps in defenses.

Many organizations have determined that while traditional security monitoring systems can help information assurance efforts, they are rarely adequate for today's external, targeted, persistent attacks. As a result, enterprises are beginning to replace point-in-time audits and compliance checks with continuous monitoring programs to help them prioritize controls and provide visibility into current threats.

What is Continuous Monitoring?

Organizations perform regular reviews of their information systems' security controls to ensure that system changes do not have a significant negative impact on security, that security plans remain effective following changes, and that security controls continue to perform as intended.

Continuous monitoring differs from traditional periodic assessments or “snapshot” audits by performing **continuous and real-time** monitoring of transactions and controls, so that weak, poorly designed, or poorly implemented controls can be corrected or replaced rapidly, thus enhancing an organization's risk profile.

The National Institute of Standards and Technology (NIST) has been a thought leader in the development of information security standards. The NIST Special Publication 800 series¹ of standards for cyber security have become **the de facto standard for securing network data systems in the United States and many other countries**. Leading IT security regulators employ the key concept of managing and tracking the security state of information systems – moving away from point-in-time snapshot testing of security infrastructure effectiveness to continual analysis of the ability of security systems to protect critical assets and data.

NIST defines information security continuous monitoring as “maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions².”

Continuous monitoring of security controls is essential to mitigating enterprise-wide risk through system-level network monitoring and detection. An effective continuous monitoring program should detect and alert information security professionals regarding network changes that require attention.

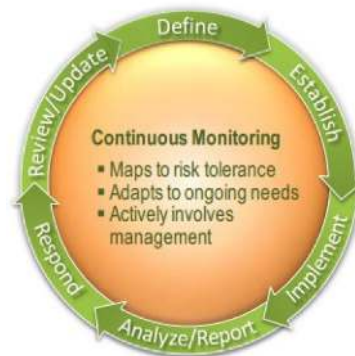


Figure 1: Information Security Continuous Monitoring Process – NIST Special Publication 800-137³

¹ <http://csrc.nist.gov/publications/PubsSPs.html>

² NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, published September 2011

³ http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909726

Continuous monitoring enables information security and network professionals to quickly analyze a stream of real-time data regarding the state of risk to their security, network, and end points, as well as cloud, software-defined, and other virtual devices and applications. This allows IT security teams to plug obvious security gaps, eliminate known threats and vulnerabilities, deny unnecessary connections, keep security policies up to date, and more effectively enforce security policies.

NIST defines six components – the Risk Management Framework (RMF) – that work together to provide comprehensive guidance on how to implement continuous monitoring into the security lifecycle (illustrated in Figure 2). The RMF emphasizes the importance of near real-time risk management through strong and effective continuous monitoring processes. It also encourages the use of automation to give top-level management the critical information needed to make cost-effective, risk-based decisions that support their primary missions and business processes.

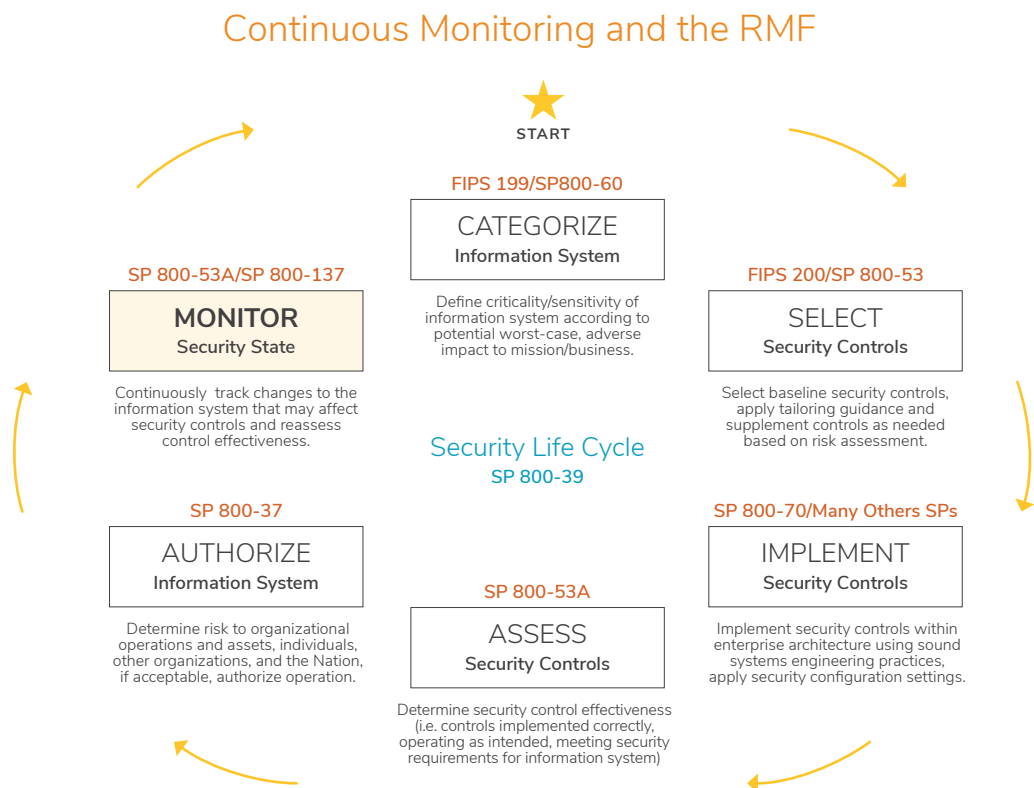


Figure 2: Continuous Monitoring and the Risk Management Framework proposed at NIST⁴

⁴ <http://csrc.nist.gov/groups/SMA/forum/documents/Forum-121410-Continuous-Monitoring-AJohnson.pdf>

While each organization's requirements are different, continuous monitoring should include the following types of monitoring and correlation capabilities:

- Vulnerability, configuration and asset management
- System and network log collection, correlation and reporting
- Advanced network monitoring using real-time network forensics
- Threat intelligence and business analytics that fuse data from all monitoring feeds for correlation and analysis

"Continuous monitoring is a proven technique to address the security impacts on an information system resulting from changes to the hardware, software, firmware, or operational environment. A well designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information system."

» NIST Special Publication 800-37, Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems, published February 22, 2010

A key component of continuous monitoring is real-time notification of events outside of security policies that trigger the immediate need to assess security controls or verify security status. Security-related data resulting from continuous monitoring is analyzed in the context of stated risk tolerances, the potential impact that vulnerabilities may have on information systems, business processes, and the organization as a whole, and the potential impact of mitigation options. The end result is improved organization-wide risk management and continual improvement from collecting information and responding to findings.

Protective Monitoring, also known as Good Practice Guide 13 (GPG13), is a UK government⁵ recommended set of processes and technology to improve risk profiles – essentially, providing visibility and an understanding of who is accessing a company's or public sector organization's sensitive data. The GPG13 was developed in an effort to better protect systems from internal and external threats through monitoring practically every component within an organization's IT infrastructure. Many of the concepts regarding Continuous Monitoring can also be applied to the Protective Monitoring guidelines and will help organizations gain situational awareness of risk events.

⁵ CESG (Communications-Electronics Security Group), the United Kingdom's National Technical Authority for Information Assurance (IA).

The Requirements for and Benefits of Continuous Monitoring

In the public sector, OMB and NIST mandates and standards require continuous monitoring. In the commercial sector, Payment Card Industry (PCI) standards, data breach laws, and regulations such as Sarbanes-Oxley have requirements for continuous or regular monitoring of security controls.

Although details of the mandates and regulations differ, they share common policy requirements with respect to continuously monitoring security controls and boundaries around sensitive network data.

Industry and government compliance mandates go a long way toward addressing the issues of maintaining a secure IT infrastructure, with policies and procedures to guard against security breaches and access to sensitive data. To be compliant, an organization needs to undergo an audit to ensure that its IT security controls are functioning appropriately, and that proper policies and procedures are in place. However, IT audits are typically snapshots that may not adequately reflect the true operational security posture of the network.

Change is constant in a large complex network. Companies and agencies can quickly fall out of compliance, becoming more open to the risk of having their network and data assets compromised. A continuous program is needed to monitor transactions and controls ensuring that compliance is effective on an ongoing basis.

Real-time monitoring and reporting can enable organizations to make immediate, cost-effective decisions that mitigate IT risk in information systems. Depending on the vertical industry, this might include:

GOVERNMENT AGENCIES

The information and systems agencies need to protect are critical to the nation and national security. FISMA regulations now mandate continuous monitoring of security controls.

CRITICAL INFRASTRUCTURE PROVIDERS

The protection of electric grids, mass transportation, and facilities that manage the nation's water supply and other industrial systems deserves serious attention on a continuous basis.

FINANCIAL SERVICES

Ensuring the integrity of financial transactions to guard against fraud, error and misuse is a daily essential.

OTHER COMMERCIAL ENTERPRISES

Vertical industry compliance mandates more frequent ongoing testing of security systems and policies to replace traditional once a year "snapshot" assessments. In many cases, the savings in expenditures, resources, and continued compliance may outweigh the costs of a once-a-year audit and the consequences associated with a security breach.

BUSINESS IS CONTINUOUS. SECURITY SHOULD BE AS WELL.

The benefits of continuous monitoring are not simply to comply with monitoring mandates. By using a continuous monitoring program, organizations can improve the quality and timeliness of decision-making as network security is aligned to key business objectives and managed holistically. Continuous monitoring allows organizations to manage IT assets in a proactive manner, and identify risks and gaps in security posture, so that IT professionals can react, recover and maintain key business operations. Overall, organizations will gain:

- Tighter risk control
- Better network assurance
- An enhanced security posture
- Reduced operations and compliance costs

Virtualization / Containerization / Micro-segmentation / Cloud

VIRTUALIZATION, CONTAINERIZATION, MICRO-SEGMENTATION AND MORE

Enterprises are embracing cloud, virtual, containerized and micro-segmented networks to take advantage of newfound speed and flexibility—but those networks must integrate seamlessly with traditional network infrastructure.

As hybrid networks become the norm, they can be complex, fragmented and unpredictable. Organizations should consider the gaps in network visibility that these technologies introduce. IT professionals should review their security architecture, policies and processes in order to implement strategies that bridge these gaps.

MOVING TO THE CLOUD AND A CONTINUOUS MONITORING STRATEGY

When an organization moves a workload to the cloud, the security requirements of that workload have not changed. However, the organization no longer has complete control over that workload. As such, organizations should reassess their security controls with respect to the Service Level Agreement (SLA) with the cloud provider.

Guidance from the Cloud Security Alliance (CSA) calls for a concerted continuous monitoring effort of a cloud provider's environment, operations, and governance-related activities, such as updating information security. The CSA advises implementing a systematic vulnerability scanning and mitigation program for provider systems and networks, and continuously monitoring for data protection and unauthorized activities in the cloud. For organizations using a public cloud provider, it is the provider's responsibility to monitor its own log data (e.g., host audit logs, firewall logs). Understanding the provider's policies and establish alerting criteria and procedures is critical.

With the predicted growth in cloud adoptions over the next few years, it is important to develop a continuous monitoring program with the cloud in mind. In the U.S. federal government, continuous monitoring requirements are the same for federal agencies and any external service providers (e.g., cloud service providers) used by the agencies. To receive reauthorization of a Federal Risk and Authorization Management Program (FedRAMP) security authorization from year to year, cloud providers must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable.

Implementation Guidelines

Continuous monitoring is most effective when implemented as part of a comprehensive enterprise-wide risk management approach.

STEP 1 – UNDERSTAND THE ENTERPRISE

You cannot protect what you cannot see. Consequently, the first step of continuous monitoring is to gain a thorough understanding of what makes up your hybrid cloud environment. This includes connected devices, network infrastructure, virtualized assets, cloud connectivity, partner and gateway connectivity, and network perimeter boundaries. Without a clear understanding of the components that make up the enterprise, a continuous monitoring program will struggle to be successful.

The SANS Institute defines practical suggestions for implementing a process of continuous monitoring and other top defenses for protecting technology systems. These recommendations have been released in the form of the Consensus Audit Guidelines (CAG), published under the title: Twenty Critical Security Controls for Effective Cyber Defense.⁶ Control 1, for example, defines the need for an inventory of authorized and unauthorized devices as a first step in preventing attackers from exploiting new and unprotected systems attached to the network.

STEP 2 – DESIGN FOR AUTOMATION IN CONTINUOUS MONITORING

A continuous monitoring program applies automation to the assessment of defenses, with a clear focus on proactive risk management, ahead of any attacks. Through the use of automation, IT professionals can:

- Monitor a greater number of security controls on an ongoing basis and with increased frequency
- Ensure that they have not been negatively impacted by changes to the infrastructure
- Provide senior management with an essential, up-to-date security status
- Allow for immediate, cost-effective, risk-based decisions about their information systems

Automated processes, including the use of automated support products (e.g., vulnerability scanners, network scanning devices), can make the process of continuous monitoring more cost-effective, consistent, and efficient. Real-time monitoring of controls using automation can provide an organization with a much more dynamic view of its security state.

Automated products recognize patterns and relationships, such as:

- Verifying technical settings on individual network endpoints
- Ensuring that the software on a machine conforms to organizational policy
- Addressing advanced persistent threat (APT)

⁶ www.sans.org/critical-security-controls

Automation serves to augment the security processes conducted by security professionals within an organization and reduces the amount of time a security professional spends on redundant tasks. In addition, automation supports collecting more data, more quickly and can therefore make comprehensive, ongoing control of information security practical and affordable.

STEP 3 – IDENTIFY TECHNOLOGIES FOR ENABLING CONTINUOUS MONITORING

There are a variety of technologies available that an organization can use to efficiently and effectively gather, aggregate, analyze and report data. They provide visibility into the information assets, awareness of threats and vulnerabilities, and status of security control effectiveness. Continuous monitoring supports a variety of organizational processes, including but not limited to:

- Ongoing assessments of security control effectiveness
- Reporting of security status at the appropriate level of granularity to personnel with security responsibilities
- Management of risk and verification and assessment of mitigation activities
- Assurance of compliance with high-level internal and external requirements
- Analysis of the security impact of changes to the operational environment

TECHNICAL CONSIDERATIONS FOR CONTINUOUS MONITORING

There are three approaches to continuous network monitoring techniques: active, passive, and hybrid active/passive.

Active continuous network monitoring techniques function independently of other network management and security assessment products. They probe for information about the network topology, connected hosts, devices and services. Active monitoring techniques are generally accepted as more comprehensive (a greater reach to the endpoints), while generally lacking in detail.

Passive continuous network monitoring techniques are highly effective at real-time detection and at gathering deep levels of host information. The majority of passive monitoring techniques rely on devices to participate within traffic flow on the network, which allows them to sense the traffic a device emits before they can begin to gather data about those devices. While these techniques have the real-time and deep-dive advantages, it is generally accepted that passive monitoring techniques provide less visibility.

Cyber situational awareness requires a hybrid active/passive continuous monitoring approach to produce real-time visibility. Hybrid active/passive continuous monitoring methodologies allow for a real-time discovery of the infrastructure across the entire network. This real-time network visibility offered through passive techniques is continuously tuned by what the active component probes on the network, ensuring that the deep dark corners of the network do not go unexplored.

FireMon and Continuous Monitoring

FireMon offers an industry-pioneering hybrid approach to active/passive continuous, always-on monitoring. This hybrid active/passive discovery offers comprehensive hybrid cloud visibility coupled with real-time, instant discovery of the dynamic enterprise.

HYBRID ACTIVE/PASSIVE

FireMon Lumeta includes a passive monitoring, sensing and analysis technology that participates in the network. It utilizes non-disruptive network discovery to obtain real-time information on routing changes across large-scale networks. Continuous monitoring provides a clear picture of the network security state at any given time, while providing a mirror of control effectiveness over time. Lumeta maintains historical, passively collected network intelligence, and uniquely analyzes this information against network norms and policies. Components requiring additional analysis are probed through a hybrid active network discovery engine for further assessment of devices participating in routing changes.

Effective cyber situational awareness requires broad coverage to gather and correlate the high volume of data about the network itself, its routers and routes, as well as device profiles. Scouts facilitate accurate and complete depth-of scanning on complex, distributed global networks. Lumeta provides the flexibility to address network discovery, topology mapping, and network leak discovery in real-time even as networks change and new connections or devices are added. Particularly in this age of BYOD and IoT, detecting new devices on the network and changes to the network topology as they happen allows for proactive defense and intrusion detection.

ZONES

Lumeta allows for the creation of zones to allow an organization to segment continuous compliance monitoring of network access controls for compliance with regulatory and internal information security policies. Zones can be as simple or as complex as defined by an organization and can be comprised of logical networks and subnets, regardless of where they are physically deployed around the world.

ANALYTICS AND VISUALIZATION

A security management dashboard consolidates and communicates relevant security status in real-time, translating raw technology feeds into actionable information and alerts for events that require immediate action. The dashboard presents information in a meaningful and easily understandable format that can be customized to provide the appropriate information to users with specific roles and responsibilities within the organization.

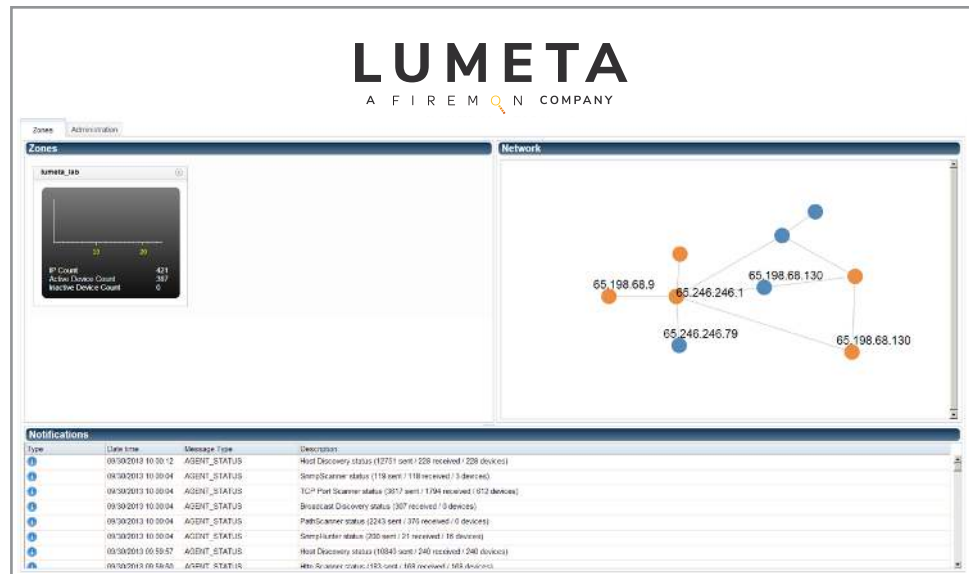


Figure 3: Lumeta continuously monitors network connections and devices. Data is displayed on a single executive dashboard. Lumeta provides the real-time visibility and flow analysis required to fully understand and respond to changes taking place in the network.

SITUATIONAL AWARENESS THROUGH INTEGRATION

It is crucial to understand comprehensively the dynamic state of the network. This information is foundational intelligence for an effective continuous monitoring program.

Through integration, this foundational intelligence can be provided to technologies including:

- Security Incident and Event Management (SIEM)
- Vulnerability Management
- IDS/IPS
- NAC
- Flow data analysis tools
- Network metadata, packet capture and analysis tools
- Network forensics

Lumeta Technology Partner Integrations

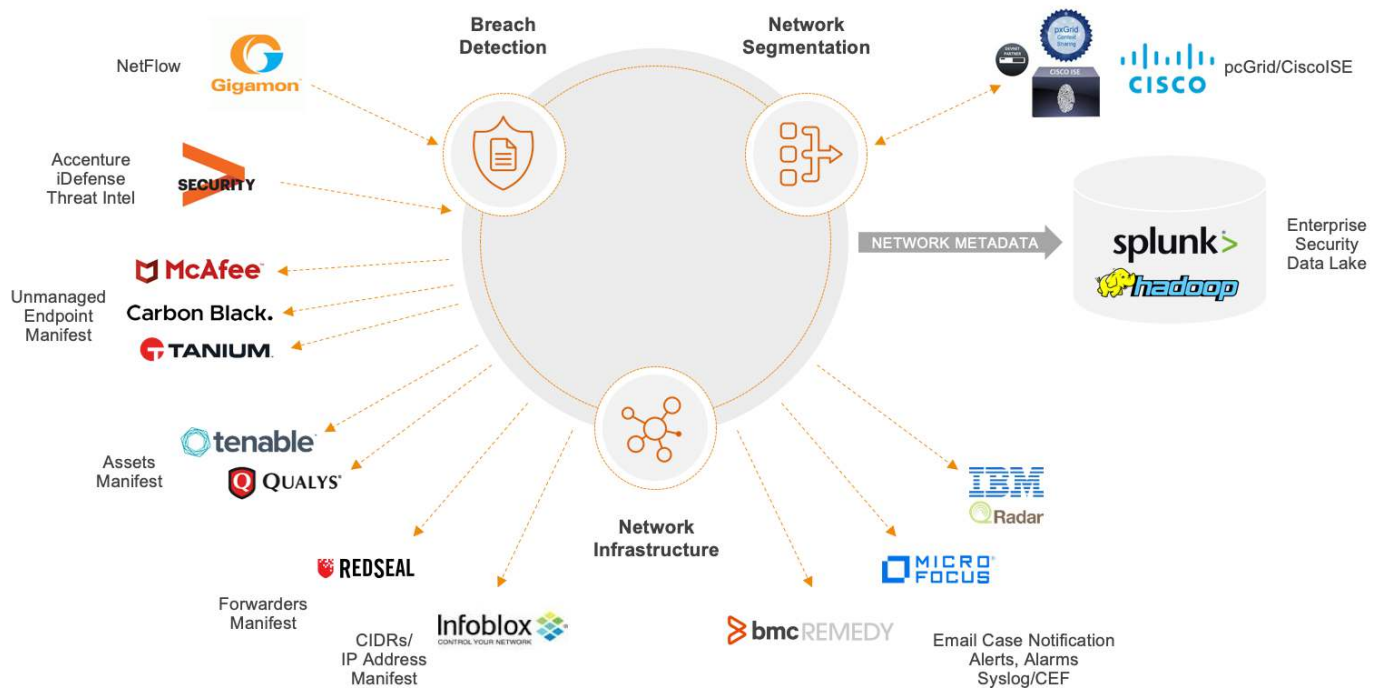


Figure 4: Lumeta is a necessary foundation for continuous monitoring and comprehensive cyber situational awareness. It integrates with an organization's existing products, such as VM, SIEM and NAC. Network, security and compliance products can only be fully effective when operating with 100% network visibility.

Continuous monitoring using Lumeta provides a complete view of network assets and connections to monitor network availability and assess business impact due to network changes. Lumeta is an effective means for both data capture and data analysis to support real-time, risk-based decision making.

Conclusion

In today's environment of widespread cyber-intrusions, advanced persistent threats and insider threats, it is essential to have real-time and complete visibility throughout hybrid networks. This allows for a swift response to external and internal threats.

Sophisticated attackers continue to exploit the weakest controls. Enterprises need to conduct continuous monitoring to determine the security posture of systems and the organization at any given moment.

The ongoing support of business functions requires organizations to constantly alter their network security environments and device settings, creating the potential for new points of risk. As a result, it's crucial for organizations to maintain constant visibility into their security standing to verify that they haven't opened a back door that could allow attackers to access protected mission-critical information or systems.

Continuous monitoring is a risk management approach to cyber situational awareness that maintains a picture of an organization's security risk posture and provides visibility into assets, which is critical for organizations with a BYOD and/or IoT policy. Automated data feeds allow IT professionals to quickly quantify risk, ensure effectiveness of security controls and implement prioritized remedies.

Organizations of all sizes should consider a comprehensive continuous monitoring strategy to decrease risk. A continuous monitoring program helps to ensure that deployed security controls continue to be effective and operations remain within stated organizational risk tolerances, in light of the inevitable changes that occur over time. In cases where security controls are determined to be inadequate, continuous monitoring programs facilitate security response actions based on risk.

Continuous monitoring is most effective when automation techniques are employed for data collection and reporting. By implementing technologies that automate continuous monitoring activities, organizations can make more effective use of their security budgets.

FireMon provides complete, real-time visibility throughout the hybrid enterprise to power continuous cyber situational awareness.

About FireMon

FireMon delivers continuous security for hybrid enterprises through a powerful fusion of vulnerability management, compliance and orchestration. Since creating the first-ever network security policy management solution, FireMon has continued to deliver visibility into and control over complex network security infrastructures, policies, and risk postures for more than 1,700 customers around the world. For more information, visit www.firemon.com.

