

FirstWave

NMS Security Architecture Considerations & Approaches

Whitepaper by

Anthony Kirkham

Principal Consultant, Neon Knight Consulting



Table of Contents

01	Introduction	
02	Defining the Problem	4
03	Where do we start?	4
	Mitigation Strategies to Prevent Malware Delivery and Execution	5
	Mitigation Strategies to Limit the Extent of Cyber Security Incidents	5
	Mitigation Strategies to Recover Data and System Availability	5
04	A Quick Word on Security Policy	6
05	Security Visibility	6
06	High-Value Security Visibility	6
	Engage Continuous Monitoring	6
07	Raise the Bar – Security Analytics	7
08	Aligning with Zero Trust Architectures	7
	Endpoint Detect and Response	9
	Other Practical Suggestions	10
09	Out-of-Band Management (OOB)	10
10	SNMP v3 Usage	11
11	Conclusion	11



NMS Security Architecture Considerations & Approaches

The SolarWinds compromise became public in December 2020 and was a massive wake up to the industry. Likely a state-sponsored attack, it compromised potentially thousands of governments and other high-profile organisations across the globe. Many organisations are currently in damage control following the breach. Many of them are unsure if the perpetrators have entered, spread and are still persistent within their environment - even after they shut down the SolarWinds Platforms.

The incident itself was complex and involved a sophisticated malware (SUNBURST) planted via a supply-chain attack. While some information on the attack's approach is clear, other elements are not fully understood. Many highly credible and technically capable organisations have to-date provided detailed coverage of the known facts. It is not the intent of this article to attempt to repeat that coverage.

The purpose of this article is to provide some practical guidance on securing Network Management systems and associated infrastructure. While it can't make any guarantees of absolutely protecting from similar attacks in the future, implementing these approaches can make the job of an adversary significantly harder. It will also propose techniques for increasing the probability of detecting breaches, which should be a significant consideration within any security solution.

This article cannot provide exhaustive coverage. However, it will focus on delivering actionable guidance that will have a tangible impact in strengthening the Network Management's security posture (and potentially other) Systems.

Defining the Problem

Network Management Systems (NMS) have tendrils whose reach is far and wide, touching many systems throughout an organisation. Many of these may be high-value systems, including the highly critical network infrastructure itself. NMSs often have privileged credentials (such as Service Accounts) stored within them.

For this reason, NMSs themselves are a high-value target. A compromised NMS has a high potential be used to gain access into managed endpoints and, often closely coupled administrative systems. NMS is an ideal foothold for an attacker to begin lateral movement.

Given both the potential reach and the possibly privileged access, utilising both an appropriate security architecture, coupled with the relevant security controls, is recommended as a critical initiative.

Where Do We Start?

Answer – With the fundamentals.

Time and time again, compromises succeed and malware spreads because fundamental security practices are not adequate. Of critical importance, Organisations must initially focus on strong Security Fundamentals.

FirstWave provides its products as either a Virtual-Machine platform or as an installable package that is supported on a several common Linux Distributions. The VM platform is shipped on a current Linux build with only the necessary services enabled. Following deployment, it becomes the customer's responsibility to keep the build updated with appropriate security patches, etc.

There are many sources that discuss fundamental Linux OS security practices at length. For example, NIST and the Centre for Internet Security (CIS).

It is worth emphasising some of the baseline principals that significantly and positively impact any platforms overall Security Posture. An excellent reference is the 'Essential Eight', published by the Australian Signals Directorate. Seven of the eight Security Controls are directly relevant to the security of a Linux based system such as NMIS. While this is an Australian Government publication, the principals and supporting material are globally relevant.

Learn about 'The Essential Eight' [HERE](#).

While somewhat focused on User Systems, the 'principals' are equally applicable to server platforms. These security controls fall into three categories, in summary;

Mitigation Strategies to Prevent Malware Delivery and Execution

- Application control to prevent the execution of unapproved/malicious programs
- Patch applications
- User application hardening

Mitigation Strategies to Limit the Extent of Cyber Security Incidents

- Patch operating systems
- Restrict administrative privileges to operating systems and applications based on user duties
- Multi-factor authentication for all users, particularly when they perform a privileged action

Mitigation Strategies to Recover Data and System Availability

- Daily backups of important new/changed data, software and configuration settings.



A Quick Word on Security Policy

While this article focusses on many technical controls, these must be supported within a robust and over-arching Security Policy. For any security initiative to be effective, senior management must understand the risks, actively support and encourage the initiative.

Security Visibility

If there was one thing that was clear from the SolarWinds compromise, despite the significant number of affected organisations, no one appeared to have detected the anomalous beacons associated with the Sunburst malware!

One of the most important concepts within security is that of 'Visibility'. It comes in many forms depending on the context. Network Management itself is a form of Visibility, as are many varieties of logs and the output of security tools, including Intrusion Detection Systems (IDS).

High-Value Security Visibility


Within an NMS context, the following tools or techniques can be used to provide high value in improving the security posture through Visibility.

- An Agent-Based – Endpoint Detect and Response (EDR) solution, installed on the NMS server itself. EDR provides Visibility inside the system at an OS level. Two current examples include CrowdStrike and Cisco's AMP for Endpoints.
- Next-Generation Firewall based Traffic Monitoring. Two examples include Palo Alto Networks NGFWs and Cisco Firepower Threat Defence. Both have additional inspection capabilities such as Intrusion Prevention, Network Anti-Virus and Day-Zero Malware inspection.
- Storing and retaining Logging. FirstWave offers the opEvents product, which provides the additional capability of analysing log information. It can alert and or take action on many types of security alerts.

Engage Continuous Monitoring

There is a sad reality across the industry of very poor statistics surrounding the time it takes organisations to detect internal compromises (known as the Dwell Time). Commonly detection times are in the order of many, many months, if at all. Very often, it is an outside organisation that raises the alert of a compromise.

The key point and recommendation is that unless your organisation is entirely confident, it has the resourcing and expertise to perform a continuous monitoring function, then engage an external firm.



These days it is essential to work on the premiss that your organisation will be breached at some time.

You must be prepared for that eventuality! Quick detection may be the difference between being able to respond quickly and effectively, or, incurring a severe business and reputational impact.

Raise the Bar – Security Analytics

As noted previously, it did not appear that any organisation actually detected the anomalous network traffic associated with the Sunburst Malware. When sophisticated classes of attack are involved, the detection strategies need to be raised to the next level. Achieving that requires the use of specialist Analytics platforms.

There are currently several vendors who can provide this capability – Two include Awake Security (now part of Arista Networks) and Darktrace.

Aligning with Zero Trust Architectures

The concept of Zero Trust Architectures (ZTA) has been in existence for around a decade now and has significantly risen in profile over the last few years. Fundamentally Zero Trust (ZT) is about restricting unnecessary Trust Relationships.

The creators of Zero Trust have argued that loose or open trust relationships of various forms have allowed many intrusions to occur and then propagate throughout an organisation initially.

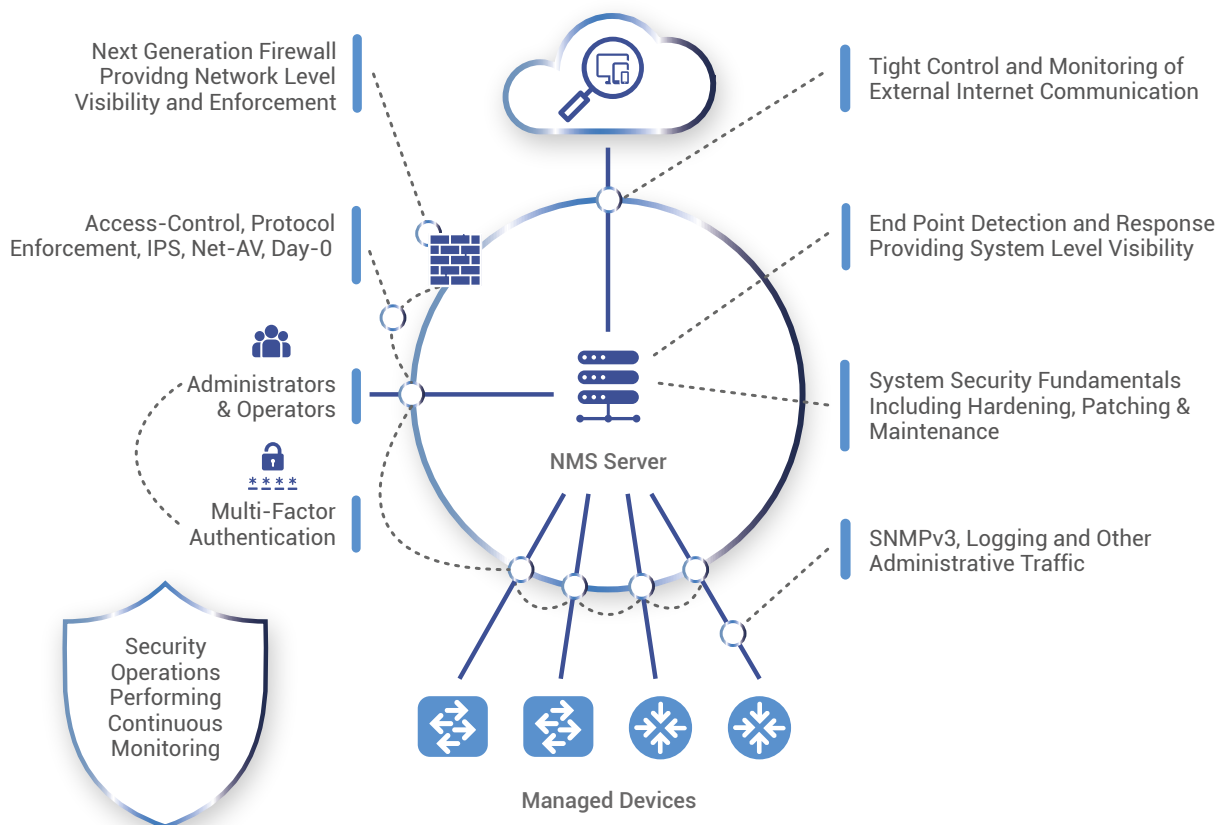
“Never Trust, and Always Verify”.
The Zero Trust Architecture.

Within the context of securing Network Management, there are two key elements of ZTA that are particularly relevant.

These are;

- Robust Identity – Using a variety of security techniques, including Certificates, robust credential management, Multifactor Authentication, etc. to ensure that users or other systems (or even applications) are who they claim to be.
- Restricted Network Access – Restricting access and communication between systems to only what is necessary and validating those traffic flows as legitimate and non-malicious.

It is the fact that many NMS deployments have some type of trust relationship with just about everything in the network that makes them such an attractive target.



Translating the above into practice generally means combining a Next-Generation Firewall (NGFW) and a Two (or Multi) Factor Authentication solution (particularly for privileged operations). NGFWs provide many security features which can be used to help secure an NMS and associated systems. Placing an NMS within



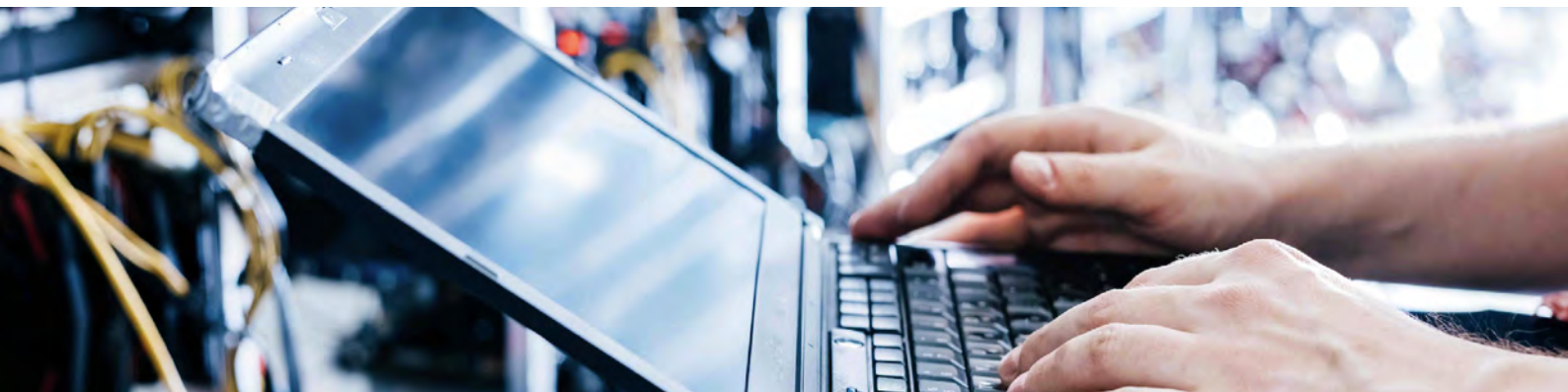
the confines of NGFW protection, isolates it and tightly controls traffic to and from the platform. For example, Application ID can provide detailed visibility of the applications traversing the network and enforce protocol compliance by determining if the traffic on ports 161 and 162 is actually SNMP or something nefarious.

Integrated Intrusion Prevention Systems (IPS) and Network Anti-virus can block exploitation attempts and malware in transit across the network. User Identity integration can provide various access levels based on a user's identity and role in the organisation (not just their IP address).

Endpoint Detect and Response

Endpoint Detect and Response (EDR) solutions can monitor and provide Visibility into an endpoint's system-level behaviour. EDR solutions typically use sophisticated techniques to detect suspicious system behaviour, provide contextual information, and block malicious activity. In some respects, EDR can be thought of within a ZT context as it serves to increase

An EDR solution installed on the NMS Server will provide high-level internal Visibility that cannot be gained with other approaches alone. A 'Managed' EDR solution can ensure that an operator is actioning suspicious behaviour. As such, Managed EDR is a strong recommendation.



Other Practical Suggestions

If your organisation is on a tight budget, two practical things can be done.

1. Limiting external communications.

It is the reality that any system today will require some external communication via the Internet for activities such as downloading updates and other system maintenance activities. The only alternative is a 'swivel chair' approach which is often used in high-security environments. The key point is that while some communication will be legitimate, those destinations should be known, monitored and controlled.

In the case of the Sunburst malware, if outbound communication was limited to the small number of essential Internet destinations, it would not have been possible for the Sunburst malware to 'call home' to the Command-and-Control (C&C) systems.

2. Limiting DNS resolution

Today all quality firewalls provide the ability to construct rules based on a Fully Qualified Domain Name (FQDN) to limit DNS resolution to a set of known domains. It is also easy to log any failed attempts outside of those in the permitted list. For instance, DNS logs are incredibly useful in performing forensics or security investigations.

Out-of-Band Management (OOB)

OOB is an architectural technique that has been used within Telecommunication and Service Providers for many years. Essentially these networks separate the Data and Management Planes, avoiding the ability for Data plane and User/Subscriber traffic being able to reach the management interfaces of the infrastructure.

To a lesser extent, OOB based management has been used within Enterprise networks. As the threat landscape has grown over the last several years and the criticality of the supporting infrastructure increased, OOB Management's use is an architectural approach that should be seriously considered. From a risk perspective, it isolates critical management interfaces and makes it far harder for a foothold gained on a user's system (which is very common) to subsequently gain access to critical management systems and vice versa.





SNMP v3 Usage

Products supporting SNMPv3 started appearing in approximately the 1997 timeframe to overcome security weaknesses in the then prevalent SNMPv2 protocol. 'yes', that's well over 20 years ago. While there were practical issues with the cryptographic overheads involved in SNMPv3, those have been long overcome and there are few legitimate excuses for not using SNMPv3 today.

Any possible weakness that can be closed, from a security perspective provides one less vector that can be exploited should an adversary gain a foothold inside an organisation.

SNMPv2 in Read-Write mode should never be used as attacks leveraging the protocol's weakness and very commoditised and widely taught in infrastructure hacking courses. security tools, including Intrusion Detection Systems (IDS).

Conclusion

In conclusion, many things can be done to significantly increase the Security Posture of a Network Management System within an organisation. There are numerous others that go beyond what could be described in a short article. Organisations must understand their risks and deploy appropriate security controls to mitigate those. The SolarWinds attacks have shown the bar has been raised significantly, which requires increased security to manage the potential organisational and business risk.



Anthony Kirkham

Principal Consultant, Neon Knight Consulting

Tony has over 20 years experience in Network Engineering and Security covering the design, deployment and operations of both large-scale Enterprise and SP/Telco networks.

He authored numerous white papers on both network design and security design, including RFC 6752 (IETF).

Tony has a deep and current (circa 2021) understanding of "How networks get broken into" and the design approaches and control frameworks which can be deployed to minimise the risk of these security incidents.

Industry Certifications: Cisco CCIE R&S, ISC2 CISSP, Palo Alto Networks CNSE.

FirstWave

If you'd like some guidance around NMS Security Architecture Considerations and Approaches, or If there's a specific issue you're trying to solve in your network environment - click below to request a demo

[Book a demo](#)



FirstWave

Our passion is to create intelligent software that our service provider partners and customers love.

Get Expert
Solutions

Book a demo

FirstWave is a publicly-listed, global technology company formed in 2004 in Sydney, Australia. FirstWave's globally unique CyberCision™ platform provides best-in-class cybersecurity technologies, enabling FirstWave's Partners, including some of the world's largest telcos and managed service providers (MSPs), to protect their customers from cyber-attacks, while rapidly growing cybersecurity services revenues at scale.

In January 2022, FirstWave acquired Opmantek Limited (FirstWave), a leading provider of enterprise-grade network management, automation and IT audit software, with 150,000 organisations using their software across 178 countries and enterprise clients including Microsoft, Telmex, Claro, NextLink and NASA.

Integrating CyberCision™ with FirstWave's flagship Network Management Information System (NMIS) and Open-Audit product enables FirstWave to provide a comprehensive end-to-end solution for network discovery, management and cybersecurity for its Partners globally.

With over 150,000 organisations now using FirstWave technology, we are well positioned to be a leader of transformational change in the IT Operations and Cybersecurity world.