Monitoring Tool

SolarWinds

Comprehensive Analysis

Understanding SolarWinds

SolarWinds is a suite of network and IT infrastructure monitoring and management tools. It offers a wide array of modules within its Orion Platform. Here's a breakdown of key areas and use cases:

Monitoring Capabilities & Functionalities

- **Data Collection:** SNMP, WMI, syslog, agents, APIs, etc.
- **Visualization:** Dashboards, charts, maps, customizable reports, etc.
- **Alerting:** Threshold-based, intelligent baselining, various notification methods.
- **Integrations:** With ticketing systems, CMDBs, other IT tools, etc

Licensing

- **Subscription-based:** Common for most modules.
- **Pricing Factors:** Number of nodes/elements monitored, specific modules, support levels.
- **Contact SolarWinds for quotes:** They'll tailor pricing to your needs.

Customization

- **Alerts:** Highly customizable thresholds and complex trigger conditions.
- **Reports:** Creation of custom reports and dashboards.
- **Scripting:** Some API access and scripting capabilities for automation.

Customer Success Stories

- **Refer Official documentation**

When SolarWinds May NOT be Ideal

- **Cost:** Can be expensive for large, complex environments.
- **Smaller Networks:** Might be overkill if your needs are basic.
- **Open-Source Preference:** Alternatives like Zabbix/Nagios exist.

Performance Metrics

- **Availability/Uptime:** Overall network and individual device uptime.
- **Response Times:** Application/network latency, page load times, etc.
- **Alerts:** Time to acknowledge, time to resolve issues.
- **Data accuracy:** Matching with other monitoring sources

KPIs for Tool Usage

- **Adoption Rate:** # users actively using the tool.
- **Alert Volume vs. True Positives:** Efficiency of alerting configuration.
- **Ticket Reduction:** Related to identified problems proactively fixed.

Additional Benefits

- **Proactive Problem Solving**
- **Capacity Planning**
- **Compliance Adherence**
- **Improved IT Efficiency**

SolarWinds – Features

Comprehensive Use Cases – Category A

1. **Network Performance Monitoring (NPM):** Real-time network visibility, traffic analysis, fault detection, bandwidth monitoring, hop-by-hop path analysis.
2. **Server & Application Monitoring (SAM):** Hardware health, operating system metrics, application performance & uptime monitoring (physical and virtual servers).
3. **Database Performance Monitoring (DPA):** Tracks database performance, identifies bottlenecks, optimizes queries across various database types (SQL Server, Oracle, MySQL, etc.)
4. **Web Performance Monitoring (WPM):** End-user experience testing, website uptime checks, synthetic transactions simulating user actions on web applications.
5. **Configuration Management (NCM):** Backup/restore network device configurations, compliance auditing, change detection.
6. **IP Address Management (IPAM):** Centralized IP address tracking, subnet allocation, DHCP and DNS management.
7. **Security Event Manager (SEM):** Log collection, correlation, threat detection, real-time security alerts.
8. **NetFlow Traffic Analyzer (NTA):** Deep packet inspection, bandwidth usage analysis, identification of traffic anomalies.
9. **Virtualization Monitoring (VMAN):** Visibility into virtualized environments (VMware, Hyper-V etc.), resource optimization, capacity planning.
10. **Storage Resource Monitor (SRM):** Storage capacity and performance monitoring across storage arrays from various vendors.

Comprehensive Use Cases – Category B

1. **Log & Event Manager (LEM):** Comprehensive log management, event correlation, compliance reporting, and threat analysis
2. **Service Desk:** ITIL-based Help Desk ticketing, asset inventory, knowledge base, problem and change management.
3. **User Device Tracker (UDT):** Tracks and monitors endpoint devices (laptops, desktops, mobile) connected to your network.
4. **Bandwidth Analyzer Pack (BAP):** Combines NPM and NTA for a complete picture of network bandwidth usage.
5. **Voice Quality Manager (VQM):** Monitors VoIP call quality and troubleshoots performance issues.
6. **Patch Manager:** Automated patching of Windows systems and third-party applications.
7. **Network Topology Mapper (NTM):** Automatic network discovery and mapping.
8. **Cloud Monitoring:** Monitoring of resources in Azure, AWS, and hybrid environments
9. **Network Insight (for Cisco ASA, F5 BIG-IP, etc):** Deep visibility and performance insights into specific network devices
10. **Access Rights Manager (ARM):** Monitors and controls user access permissions to files, folders, and critical systems. .

Network Performance Monitoring (NPM)

- **Traffic Anomaly Detection:** Identifying unusual traffic patterns potentially indicating security incidents or misconfigurations.
- **QoS Monitoring:** Ensuring traffic prioritization for critical applications (voice, video, etc.).
- **BGP Route Monitoring:** Tracking BGP routing changes and stability for internet connectivity.
- **WAN Link Optimization:** Identifying underutilized WAN links to balance traffic.
- **Wireless Network Troubleshooting:** Detailed analysis of Wi-Fi interference, channel overlaps, and rogue access points.
- **NetPath Analysis:** Visualizing end-to-end network paths for applications, pinpointing bottlenecks beyond your own network (e.g., at ISPs).
- **Vendor-Specific Device Monitoring:** Using Network Insights for deep visibility into Cisco, F5, Palo Alto, etc.
- **Bandwidth Hog Identification:** Finding specific devices or users consuming excessive bandwidth.
- **Detailed Interface Error Tracking:** Monitoring for discards, CRC errors, input/output queue drops on interfaces.
- **Microburst Detection:** Catching short-lived traffic spikes that impact apps but might be missed by standard polling.
- **Capacity Forecasting:** Baselining network usage to predict future bandwidth needs and prevent congestion.
- **Voice & Video Performance:** Monitoring jitter, packet loss, and MOS score for VoIP/video quality.
- **SD-WAN Monitoring:** Visibility into performance and overlay paths in software-defined WAN setups
- **IP SLA Monitoring:** End-to-end measurement of voice and network service quality.

Server & Application Monitoring (SAM)

- **Hardware Failure Prediction:** Analysing SMART data on disks, predictive fan failures, etc.
- **Process Monitoring:** Ensuring critical business processes are running, with restart capabilities.
- **Custom Application Monitoring:** Creating monitors for in-house applications via scripting or templates.
- **Windows Service Monitoring:** Tracking the state and availability of essential Windows services
- **Linux Daemon Monitoring:** Ensuring the stability of background processes on Linux servers.
- **Certificate Expiration Monitoring:** Alerts for certificates on servers and network devices.
- **Detailed Storage Metrics:** IOPS, latency, array health on storage devices.
- **VM Sprawl Identification:** Tracking unused or underutilized virtual machines for optimization.
- **Hardware/Software Inventory:** Maintaining up-to-date information on assets across the environment.
- **Dependency Mapping:** Understanding component relationships for applications, aiding change control.

Database Performance Monitoring (DPA)

- **Wait-Time Analysis:** Pinpointing the exact bottleneck in SQL queries (disk I/O, locking, CPU, etc.).
- **Index Advisor:** Recommendations for improving database performance by adding or changing indexes.
- **Blocking & Deadlock Analysis:** Monitoring chains of locked processes that impact database performance.
- **Long-Running Query Identification:** Finding poorly optimized queries that hog database resources.
- **Table Tuning:** Identifying tables that need additional tuning, archiving, or partitioning.
- **Database Anomaly Detection:** Identifying performance patterns that deviate from the norm.
- **Cross-Platform Support:** Monitoring a mixture of database types (SQL Server, Oracle, MySQL, PostgreSQL, etc.).

Web Performance Monitoring (WPM)

- **Transaction Recording:** Script user actions (login, shopping cart) for ongoing performance testing.
- **Multi-Step Web Transactions:** Simulate complex user journeys across multiple pages of applications.
- **Global Monitoring:** Checking performance from various geographic locations to identify regional issues.
- **Content Validation:** Ensuring correct page elements and text are displayed to the end-user.
- **Real Browser Monitoring:** Testing performance on real browsers (Chrome, Firefox, etc.) rather than just emulations.
- **Third-Party Content Monitoring:** Identifying slow-loading external elements (ads, analytics) impacting the overall page experience

Detailed Use cases

Network Configuration Manager (NCM)

- **Automated Configuration Backups:** Regular backups of network device configurations for disaster recovery.
- **Bulk Configuration Changes:** Pushing changes to multiple devices simultaneously, saving time.
- **Configuration Change Auditing:** Tracking who made changes, when, and what the changes were.
- **Compliance Policy Enforcement:** Automated checks for configurations adhering to standards (PCI-DSS, HIPAA, etc.).
- **Firmware Rollout & Vulnerability Tracking:** Manage firmware updates and identify vulnerable firmware versions
- **Network Inventory Reporting:** Detailed reports on network devices, firmware versions, and configurations
- **Script-Based Remediation:** Trigger scripts or actions based on detected configuration deviations

IP Address Manager (IPAM)

- **IP Conflict Detection:** Alerts when duplicate IP addresses are assigned.
- **Subnet Utilization Tracking:** Visualizing free vs. used IP space to aid capacity planning.
- **Centralized DHCP & DNS Management:** Managing these services from a single console for consistency.
- **Historical IP Tracking:** See which devices had specific IPs in the past, useful for audits and troubleshooting.
- **Integration with Virtualization:** Tracking IP allocation within virtual environments (VMware, Hyper-V).
- **IP Request Workflow:** Manage IP address requests and approvals with built-in processes.

Security Event Manager (SEM)

- **Log Aggregation:** Centralized collection of logs from firewalls, servers, switches, etc.
- **Real-time Threat Detection:** Active correlation rules to identify security events as the logs come in.
- **User Activity Monitoring:** Tracking logons, file access, privilege changes, and other user behavior anomalies.
- **Forensic Analysis:** Detailed search and filtering of log data for investigations.
- **Compliance Reporting:** Pre-built reports for various regulations (PCI, HIPAA, SOX, etc.).
- **USB Device Monitoring:** Alerts and auditing on USB storage device usage.
- **Integration with Threat Intelligence Feeds:** Enriching log data with external threat information.

Use Cases (NTA. VMAN, SRM)

NetFlow Traffic Analyzer (NTA)

- **Distributed Denial of Service (DDoS) Attack Identification:** Detect abnormal traffic surges and source IPs.
- **Suspicious Conversation Tracking:** Analyze traffic patterns of internal IPs communicating excessively with external ones.
- **Peer-to-Peer Traffic Analysis:** Identify P2P file-sharing applications on your network.
- **NetFlow Export Monitoring:** Monitor devices sending NetFlow data to ensure proper collection.
- **Source/Destination AS (Autonomous Systems) Tracking:** Gain insights into traffic exchanged across internet providers.
- **Application Response Time Analysis:** Break down network time vs. server-side processing time for apps.

Virtualization Monitoring (VMAN)

- **VM Right-Sizing Recommendations:** Identify over/under-provisioned VMs based on resource usage.
- **Sprawl Detection:** Find abandoned or rarely used VMs for cleanup and optimization.
- **Host Capacity Planning:** Project when physical hosts will reach capacity based on VM growth trends.
- **Cross-Vendor Support:** Monitor VMware vSphere, Hyper-V, and Nutanix environments in a single view.
- **Storage I/O Contention Tracking:** Identify VMs impacting datastore performance.
- **Snapshot Monitoring:** Track snapshot age, size, and impact on datastore capacity.
- **VM Migration Tracking:** Historical records of VM migrations across hosts.

Storage Resource Monitor (SRM)

- **Vendor-Agnostic Monitoring:** Supports arrays from Dell EMC, NetApp, IBM, Pure Storage, and more.
- **Thin Provisioning Analysis:** Track over-allocation and potential space exhaustion on thin-provisioned volumes.
- **Predictive Capacity Alerts:** Estimate when storage pools or volumes will run out of space.
- **Performance Troubleshooting (LUNs, RAID groups):** Identify bottlenecks at different layers of the storage stack.
- **Historical Performance Trend Analysis** Helps with capacity planning and performance baselining.

Use cases...

Voice Quality Manager (VQM)

- **Call Path Analysis:** Visualize the network path traversed by specific VoIP calls.
- **Mean Opinion Score (MOS) Tracking:** Historical tracking to identify trends or problematic network locations.
- **Codec Analysis:** Determine the codecs used for calls and their impact on quality
- **SIP Call Monitoring:** Analyze SIP signaling to troubleshoot call setup and registration issues.
- **Voice Infrastructure Monitoring:** Monitor IP phones, VoIP gateways, and call manager servers for availability and errors.
- **Capacity Planning for VoIP:** Project bandwidth needs based on call volume and concurrent calls.
- **Troubleshooting Specific Calls:** Isolate and analyze performance metrics for single identified calls.

Patch Manager

- **Pre-Deployment Testing:** Test patches in a staging environment before production rollout.
- **Custom Patch Creation:** Package and deploy patches not available in SolarWinds' built-in catalog.
- **Offline Patching:** Support for devices not always connected to the network.
- **Dependency Mapping:** Understand dependencies between patches for successful deployment order.
- **Rollback Planning:** Have rollback procedures in place if patches cause issues.
- **Third-Party Application Patching:** Extend patching beyond just Windows operating systems.
- **Security Patch Prioritization:** Prioritize patches based on severity scores (CVSS).

Network Topology Mapper (NTM)

- **Scheduled Network Scans:** Regularly rediscover your network topology to capture changes.
- **Layer 2 and Layer 3 Mapping:** Map both switch port connections and routed connections.
- **Detailed Device Information:** Get hardware details, OS versions, and open ports for network devices.
- **Custom Icons and Backgrounds:** Upload your own icons for device types or floor plans for better visualizations.
- **Topology Export:** Export maps as images or Visio diagrams for documentation.
- **Dependency Visualization:** See how device outages might impact other connected systems.

Cloud Monitoring

- **Cost Analysis:** Track resource usage costs across cloud providers (Azure, AWS).
- **Resource Tagging:** Monitor costs by department, project, or other custom tags.
- **Right-Sizing Recommendations:** Identify underutilized resources for cloud cost optimization.
- **Security Posture Checks:** Monitor cloud configurations against security best practices.
- **Hybrid Environment Visualization:** Visualize dependencies between on-premises and cloud resources.
- **Performance Anomaly Detection:** Baseline cloud resource usage and alert on deviations.

Network Insight (for F5, Cisco, etc.)

- **F5 BIG-IP Deep Dives:** Performance metrics of virtual servers, pools, load balancer status, etc.
- **Cisco ASA Firewall Insights:** Firewall policy analysis, VPN tunnel monitoring, site-to-site connectivity checks.
- **Palo Alto Firewall Monitoring:** Security rule hit counts, session tracking, threat analysis.
- **Vendor-Specific Troubleshooting:** Get guided troubleshooting workflows based on the monitored device type.

Use cases - Modules

Access Rights Manager (ARM)

- **Share Permission Auditing:** Analyze excessive or misconfigured permissions on file shares.
- **Active Directory Permissions Reporting:** Visualize group memberships and effective permissions of AD users.
- **Critical Data Access Monitoring:** Alert on changes in permissions to sensitive folders or files.
- **Permission Change Simulation:** Preview the impact of permission changes before applying them.
- **Ownerless Data Identification:** Find files and folders without clear ownership for risk assessment.
- **Remediation Workflow:** Create approval flows for permission changes requests.

Log & Event Manager (LEM)

- **Windows Event Collection:** Centrally gather security, application, and system logs from Windows servers and workstations.
- **Log Collection from Syslog Sources:** Ingest Syslog messages from firewalls, routers, switches, Linux systems, etc.
- **Agentless Log Collection:** Gather logs via WMI or other protocols without installing software on monitored devices.
- **Custom Log Parsing:** Create rules to extract relevant data from non-standard log formats.
- **Active Response Triggers:** Initiate scripts, send emails, open tickets, or quarantine systems based on log events.
- **USB Device Usage Monitoring:** Track USB storage connection events and file transfers.
- **File Integrity Monitoring (FIM):** Detect critical file modifications on sensitive systems.
- **PCI DSS Compliance Reporting:** Pre-built reports tailored to PCI DSS log monitoring requirements.
- **HIPAA Compliance Reporting:** Reports demonstrating log collection, retention, and access controls for HIPAA audits.
- **GDPR Compliance Tracking:** Log access reports and user activity monitoring that supports GDPR needs.
- **NIST 800-53 Compliance Mapping:** Correlate log events to controls outlined in NIST security frameworks.
- **Log Retention & Archiving:** Configurable retention periods, and archiving options for long-term storage.
- **Threat Feed Correlation:** Enrich log data with external threat intelligence to highlight potential malicious activity.
- **Forensic Investigations:** Powerful search and filtering to drill into historical logs for incident investigations.
- **Log Normalization:** Transform logs from various formats into a normalized structure for easier analysis.
- **Behavior-Based Anomaly Detection:** Identify unusual user or system activity even without pre-defined rules.

Use cases - Modules

Service Desk

- **Ticket Prioritization:** Categorize tickets based on severity, impact, or service level agreements (SLAs).
- **Automatic Ticket Routing:** Assign tickets to specific teams or technicians based on defined criteria.
- **Ticket Escalation:** Define escalation paths and timeframes to ensure critical issues are addressed promptly.
- **End-User Self-Service Portal:** Allow users to submit tickets, search a knowledge base, and track resolution progress.
- **Asset Discovery & Tracking:** Link assets (laptops, software licenses, etc.) to tickets for better context.
- **Hardware & Software Inventory:** Maintain detailed inventory for audits and change management.
- **Problem Management Workflows:** Track recurring issues, root cause analysis, and implement permanent fixes.
- **Change Management Approvals:** Formalize change requests, risk assessments, and approval workflows.
- **CMDB Integration:** Bi-directional data exchange with a Configuration Management Database for greater IT visibility.
- **SLA Tracking & Reporting:** Measure service desk performance against service level agreements.
- **Customer Satisfaction Surveys:** Collect feedback upon ticket closure to gauge help desk effectiveness.
- **Vendor Management Integration:** Link tickets to external vendors for tracking and managing support contracts.

User Device Tracker (UDT)

- **Desktop & Laptop Inventory:** Detailed hardware and software information for Windows and macOS devices.
- **Mobile Device Tracking:** Monitor iOS, Android, and Windows Mobile devices connected to the network.
- **User Login History:** Track user logins, logouts, and session duration on monitored devices.
- **Software Installation Tracking:** Identify unauthorized or potentially unwanted software installations.
- **Software License Compliance:** Monitor software usage against purchased licenses to avoid overages or true-ups.
- **Device Location Tracking:** Geolocation for laptops (if enabled) to aid in recovery of lost or stolen devices.
- **Network Access Policy Enforcement:** Integrate with network access control (NAC) to quarantine non-compliant devices.
- **Active Directory User Association:** Link devices to their primary user based on Active Directory accounts.
- **Bandwidth Usage Tracking:** Identify network bandwidth hogs down to specific devices or users.
- **Endpoint Security Integration:** Augment security tools by providing device and user context.

Use Cases

Bandwidth Monitoring & Troubleshooting

- **Interface-Level Utilization:** Track bandwidth utilization by percentage, megabits-per-second, etc., on individual network interfaces.
- **Top Talker Identification:** Pinpoint the top bandwidth consumers by device IP, hostname, application, or user.
- **Historical Bandwidth Trends:** Analyze bandwidth usage patterns over hours, days, weeks, or months for baselining.
- **Burst Detection:** Catch short-lived traffic spikes often missed by standard polling intervals.
- **Capacity Planning:** Project bandwidth growth trends to proactively plan upgrades before congestion occurs.
- **Traffic Anomaly Detection:** Identify unusual traffic patterns that could indicate security incidents or network issues.
- **Traffic Shaping & QoS:** Apply bandwidth controls and prioritize critical applications (voice, video, etc.).
- **Network Misconfiguration Troubleshooting:** Spot configuration errors that lead to inefficient bandwidth use.
- **Application Traffic Analysis**
- **Application Identification:** Go beyond protocols; see bandwidth used by specific apps (Skype, YouTube, file-sharing, etc.).
- **Conversation Monitoring:** View source and destination IPs, ports, and total data transferred for network conversations.
- **Performance Troubleshooting:** Isolate slowdowns caused by the network vs. slow application server responses.
- **Cloud Application Visibility:** Monitor bandwidth consumed by SaaS applications (Office 365, Salesforce, etc.).
- **Unexpected Application Usage:** Detect unauthorized or non-business-critical applications draining bandwidth.
- **WAN Link Optimization:** Identify bandwidth-hogging traffic on expensive WAN links to optimize usage.

Flow Data Deep Dives (from NTA)

- **Protocol Analysis:** Break down traffic distribution by protocols (TCP, UDP, ICMP, etc.).
- **Source/Destination AS Tracking:** Analyze traffic patterns across internet providers (useful for peering issues).
- **Differentiated Services (DSCP/QoS):** Monitor and enforce QoS markings on network traffic.
- **TCP Retransmission Analysis:** Identify network segments or devices causing packet loss, impacting performance.
- **NetFlow Anomaly Detection:** Baseline normal NetFlow patterns to alert on unexpected deviations.
- **Suspicious Conversation Identification:** Track large data transfers from internal sources to unknown external IPs.
- **Distributed Denial of Service (DDoS) Attack Recognition:** Detect traffic surges aimed at overwhelming network resources.

CBQoS (Class-Based Quality of Service)

- **CBQoS Policy Creation:** Design traffic shaping policies based on application, protocol, IP address ranges, etc.
- **Policy Simulation:** Preview the effects of QoS policies before enforcement on the network.
- **Performance Monitoring:** Track how QoS policies impact the network and application performance.
- **QoS Reporting:** Demonstrate network traffic prioritization or compliance with Service Level Agreements.
- **Important:** Bandwidth Analyzer Pack's power comes from the combination of NPM's broad visibility and NTA's in-depth flow analysis

Additional Valuable Use Cases

•**Peer-to-Peer Traffic Control:** Identify and limit bandwidth usage by P2P file-sharing applications.
•**Rogue Device Detection:** Discover devices consuming bandwidth that aren't part of the managed network.
•**Internet Usage Monitoring:** Track employee web browsing activity and bandwidth consumed.
•**Cloud Migration Impact:** Measure bandwidth changes before and after migrating applications to the cloud.
•**Vendor SLA Verification:** Validate that network service providers are delivering contracted bandwidth.
•**Billing & Cost Allocation:** Generate usage reports to chargeback departments or customers based on bandwidth.
•**Security Incident Support:** Deep traffic data aids investigations of malware distribution or data exfiltration.

Business Scenarios

- **Scenario 1: Proactive Issue Resolution for a Critical Application**
- **Problem:** Slowdowns in a critical business app lead to lost productivity and customer complaints.
- **Modules Involved:** SAM, DPA, NPM, VMAN
- **Integration Flow:**
  - SAM detects high CPU usage on the application server.
  - DPA pinpoints a slow database query within the application code causing the bottleneck.
  - NPM shows network congestion on the link between the application and database servers.
  - VMAN reveals that the application server's virtual machine is resource-constrained.
- **Solution:** Armed with this data, IT can:
  - Work with developers to optimize the database query.
  - Upgrade the network link for increased bandwidth.
  - Provision more CPU/memory for the virtual machine.

- **Scenario 2: Rapid Response to a Security Incident**
- **Problem:** A potential data breach is suspected due to unusual network activity.
- **Modules Involved:** SEM, NTA, NCM, IPAM
- **Integration Flow:**
  - SEM triggers an alert on suspicious login attempts and file access from an unknown IP.
  - NTA confirms large data transfers out of the network and identifies the source system.
  - IPAM reveals the compromised system belongs to a specific user/department.
  - NCM checks reveal a recent, unauthorized configuration change opening a firewall port.
- **Solution:** IT team can:
  - Quarantine the affected system to prevent further spread.
  - Rollback the erroneous configuration change.
  - Trace user activity for forensic investigation.
  - Patch the vulnerability exploited in the attack.

Business Scenarios

- **Scenario 3: Ensuring Business Continuity During a Disaster**
- **Problem:** A hurricane threatens a data center, potentially causing extended downtime.
- **Modules Involved:** VMAN, SRM, Backup Exec
- **Integration Flow:**
  - SRM proactively warns about insufficient storage capacity for failover in a secondary data center.
  - VMAN enables rapid replication of critical VMs to the secondary site in anticipation of the data center going offline.
  - Backup Exec ensures regular backups of critical data are taken offsite in case restoration is needed.
- **Solution:** Business operations can continue with minimal disruption by:
  - Expanding storage resources in the secondary site.
  - Failing over applications to the replicated VMs.
  - Restoring data if a worst-case scenario occurs at the primary site.

- **Scenario 4: Optimizing Cloud Migration Costs**
- **Problem:** Uncontrolled cloud resource usage leads to unexpectedly high costs.
- **Modules Involved:** Cloud Monitoring, SAM, VMAN
- **Integration Flow:**
  - Cloud Monitoring shows underutilized or oversized cloud instances (across Azure, AWS, etc.).
  - SAM identifies applications with low resource usage on those instances.
  - VMAN provides recommendations to downsize instances or consider re-architecting applications.
- **Solution:** The organization can:
  - Right-size cloud instances for improved cost efficiency
  - Re-platform applications to a more suitable cloud service model (e.g., PaaS instead of IaaS).
  - Establish usage thresholds and alerts to prevent future cost overruns.
- **Key Takeaways:**
- **Cross-Module Visibility:** No single module solves every problem; integration is what gives IT full situational awareness.
- **Troubleshooting Efficiency:** Instead of blind guesswork, IT moves quickly from problem identification to root cause analysis.
- **Data-Driven Decisions:** Integrations make the business impact of IT actions measurable, justifying investments.

Business Scenarios

- **Scenario 5: Mitigating a Security Breach**
- Situation: A critical business application experiences anomalous traffic patterns and suspicious user activity during off-hours.
- Complication: Security analysts must quickly determine if this is a targeted attack, pinpoint the breach point, and assess the extent of potential data compromise.
- Resolution:
- SEM triggers an alert based on unusual login attempts, file access patterns, and large outbound data transfers.
- NTA confirms the source device of the suspicious traffic and identifies abnormal communication with external IPs.
- UDT reveals that the compromised device belongs to an employee within the finance department.
- IPAM provides historical IP data, helping to trace back the attacker's initial entry point into the network.
- NCM logs indicate a firewall configuration change the previous day that inadvertently opened the exploited port.
- Outcome: The security team rapidly contains the breach by isolating the affected device. Integration provides the context to understand the attack timeline, scope, and remediation steps (rolling back firewall change, investigating compromised account).
- **Use Case 6: Ensuring Application Availability During Peak Demand**
- Situation: An online retailer approaches its busiest sales season. Past seasons have seen website slowdowns and outages under the increased load.
- Complication: It's unclear whether slowdowns originate from overloaded servers, database bottlenecks, or insufficient network capacity.
- Resolution:
- VMAN provides performance metrics for virtual machines involved in the web application stack (web server, application server, database).
- SAM provides deeper OS-level metrics, identifying memory pressure on the application server.
- DPA shows that query response times from the database tier are within normal ranges.
- NPM reveals that the physical network link between the application and database tiers is nearing saturation.
- Outcome: Armed with this data, IT provisions additional memory for the application server VM and upgrades the network link. The retailer handles peak season traffic smoothly, avoiding lost revenue.

Business Scenarios

- **Scenario 7: Maintaining Compliance in the Healthcare Industry**
- Situation: A healthcare provider needs to demonstrate HIPAA compliance across its IT systems. This includes log retention, access controls, and prompt detection of potential breaches.
- Complication: Evidence of compliance needs to be centralized and easily accessible for audits, spanning multiple systems.
- Resolution:
- LEM collects and stores security logs from servers, network devices, medical equipment, and applications.
- NCM monitors for any changes to systems storing electronic Protected Health Information (ePHI).
- UDT tracks user logins and device association for patient data access and endpoint security posture.
- SEM correlates events to identify potential unauthorized access attempts or data modification actions.
- Service Desk provides auditable ticketing workflows for incident response and change approvals.
- Outcome: The organization has a robust audit trail, streamlines reporting, and proactively identifies security risks thanks to integrated monitoring.
-

Scenario 7: Rapid Cloud Migration Troubleshooting

- Situation: A critical business application is migrated to the cloud (e.g., AWS), but users report severe performance degradation compared to the on-premises version.
- Complication: The root cause is elusive. It could be under-provisioned cloud instances, network bottlenecks, latency to cloud resources, or an application code issue exacerbated by the new environment.
- Resolution:
- Cloud Monitoring provides performance metrics of the cloud instances (CPU, memory, disk, network I/O).
- VMAN offers insights into potential resource contention within the cloud environment, if virtualized.
- NPM and NTA analyze traffic between the cloud and remaining on-premises components, as well as traffic within the cloud VPC for latency or bandwidth issues.
- WPM simulates end-user transactions, pinpointing which step of the application process is causing the slowdown.
- SAM provides OS and application-level metrics (if agents can be deployed in the cloud).
- Outcome: The data reveals the application is poorly optimized for cloud database access patterns. Developers refactor database queries, and performance returns to acceptable levels.
-

Business Scenarios

Scenario 8: Proactive Ransomware Protection

- Situation: Ransomware attacks are on the rise. The organization wants to prevent an attack or, at the very least, limit its impact.
- Complication: Ransomware techniques evolve rapidly. Traditional antivirus and perimeter security aren't always sufficient.
- Resolution:
- SEM establishes behavior-based alerting, detecting unusual file modifications, mass encryption activities, or access patterns that could signal ransomware.
- NCM rigorously tracks configuration backups for rapid restoration of critical systems if impacted.
- LEM securely stores logs off-site, ensuring forensic data is preserved even if the attack compromises primary systems.
- UDT assists in identifying the initial patient-zero device and potentially unusual user activity associated with the attack's start.
- Backup Exec provides reliable and tested backups stored off-site to aid in system recovery.
- Outcome: While an attack might still occur, the organization is well-prepared to detect it early, minimize damage, and recover essential operations quickly.

Scenario 9: Optimizing Data Center Power and Cooling

- Situation: Rising energy costs strain the IT budget for maintaining a data center. Inefficient cooling leads to hotspots within server racks.
- Complication: It's difficult to pinpoint where power usage is highest, or if cooling airflow is optimal for the equipment layout.
- Resolution:
- NPM or IPAM provides IP addresses of devices within data center racks.
- SAM gathers detailed power consumption data from power distribution units (PDUs) if compatible.
- Environment Monitoring (a separate SolarWinds module, or 3rd party integration) provides temperature and airflow sensors within the racks.
- VMAN can potentially track virtual machine placement to physical hardware within the data center.
- Outcome: IT identifies servers with unnecessarily high power draw and optimizes virtual machine placement to balance load across the hardware. Cooling is adjusted based on heat mapping. The combined result is lower operating costs.

Industry – Case References

Healthcare

- **HIPAA Compliance:** NCM tracks changes to systems handling PHI (Protected Health Information). SEM monitors for unauthorized access attempts. LEM aids in long-term log storage for audits.
- **Patient Portal Performance:** WPM ensures smooth patient access to online portals and critical functions. NPM troubleshoots network bottlenecks impacting data exchange with healthcare providers.
- **Medical Device Management:** UDT inventories and monitors connected medical devices (infusion pumps, monitors, etc.). SAM tracks their software versions for patch management and vulnerability tracking.
- **Network Segmentation:** NCM enforces network segmentation policies to isolate sensitive patient data. NTA identifies anomalous traffic patterns potentially indicating a breach attempt.

Finance

- **PCI DSS Compliance:** NCM and SEM work in concert to monitor file integrity on systems handling payment data, detect unauthorized changes, and log access attempts in line with PCI requirements.
- **Fraud Detection:** NTA helps establish normal network and application traffic baselines. Deviations from these patterns, as monitored by NTA and SEM, could indicate fraudulent transactions or data exfiltration attempts.
- **High-Performance Trading:** Precision network time synchronization for financial systems (NTP is included in the Engineer's Toolset). Ultra-low latency network monitoring with NPM identifies even microbursts that could impact trading applications.
- **Secure Remote Access**: Dameware Remote Support enables controlled access for support personnel to troubleshoot issues with systems in secure environments.

Manufacturing

- **Production Line Optimization:** SAM monitors the health and performance of control systems (PLCs, SCADA) ensuring production uptime. NPM analyzes traffic patterns to prevent bottlenecks impacting machinery communication.
- **Predictive Maintenance:** VMAN monitors vibration, temperature, and other sensor data from machines, feeding into SAM or specialized monitoring platforms for early detection of potential failures.
- **Inventory Management:** UDT tracks equipment and tools, while IPAM manages IP assignments in potentially large-scale manufacturing plant IT environments.
- **Supply Chain Visibility:** Cloud-based WPM (Pingdom) checks the health and responsiveness of supplier portals or logistics systems integrated with manufacturing operations.

Retail & E-commerce

- **Peak Season Readiness:** VMAN assists with capacity planning for handling spikes in website traffic. Load testing with WPM ensures critical e-commerce applications scale properly.
- **Point-of-Sale (POS) System Health:** SAM monitors POS terminals and payment gateways, proactively resolving issues that could impact sales.
- **DDoS Protection:** NTA detects abnormal traffic patterns early on. Integration with SEM and NCM aids in isolating traffic and mitigating such attacks to protect revenue.
- **Inventory and Warehouse Management:** UDT tracks location and status of goods, while IPAM supports IP address planning within large warehouses that often have extensive wireless networks.