

Security Information Management (SIM)

Network and system security is as much about gathering and analyzing data as it is about implementing protective solutions. Good security requires the intelligent monitoring of traffic flows. Administrators who are aware of all traffic but without an understanding of its purpose have an “at risk” state of security. The lower the awareness the greater the risk.

Intelligent Monitoring requires context. Consider the example of a network firewall; knowing the first interface connects to a group of desktop users, the second to the Internet, and the third to e-commerce systems will lend a far better understanding of traffic expectations than simply knowing about a firewall with three interfaces. Although a skilled administrator may understand the context, a firewall can rapidly generate hundreds of thousands of logs and overwhelm any manual review.

Security Information Management (SIM) is the central repository to collect the mass of network data, review it against context and alert against known baselines with specific rules applicable to individual environments. Virtela’s Managed SIM service tracks traffic events on a multitude of network devices, including routers, switches, firewalls and IDS/IPS – all the way down to the server. It provides the tools to review data generated by an enterprise network and interpret against the context of the source, destination and historical baseline.

Virtela’s Managed SIM solution assures the recognition and prioritization of actionable events. Through SIM, assets can be valued based upon the purpose they serve. An e-commerce company’s most valuable asset could be the order-tracking database for online sales. Loss of such a database could represent tens of thousands of dollars per minute lost. Any suspicious event related to that asset should be vigilantly reviewed. Virtela’s Managed SIM not only provides this level of detail, but also extends it to every monitored device in an infrastructure. It filters through suspicious events across an entire network to better identify malicious traffic targeting critical assets.

Any Internet facing application with login features will suffer brute-force attacks. These attacks are usually perpetrated via scripts that randomly target systems that respond to login requests. Most scripted brute-force attacks are not a threat to properly patched and configured systems. Due to the frequency, administrators often ignore them. But when multiple attacks originate from a common location and/or are repeated over time it may be indicative of a more troublesome situation. The SIM tracks both historical events and related events across the entire infrastructure. SIM removes the burden of manually accessing and reviewing logs on multiple devices, (an activity that usually occurs after-the-fact) and replaces it with historical trending across an infrastructure inclusive of real-time notification.

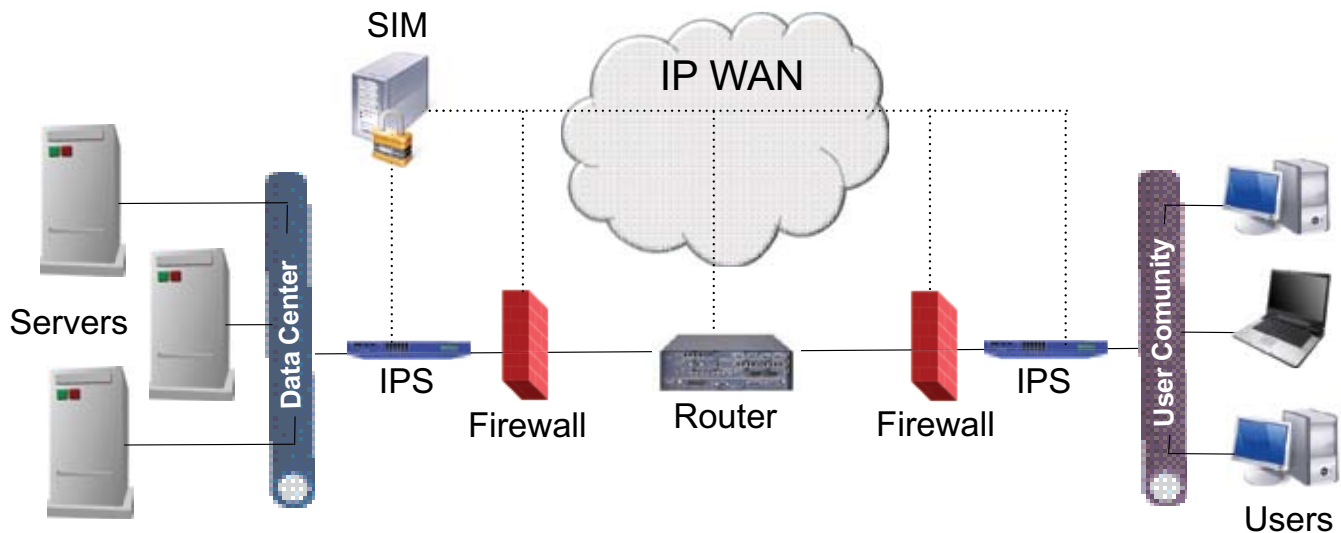


Key Benefits:

- Enterprise-wide event monitoring
- Individual asset valuation
- Cross-platform correlation
- Historical reporting and event notification
- Customer-specific policy definitions
- Regulatory reporting capabilities for SOX, HIPAA, GLBA, CA SB-1386, etc.

Security Information Management (SIM)

Virtela's Managed SIM provides the enhanced tools to monitor an entire infrastructure through a single interface. The granular alerting capabilities allow custom rule definitions tailored to each customer's requirements. Through the application of asset valuation, events are reviewed against a security policy that considers the impact if a vulnerability is exploited. The resulting alert is based upon the likelihood of a successful attack considered against the value of the targeted system(s). Virtela's management of this service includes perpetual tuning to assure focus remains tightly aligned with customer priorities.



About Virtela:

Virtela Communications Inc. delivers award-winning network and security solutions to many of the world's largest and fastest-growing multinational companies. Currently serving customers across six continents, Virtela's network reach spans more than 190 countries. Virtela's unique Global Service FabricSM offers the foundation for delivering critical applications via the company's acclaimed service methodology, with a services suite that includes MPLS and IP-based virtual private networks (VPNs), security services, remote monitoring and management of WAN/LAN infrastructure, and converged services (data, video, voice).

