

## Managed Security Monitoring

Virtela practices vigilant Security Monitoring. We have deployed state of the art tools aligned with high-caliber talent to assure outstanding depth and breadth in our Security Monitoring services. Virtela's monitoring is a real-time service that yields robust protection with the first monitored device and grows exponentially stronger with every additional device. The primary goal in maintaining security is simply knowing what is going on - the more devices, the greater the knowledge, the greater the knowledge, the stronger the security.

Security Monitoring is only as good as the people performing it. At Virtela, we employ skilled engineers with a solid understanding of the platforms we support. Virtela maintains strong vendor relationships and receives regular training on our current platforms and emerging technologies to ensure we can support all of our customer's needs. The depth of our knowledge allows for greater collaboration and information sharing with our customers.

Three factors in Security Monitoring:

1) Resource and Asset Valuation: Through Security Information Management (SIM) enhanced monitoring; customers assign values to resources under the protection of Virtela Security Monitoring. This influences the reaction of automated tools, as well as security engineers. Alerts are generated and reviewed by Virtela engineers as issues occur. Different responses can be defined based upon the value assigned to an asset. Such valuation the prevention of irreversible damage and assures rapid remediation.

2) Real-Time Alerts and Technical Review: Virtela monitoring is a 24x7x365 service. All devices report to our back-office infrastructure in real time. When automated tools identify interesting behavior, an alarm is generated for security analyst review. This two-tier relationship ensures that systems remain tuned to the recognition of security events, and events are manually verified as "real" before a customer is contacted.

3) Cross Platform Correlation: Through SIM monitoring, Virtela can translate information between multiple devices from various vendors. Each device performs a different task, but the data can be interpreted against its relationship with other monitored devices. This correlation becomes more compelling as the number of monitored devices increase. Spotting anomalies and malicious behavior becomes more accurate and easier as the number of devices grows.

Security Monitoring proves its value upon the first recognized attack. A new customer had previously believed they were suffering from poor network performance and inadequate firewall capabilities. Virtela engineers reviewed the situation, and it became readily apparent that a firewall was being inundated by multiple DDOS attacks that overwhelmed the hardware. Due to our understanding of the events, we were able to rapidly deploy an IPS to sit in front of the firewall and absorb the DDOS attacks against the network. The customer regained network performance and Virtela began security monitoring and management for several additional locations.



### **Key Benefits:**

- Deep technical expertise
- Cross-platform rule correlation for both customer and Virtela managed devices
- Vulnerability tracking and review
- Reporting available to customer-defined requirements against: SOX, HIPAA, GLBA, etc.
- Event notification within 15 minutes

## Managed Security Monitoring

Security is not a “set it and forget it” concept. While it’s good practice to design security protection into a network, that protection must be constantly monitored to extract the expected results. Good security requires constant vigilance. Virtela’s Managed Security Monitoring provides customers the benefit of automated security features as well as a set of expert eyes to protect their network 24x7x365.

### Detailed, Security-Centric Statistic Reports

Security Monitoring is a partnership between provider and customer. To be done well, each should have ready access to the same data. Virtela strives to empower our customers with intuitive reports for monitored devices that are accessible 24x7x365 through VirtelaView<sup>SM</sup> our custom online portal. Service reports include\*:

- The source and destination of blocked traffic to track down inappropriate use or infected systems
- Health statistics such as CPU and Memory utilization
- Known vulnerabilities, inclusive of severity and recommended remediation activities
- Event Matrix with a summary of security events, presented per device or all devices
- User Internet activity against permissible or restricted content
- Frequency of use of secure remote access (IPSEC or SSL)
- Network throughput/Bandwidth consumption
- Traffic type analysis – volume of HTTP, SMTP, FTP, etc.

By extending our knowledge of customer security through these reports, customers are empowered with tangible proof of their network security. Customers are armed with data to prove their investment is performing as expected, or given evidence that further investment is merited. Virtela assures that the current investment is performing as highly as possible and will make recommendations as needed.

*\* Actual reports presented dependent upon service(s) subscribed*

### 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 Fabric<sup>SM</sup> 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).

