



10011011011011001  
01010011001110101  
10011011011100100

# SIMCommander K-SOC

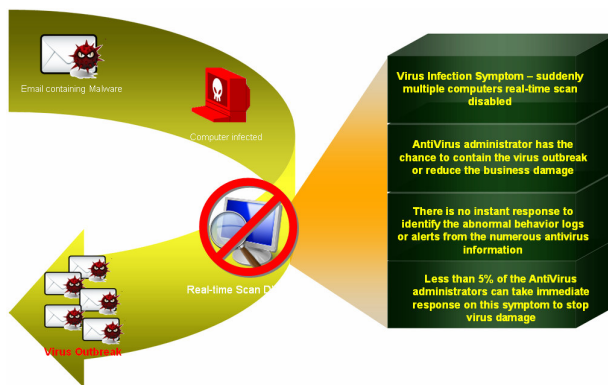
## SIMCommander K-SOC Overview

The new generation of malware is silent, dangerous and most importantly, designed for profit motive. The damages of malware attack involve not simply productivity loss, but also direct financial loss, break the trust and loyalty of your customers and ruin your reputation. Today the number of malware variants is growing exponentially with specific targets, this increases the detection complexity dramatically. Thus, AntiVirus management is moving beyond from a single computer to the whole AntiVirus infrastructure.

SIMCommander K-SOC is a revolution software that centrally collects and stores all antivirus behavioral events to provide total holistic view for better visibility and full traceability of new malware. The intelligent expert system in K-SOC automatically analyzes, classifies and observes behavioral events with alert notifications in real-time that enhances much more malware detection than the traditional AntiVirus solutions, especially in detecting the malware that even not yet identified by AntiVirus vendors.

### Self-Detection of Abnormal Event Sequences

With the intelligent expert system, SIMCommander K-SOC automated surveillance and abnormal behavior detection that proactively detect abnormal activities which AntiVirus applications fail to detect and prioritize those virus threats base on business priorities and service level in real-time to ensure virus outbreak can be stopped before spreading and overwhelm the network.



### Outbreak Containment in Less than 5 Minutes

When the virus occurred accidentally, SIMCommander K-SOC can keep the 'time to respond' to less than 5 minutes by automating the labor-intensive and manual activities on collecting and analyzing the virus threat information with the best practice incident handling guidance.

SIMCommander K-SOC Incident Management Module (IMM) provides the industry's best practices methodology and Standard Operation Procedure (SOP) that helps to prioritize, automate, and report on remediation activities for accelerating the virus response to mitigate the risk and deliver ITIL support.

### KEY BENEFITS

- **Abnormal Behavior Prediction**
  - Proactively detect and alert on abnormal situations to ensure that virus outbreaks can be stopped in the early stage before they spread and overwhelm the network
- **5 Minutes Outbreak Containment**
  - Proactively detect and alert on abnormal situations to ensure that virus outbreaks can be stopped in the early stage before they spread and overwhelm the network
- Built-in best practice virus handling process to effectively improve the response time when virus threats occurred and minimize the impact
- Transforms virus threat trends and AntiVirus system information into actionable plan for managing the risk
- Precise compliance information to meet regulatory and internal audit requirements
- Automated operations to drive productivity, team efficiency and lower the operation costs
- Web portal allows users access security posture anywhere and anytime
- Functions as a virtual 7X24 security staff to monitor and improve overall security posture.
- Scalable architecture to integrate with SIMCommander total security information management platform



100110110110110001  
01010011001110101  
10011011011100100

### Tracing the Origins of Infected Computer

SIMCom Commander K-SOC automatically draws the virus infection path to graphically identify the first infected computers to the last infected computers for root cause analysis

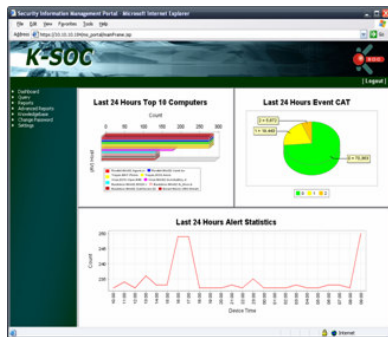
### Visualization of Virus Posture

SIMCom Commander K-SOC at-a-glance dashboard provides the holistic view of your virus protection and compliance postures from a single console. AntiVirus events from multiple AntiVirus applications are correlated and presented in a consolidated console that enables you to easily drill into information for rapidly and accurately pinpoint which computers are spreading the virus from a graphical map or network diagram.



### Master virus activities anytime and anywhere

SIMCom Commander K-SOC built-in Enterprise Web Portal that allows you to manage and generate reports on AntiVirus applications status and virus activities anytime and anywhere with an internet browser.



### Compliance Automation

SIMCom Commander K-SOC enables you to reduce the cost and effort to comply with regulations and industry standards such as ISO 27001 and SOX. Its automated compliance reporting helps you to meet compliance requirements for your business right out of the box

### Comprehensive Reporting

Out-of-the-box comes with over 200 actionable report templates including Real-time reports, Management reports, Technical reports and Compliance reports that helps to measure the success on AntiVirus management.

SIMCom Commander K-SOC Reports is automated and can be scheduled to run at any time and exported into different formats to free up your resource for other important tasks



### Fast Time to Value

SIMCom Commander K-SOC provides you with an exceptional time to value. With its quick and simple installation and configuration, you can monitor and deliver virus protection within 30 minutes.

### Upgradeable to SIMCom Commander

SIMCom Commander is a completed security information management solution which is designed for enterprises and MSSP to address the challenge in managing the complexity of security information in business terms. SIMCom Commander K-SOC can be upgradeable to SIMCom Commander for collecting security logs data from disparate security devices such as firewall, intrusion detection systems (IDS), networking devices, operating systems and applications, and transform those raw data into meaningful and actionable information.

### System Requirements

<b>SIMCom Commander K-SOC Collector</b>	<ul style="list-style-type: none"> <li>▶ Intel Dual-Core 2.0GHz Processor</li> <li>▶ 1GB Memory</li> <li>▶ 1GB Hard Disk Space</li> <li>▶ Windows XP / 2003 Server with latest Service Pack</li> </ul>
<b>SIMCom Commander K-SOC</b>	<ul style="list-style-type: none"> <li>▶ Intel Dual Core 2.0GHz Processor</li> <li>▶ 4GB Memory</li> <li>▶ SATA, RAID 160GB Hard Drive</li> <li>▶ Windows 2003 Server with latest Service Pack</li> <li>▶ Microsoft SQL Server 2005 Standard with latest Service Pack</li> </ul>