



As security and compliance become more interconnected, the need to operationalize key controls in an automated sustainable process increases. The days of separate tool silos that provide a snapshot view of one aspect of security are gone. TippingPoint and Critical Watch have integrated the industry leading intrusion prevention system (IPS) and vulnerability management (VM) system into a single solution that will allow enterprises to increase overall security, implement a closed loop process to meet regulatory compliance, while reducing demands on IT personnel.

Optimized_IPS_Security_Policies

Quickly_Implement_Highly_Targeted_IPS_Policies

The integrated TippingPoint and Critical Watch solution quickly identifies network vulnerabilities, compares those vulnerabilities to current IPS filter settings, and then recommends appropriate IPS filter changes to protect identified vulnerabilities. With this list of recommendations IT personnel can quickly implement highly targeted IPS policies and document changes.

Determine_Risk_to_Key_Assets

The Critical Watch FusionVM® vulnerability management system automatically identifies risks to key assets including network devices, applications and database vulnerabilities.

Detect_Unknown_Hosts

The VM system detects unknown hosts, wireless access points, network devices, installed applications, and known and unknown services.

Highly_Informed_and_Timely_Risk_Remediation_Decisions

These integrated tools allow enterprises to implement a simple and automated closed loop assessment and protection process in which IT personnel can make highly informed and timely risk remediation decisions.

Improved_Compliance_Processes

Clear_Automated_Process_and_Audit_Trail

TippingPoint and Critical Watch provide the tools necessary to establish clear assessment and remediation processes and document IT remediation to maintain regulatory compliance and present a clear audit trail for audit defense.

Track_Mitigation_Steps_and_Exception_Handling

This integrated solution also automates much of the assessment and remediation process and provides documentation of exception handling for continuous audit defense.

Closed_Loop_Consistent_and_Repeatable_Process

This VM and IPS protection solution gives IT the ability to implement a closed loop assessment and remediation process that is automated, consistent and repeatable. The result is improved visibility, measurability, control and reporting over network risks.

Simplified_Policy_Decisions_and_Improved_Security

This simple integrated solution provides IT personnel with the information necessary to make quick easy policy change decisions that result in improved network security.

TipingPoint_IPS / VM_Integration_Solution

VA / VM_Integration

"This combined solution saves me valuable time by providing a single source for viewing my vulnerability posture in comparison to available IPS coverage and then enabling a process to easily tune filters based on that information.

TipingPoint and Critical Watch have brought a truly forward looking solution to the marketplace that greatly simplifies and streamlines the security management challenge."

Scott Engel

Director of IT Infrastructure
Transplace

Reporting_for_SOX,_HIPAA,_GLBA,_PCI-DSS,_FISMA_and_Others

The FusionVM system provides specific reporting capabilities for demonstrating compliance to a number of different regulatory requirements including Sarbanes-Oxley, HIPAA, GLBA, PCI-DSS, FISMA, and other standards.

Automated_Alerts_for_Expedited_Security_Decisions

The automated vulnerability assessment can alert IT personnel when new vulnerability types are identified or when new assets are recognized that have vulnerabilities. These alerts allow enterprises to quickly implement recommended IPS policy changes to reduce the time between exposure discovery and remediation.

Automated_IPS_Filter_to_Vulnerability_Mapping_Updates

TipingPoint and Critical Watch are continuously deploying new assessment and protection capabilities for newly discovered vulnerabilities. In fact, the TipingPoint DV Labs security research team is one of the leading vulnerability discoverers of vulnerabilities worldwide according to Frost & Sullivan research. These newly discovered vulnerabilities are automatically mapped and deployed to the TipingPoint IPS and Critical Watch VM systems.

Automated_IPS_Filter_Updates

TipingPoint IPS filters are updated twice weekly and more frequently if required by the DV Labs research team and automatically distributed to TipingPoint customers via the Digital Vaccine filter update service providing evergreen security and minimizing time required for on-going IPS management.

Easy_to_Deploy_and_Manage_Solution

Automatically_Discover_and_Classify_Assets

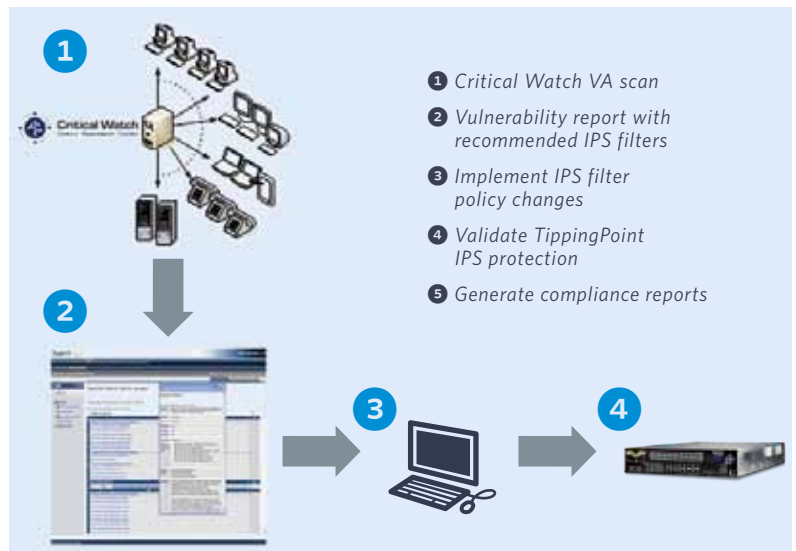
The FusionVM system automatically identifies and classifies all active and inactive hosts, devices and installed applications and risks to these key assets. This repeatable, automated assessment process minimizes IT involvement and time required to maintain network security and compliance.

Automated_IPS_Policy_Change_Recommendations

Automated IPS policy change recommendations make implementing highly accurate and targeted security remediation quicker than ever for IT personnel.

Scalability_for_Global_Deployments

Both the TipingPoint IPS Security Management System (SMS) and the Critical Watch FusionVM system are easily deployable and globally scalable for large enterprise organizations needing integrated assessment and security solutions.



Features and Benefits

- > Optimized IPS Security Policy Settings
- > Improved Overall Security Posture
- > Simple Solution to Deploy and Manage
- > Improved Compliance Processes
- > Documented Procedures for Continuous Audit Defense
- > Scalable for Global Deployments
- > Simplified Policy Decisions

Corporate_Headquarters: 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS

European_Headquarters: Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450

Asia_Pacific_Headquarters: 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999