TrueSight Vulnerability Management

Reduce risk, simplify remediation, and extend the power of Microsoft SCCM automation
In the digital economy, CEOs often cite the ability to drive business growth as their number-one priority. CIOs must support these growth initiatives while continuing to manage costs and keep the organization secure.

This is becoming particularly challenging as hackers are relentlessly targeting organizational data to steal, ransom, or simply disrupt.

The good news is that many hackers rely on old approaches and malware that attempt to exploit vulnerabilities with known fixes that have been available for months, if not years. Although most data breaches can be avoided by simply patching vulnerabilities, many organizations remain exposed because they don’t have the knowledge, tools, or time to close these gaps. These delays often occur because applying patches requires brief outages that must be fit within maintenance windows that are continually shrinking in order to keep business systems online to fuel growth initiatives.
Microsoft System Center Configuration Manager (SCCM) is a popular systems management suite for managing large groups of Windows servers and workstations, but has certain limitations related to vulnerability management that can make patching labor-intensive and onerous.

Today, IT operations teams often struggle with the time-consuming process of manually reviewing scans and prioritizing the vulnerabilities to patch. More specifically, the process of finding and remediating the most critical vulnerabilities can be difficult without understanding the business context of the affected systems or without having guidance for creating remediation plans that fit within operational maintenance windows.

SCCM does a great job of performing the remediation tasks, but falls short when it comes to operationalizing large-scale remediation plans or providing visibility into patching progress or status. What’s needed is the ability to correlate the data from scans with the operational context of the affected servers to give IT operations teams the information they need to prioritize and plan remediation activities. They also need dashboards and reporting to help security and operations teams quickly assess progress and determine risk.
TrueSight Vulnerability Management provides the visibility, analytics, and planning to help configuration management systems—such as TrueSight Server Automation and Microsoft System Center Configuration Manager (SCCM)—to reduce the pain, time, and risk of vulnerability management so that businesses can continue to focus on growth.

**SOLUTION HIGHLIGHTS**

**POWERFUL, INSIGHTFUL, AND CONTEXTUAL**
Uses an intuitive dashboard and a single view to communicate the most critical vulnerabilities and the patches to remediate them. Provides context around each vulnerability, giving operations teams quick insight to understand which are the most critical and which are not. It also gives the security teams insight into the progress made against vulnerabilities detected by security scans.

**INTEGRATED AND AUTOMATED**
Integrates easily with TrueSight Server Automation and Microsoft SCCM. It can improve vulnerability management efficiency by up to 20% by simply prioritizing and applying patches with ease and protecting the environment faster.

**PRODUCTIVE AND COST-EFFECTIVE**
Saves time for operations staff by eliminating the manual effort of sorting through volumes of information to identify key vulnerabilities and associating those vulnerabilities with the patches or jobs to remediate them. Ensures that security and operations teams have better insight into how their activities are tied together to accelerate resolution.

**ACTIONABLE AND INTELLIGENT**
Combines security and operations data to deliver actionable analysis. Imports vulnerability asset group information from vulnerability scanners, maps it to the appropriate remediation, and translates this information into action. Drives direct, timely actions to close vulnerabilities and reduce risk, including finding blind spots that aren’t known to your scanners.
THINK OUTSIDE THE TOP 10 AND PRIORITIZE, THEN SYSTEMATICALLY WORK DOWN YOUR VULNERABILITIES BACKLOG

Consider this: While operations teams may be using SCCM to close vulnerabilities in Windows, they might not be addressing the most critical vulnerabilities. Because of the significant effort involved in finding, assessing, and patching servers, many IT organizations apply shortcuts, such as only focusing on the current month’s Microsoft “Patch Tuesday” critical security bulletins or perhaps only on those that are severity 4s and 5s—leaving lesser vulnerabilities unpatched.

However, a severity 2 can quickly turn into a severity 5 vulnerability if new malicious code is developed to exploit it. This can produce a mad scramble for staff, requiring working nights and weekend hours and having emergency maintenance windows to reduce the threat. These conditions can be very disruptive and stressful to staff and can have a major negative impact on their morale.

The longer a critical vulnerability goes unpatched, the greater the risk. As a vulnerability falls off of your team’s top 10 list but still needs to be patched, how do you scale your efforts with the same people? How do you push out the right patches and go beyond the top 10 threats? How can you find the blind spots, such as old or new systems and networks, or perhaps shadow IT machines that aren’t being actively scanned but that need to be patched?

TrueSight Vulnerability Management can help.
REDUCE RISK AND REMEDIATE CRITICAL VULNERABILITIES

TrueSight Vulnerability Management reduces risks by integrating with configuration and patch management systems, such as TrueSight Server Automation and Microsoft SCCM, to rapidly identify, prioritize, and remediate critical vulnerabilities. **Without TrueSight Vulnerability Management to simplify and improve vulnerability management, the process can be extremely labor-intensive, often involving manual reviews of scans in XML or spreadsheets that can include thousands of lines of vulnerabilities.** Prioritization is often done using basic guidelines, such as only addressing the highest severities or new vulnerabilities, or just targeting certain critical systems. These approaches can leave significant gaps that provide easy access for hackers using automated bots or tools to search for random servers that lack certain patches.

SCCM administrators need a better view of where the critical vulnerabilities exist in their environment and the actions they need to take to remedy the situation. TrueSight Vulnerability Management includes an intuitive dashboard that highlights what’s important. You can look at the environment from many angles, eliminating the need to sift through volumes of data in security scans. The solution ties together the knowledge of a vulnerability to its related patch, so that operations teams can avoid the labor-intensive mapping process and instead begin executing remediation actions to protect their enterprise in a measured and strategic way.
SOLUTION OVERVIEW

TrueSight Vulnerability Management enhances the power of configuration management solutions by giving security and operations teams unprecedented visibility into their environment’s threat stature to quickly remediate risks based on business impact. It natively integrates with popular scanning tools and provides blind spot detection, vulnerability intelligence, and multi-tier remediation for the data center, multi-cloud environments, and DevOps.

BLIND SPOT DETECTION
The solution combines information from the vulnerability scanners and BMC Discovery to ensure there are no blind spots and uncovered or unmanaged systems. Operations and security managers have a full view from external and internal scanners to ensure that every system is discovered, properly scanned, and managed.
SOLUTION OVERVIEW

VULNERABILITY INTELLIGENCE
Security and operations teams can leverage a common view and use intuitive dashboards that integrate data from vulnerability scanners into TrueSight Vulnerability Management. This gives transparency to security staff to understand the remediation progress of the IT operations team. It helps operations to more effectively plan and prioritize remediation. It also dramatically limits the manual work needed to prepare for an audit.

Vulnerability Intelligence Through Visibility and Analytics

- **SYSTEM SCANNING**: Effective vulnerability scanning of disparate systems
- **VULNERABILITY IDENTIFICATION**: Easy categorization and prioritization of the IP system and network vulnerabilities
- **REMEDICATION PLANNING**: Accurate issue identification and remediation planning
- **VULNERABILITY REMEDIATION ANALYSIS AND REPORTING**: Analysis of vulnerability remediation status and efficiency
VULNERABILITY REMEDIATION
Vulnerabilities can be remediated easily because they are automatically mapped to affected servers and patches or configuration change packages. Administrators can schedule remediation activities according to maintenance windows. The remediation itself can be executed by BMC automation tools, such as TrueSight Server Automation and TrueSight Network Automation, as well as Microsoft SCCM.

Multi-Tier Remediation Across Systems and Networks
POTENTIAL TIME SAVINGS – DO THE MATH

With TrueSight Vulnerability Management, you can patch the most critical vulnerabilities on time and reduce the tedious, frustrating manual effort associated with analyzing and deploying patches. It’s not uncommon for organizations to spend over 20% of their server administration staff time analyzing and applying patches.

+ For a five person team, that’s over 160 hours per month analyzing, planning, and applying patches.
+ With TrueSight Vulnerability Management, you can do the same amount of patching in significantly less time, saving up to 150 hours per month while providing greater visibility into risks across the enterprise.
VULNERABILITY ASSESSMENT

Cyber attacks are on the rise, but IT operations teams no longer need to struggle just to keep up. This checklist below identifies common issues and where TrueSight Vulnerability Management can help.

<table>
<thead>
<tr>
<th>ISSUES</th>
<th>REQUIREMENT ADDRESSED BY TRUESIGHT VULNERABILITY MANAGEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Difficult to evaluate risks and prioritize actions</td>
<td>Evaluate risks with dashboards designed specifically to suit the requirements of both operations and security users. Quickly prioritize remediation activities based on policy. Identify performance trends and manage vulnerabilities through their lifecycle.</td>
</tr>
<tr>
<td>Patching, including planning and analysis, are time-consuming activities that can impact system availability</td>
<td>Integrate scanning solutions with configuration management solutions such as SCCM and TrueSight Server Automation to provide better visibility and improved patch planning. Apply patches with ease, reduce downtime, and prevent potential security breaches. Focus only on the vulnerabilities that need attention by filtering out activities that have already been started.</td>
</tr>
<tr>
<td>Lack of vulnerability analysis and reporting accuracy</td>
<td>Exclude scan information known to be incorrect from impacting your analysis and reporting.</td>
</tr>
<tr>
<td>Blind spots can increase exposure and risk</td>
<td>Discover the areas of your infrastructure that are not being monitored and leaving you exposed, so that you can make adjustments. Understand how infrastructure vulnerabilities relate to critical business systems.</td>
</tr>
<tr>
<td>Difficult to identify which hosts do not even have an SCCM agent</td>
<td>Automatically identify these hosts as unmapped during the vulnerability import.</td>
</tr>
<tr>
<td>It takes too long to respond to known threats</td>
<td>Save time and respond to known threats quicker by auto-importing scan exports from Qualys, Nessus, and Rapid7.</td>
</tr>
<tr>
<td>Difficult to map vulnerabilities with the right patch to the right OS version</td>
<td>Automatically map vulnerabilities (bulletins) to patches.</td>
</tr>
<tr>
<td>Lack the ability to perform deep vulnerability analysis or demonstrate compliance</td>
<td>Export the data to perform independent analyses, develop and share custom reports on vulnerabilities, and meet audit requirements.</td>
</tr>
<tr>
<td>Remediation workflows are cumbersome</td>
<td>Schedule scan verifications and remediation activities within the same workflow.</td>
</tr>
<tr>
<td>Spend too much time recreating remediations for non-patch vulnerabilities</td>
<td>Once a remediation activity is created, it is available for reuse without the need to modify cumbersome orchestration workflows.</td>
</tr>
</tbody>
</table>
Online Business Systems has built our security integration framework on BMC technology and we believe that the TrueSight Vulnerability Management will fill a critical gap in the market and be a game changer in the security operations space.”

—Jon Fraser, Managing Director, North America
Online Business Systems

Threats are growing, IT operations and security teams are working in an increasingly complex environment, and these teams need the visibility and analytics to prioritize and target risks faster and more effectively. TrueSight Vulnerability Management makes the output of the security team’s vulnerability assessment efforts easily visible and actionable while expediting and improving the effectiveness of the remediation process. Organizations that use SCCM, for example, have the ability to accelerate the closure of their most critical vulnerabilities at the right time while dramatically reducing the labor, frustration, downtime, and costs involved in this process.

For More Information

To learn more about TrueSight Vulnerability Management, please visit:
bmc.com/it-solutions/truesight-vulnerability-management
About BMC
BMC helps customers run and reinvent their businesses with open, scalable, and modular solutions to complex IT problems. Bringing both unmatched experience in optimization and limitless passion for innovation to technologies from mainframe to mobile to cloud and beyond, BMC helps more than 10,000 customers worldwide reinvent, grow, and build for the future success of their enterprises.