Anthony Mercer

Current InfoSec Management Practices – Remote Management and Monitoring

Abstract

Remote Management and Monitoring platforms (RMMs) are quickly becoming one of the most popular information security management tools. These platforms provide information security (InfoSec) managers with superior visibility of assets (servers, networking equipment, workstations, printers, etc.), simplified control and a centralized notification and reporting system. The text explores how Remote Management and Monitoring platforms provide the following primary benefits to information security managers: policy management and access controls, centralized reporting (executive summaries, asset information, network data flow, security patch compliance), controlled 3rd party application and operating system security patching, anti-virus and firewall integration, remote access to all assets, automation (software installation, patching, problem correction), network management via NetFlow or SNMP, and a web-based central management interface. The purpose of this study is to present an overview of how Remote Management and Monitoring platforms are being used by information security managers today. The following questions are examined: "What is a Remote Management and Monitoring platform? How are information security managers using them? Which platforms are most popular?" It is hoped that this paper will educate readers about the use of Remote Management and Monitoring platforms by information security managers.

Introduction

There are approximately 3.8 million records stolen via breaches every day. That's 44 records every second. Over 70% of the healthcare industry has been infected by some variant of malware in the past year. By 2020, a data breach is expected to cost $150 million on average

(Morgan 2018). If these statistics don't shock you, they should. Globally, it is expected that $1 trillion will be spent on cybersecurity between 2017 and 2021. These data points are but a small reason why information security is one of the fastest growing professions today. As this sector grows, there is an ever-increasing demand for personnel who can manage these security needs. Enter the information security manager. As the deluge of cyber threats continue pounding the shores of the information security managers' assets, the need for better management tools grows. Remote management and monitoring platforms fit this bill like a glove. Once installed, they provide myriad benefits to today's over-worked InfoSec managers, including: a much higher degree of visibility to all IT assets (hardware and software alike), centralized management of multiple layered/security platforms (anti-virus, server backups, notifications, network management, etc.), and an easy-to-use/easy-to-read reporting system. This report will explain precisely what an RMM is, what it can do for InfoSec managers and organizations, and why it should be implemented wherever possible.

Definition – What is Remote Management and Monitoring?

Remote monitoring and management (RMM) is a collection of information technology tools that are loaded on client workstations and servers. These tools gather information regarding the applications and hardware operating in the client's location as well as supply activity reports to the IT service provider, allowing them to resolve any issues. RMM usually provides a set of IT management tools like trouble ticket tracking, remote desktop monitoring, support and user information through a complete interface. RMM is the proactive, remote tracking of network and computer health. RMM helps to enhance the overall performance of present technical support staff and take advantage of resources in a much better manner (What is Remote Monitoring and Management, Techopedia). RMM has drastically changed the information security sector by

providing managers with greatly increased visibility of their network assets. These assets include, but are not limited to: servers, workstations, laptops, tablets, modems, routers, firewalls, switches, wireless access points, network printers, NAS's, etc. Now that information security managers can use RMM to accurately see, in real-time, the status and health of virtually all of the assets for which they are responsible, they are able to make far more educated and informed decisions regarding that information security (see Figure 1).

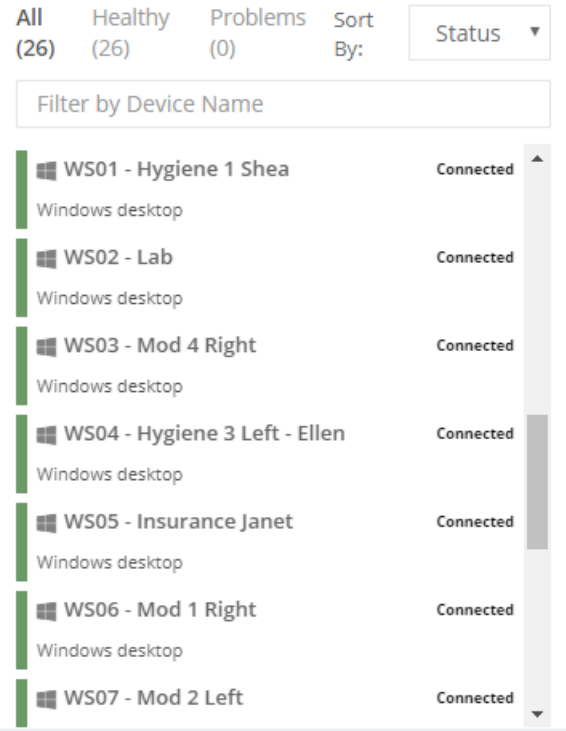

Figure 1 – RMM Asset Management

RMM is now considered by many an absolutely essential tool that information security managers need in order to perform their jobs to the best of their abilities. It has quickly grown into a staple for many business' Information Security Management Systems (ISMS). *Haufe, Colomo-Palacios and Dzombeta posit that, "Securing sensitive organizational data has become increasingly vital to organizations. An Information Security Management System (ISMS) is a

systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security".

RMM helps information security managers in myriad ways. Downtime is one of the biggest data threats to companies/entities the world over. Both a loss of clients/customers and money are a great possibility. Employees may be unable to use their standard Line-of-Business applications, communicate via an intra-office comm system or complete their daily tasks whatsoever. In order to keep systems running and data highly available, many of today's information security managers use RMM. In real-time, 24/7/365, the RMM platform monitors the health of all systems and instantly notifies the InfoSec manager if any components reach pre-defined values such as high CPU usage, low disk space availability or high memory usage. RMM also increases overall security by integrating closely with centrally-managed anti-malware and backup solutions, giving the manager an accurate and complete view of the data's health status. Reduction in the total cost of ownership (TCO) is also a key benefit. Most can agree, preventative corrections generally take far less time and cost less money than reactive corrections. With RMM, information security managers can fix "problems" before they ever arise by rectifying them prior to known thresholds being reached.

How InfoSec Managers Use RMM

There are four primary areas in which information security managers use RMM, each with their own subset of benefits/uses. Those four areas are down-time reduction, policy enforcement/compliance, automation and background management/remote access. These will be discussed in-depth, outlining the key benefits from each area thoroughly. We begin with reduction in down-time.

Upper management is never happy when employees, buildings and utilities are being paid for but there is no productivity. This is the ultimate result of down-time. Luckily, information security managers now have RMM to help them keep down-time at an all-time low. Primarily, RMM does so by alerting managers of impending problems before they happen (see Figure 2).

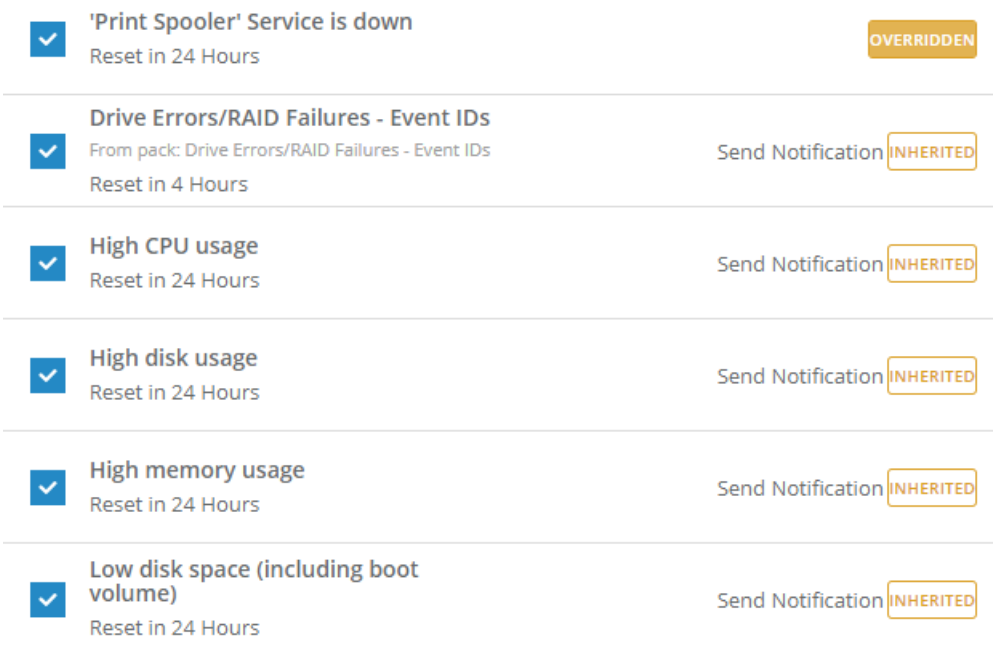

Figure 2 – RMM Alert/Notification Configuration

With this new information, potential problems can be corrected before they ever crop up in a production environment. “It is especially important that serious information security incidents that may result in disruptions to important business processes are promptly communicated to the appropriate officials so that they are involved early in decision-making and communications. In addition, compliance with various federal and state regulations requires expeditious reporting of certain types of incidents” (Information Security Incident Reporting, 2016). Let’s take the following two examples. Example 1: Bob, the information security manager for a world-wide automotive manufacturer, receives a security notification from his RMM. It alerts him to the fact that one of the RAID arrays in a primary production server is now in a

'degraded' state. Bob remotes in to the server, uses the RAID controller software, and discovers that the RAID battery has failed. Now, Bob is able to schedule the hardware maintenance outside of working hours, before it ever causes a problem such as a corrupted data set due to a loss of power without a proper RAID controller cache battery. Example 2: Tim, the InfoSec manager for a global food leader, is sitting at home on the couch with his wife and children. Suddenly, he receives an urgent notification on his cell phone. It reads, "Pre-defined threshold met – disk utilization > 80% on SERVER12". With this new and instant information, Tim calls his technical lead, informs him of the problem, directs him to add 4 additional disks to the server's array, and quietly re-joins his wife and children for their movie.

The parameters which can be pre-defined for use in notifications/alerts in most RMM platforms are virtually endless and aid greatly in the industry-standard practice of defense-in-depth. "'Defense-in-depth' builds over a layered security approach and complements it through additional mechanisms, especially for monitoring, alerting, and emergency response, including disaster recovery, as applicable. This normally includes forensic analysis and criminal activity reporting. This is also complemented where required by authorized personnel activity auditing.1 Normally, the defense-in-depth strategy monitors current activities, and alerts you to imminent threats, thus enabling you to counter such threats through an emergency response or quick recovery, whereas multi-layered security control strategy delays the threat and provides ample time to react. For defense-in-depth to be effective at monitoring the speed at which the traffic/data is monitored and analyzed, and for the alerts to be communicated to the relevant tools or experts for further action, the analysis should be very high for such emergency responses to be effective" (*Rao 2014). Some of the more frequently used are: service 'X' is down, disk/RAID errors, high memory/CPU usage and low disk/array space. However, there are so many more

options such as transfer rates, network usage, process-specific resource utilization, system uptime, etc. With these conditions, information security managers are able to very granularly define the parameters they prefer to use within their purview.

Data being online is irrelevant if there is not sufficient bandwidth to send it to the necessary destination. Oftentimes, this can be caused by botnets / spam / distributed malicious computation. "Due to their limitless size and capacity, botnets are among the most powerful components of a modern cyber-criminal's arsenal of attack techniques. They are made up of compromised workstations distributed over the public Internet that leverage the untapped processing power of a multitude of endpoints, usually to accomplish a malicious agenda. Each of these endpoints, or 'bots', typically links back to a command & control (C&C) server so the entire botnet can be used as one tool to engineer data theft/fraud or spam marketing on a mass scale, as well as to power huge Distributed Denial of Service (DDoS) attacks" (Keall, B., & Mansfield, S. 2016). Here, again, RMM helps InfoSec managers to increase their data availability by providing real-time, accurate data points regarding the network itself through NetFlow or the SMTP protocol (using MIBs). If there is a bottleneck on the network (perhaps a gigabit backbone connection is being saturated) and the proper thresholds have been configured, the manager would know of the impending problem before it occurs (perhaps when the link saturation reaches 75%, if that is where the RMM is programmed to notify). According to *Waldbusser, "Given the resources available on the monitor, it is potentially helpful for it to run diagnostics continuously and to log network performance. The monitor is always available at the onset of any failure. It can notify the management station of the failure and can store historical statistical information about the failure. This historical information can be played back by the management station in an attempt to perform further diagnosis of the cause of the problem".

The next key area in which RMM helps InfoSec managers is enforcement of policy compliance. As central-management and organization-wide reporting are primary components of RMM, information security managers have exponentially better visibility, in real-time, of their assets and the status of software installed. Whether being audited by a local or federal government, or simply providing asset inventory to upper management, RMM suites make InfoSec managers' lives far easier.

Donovan K. states that, "with cyber-criminals constantly inventing new techniques and looking for new vulnerabilities, an optimized security network is only optimized for so long. Even as recent as a couple months ago, organizations fell victim to a major breach with the Heartbleed vulnerability. To keep your network protected, make sure your software and hardware security is up to date with the latest and greatest." One of the most critical software aspects to keep updated for increased security is 3rd party applications such as Adobe Reader and Google Chrome. This is where RMM suites truly shine. InfoSec managers can configure the frequency with which they would like the RMM to scan their assets. Upon scan completion, the RMM will compare the versions of the currently installed 3rd party applications to the most up-to-date and secure available versions via a 3rd party application database repository. Unless specifically programmed otherwise, the RMM will automatically silently download and install the most secure 3rd party application versions. This is all done with exactly 0 InfoSec manager work. If any problems were to ever arise, the manager could simply view the logs to see which application(s) were updated recently and roll them back.

Not only do RMM's keep systems secure by automatically downloading and installing updated 3rd party applications, but they also completely manage the Microsoft Windows updates, patches and service packs. This is superior in virtually every way, shape, form and facet to the

"just automatically download and install everything" mindset that Microsoft has taken on. With the RMM controlling the OS updates, InfoSec managers can stop known-bad updates or instantly push security-related updates to their entire organization with a single click of the mouse. Furthermore, policies can be created which dictate whether OS updates should be installed based on severity criteria such as optional, recommended or critical. This granularity truly gives today's information security managers far more control than ever before over their assets' software updates.

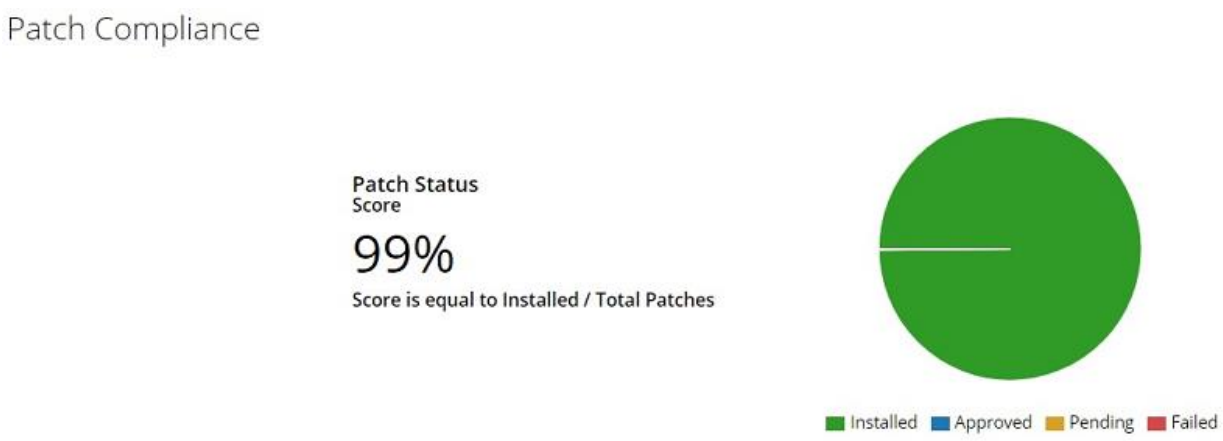

Figure 3 – RMM Patch Management

In addition to 3rd party application and OS updates, RMM suites centrally manage an organization's anti-virus application. Few things are more crucial to a system's overall health than anti-virus software. "It is clear that viruses and antivirus security plays a very important role in the computing world. In these times, new types of viruses are always on the rise and their destructive power is always increasing" (*Kaur 2016).

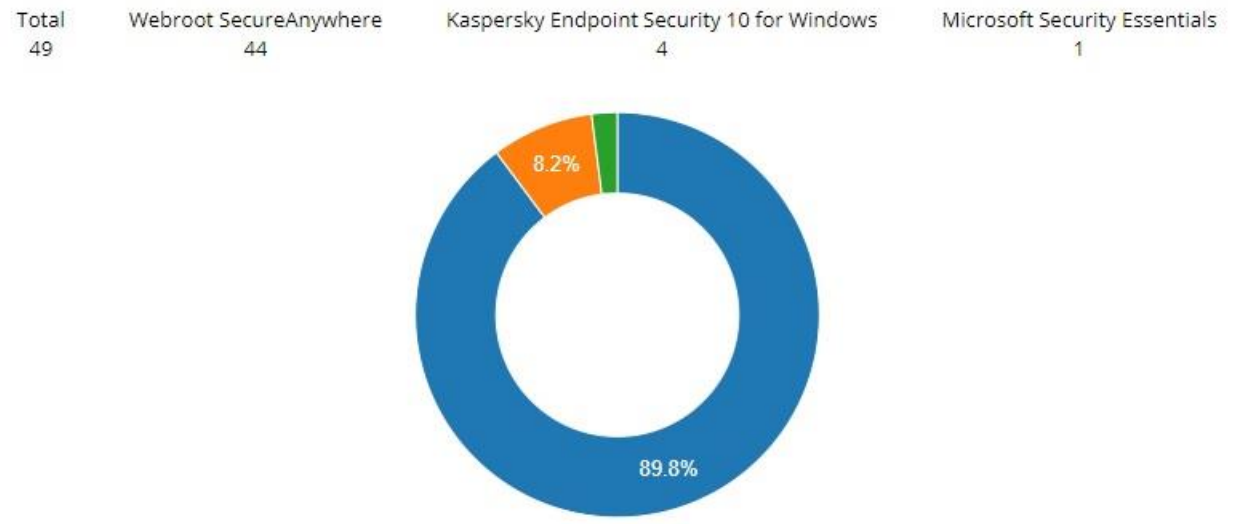

Figure 4 – RMM Anti-Virus Management

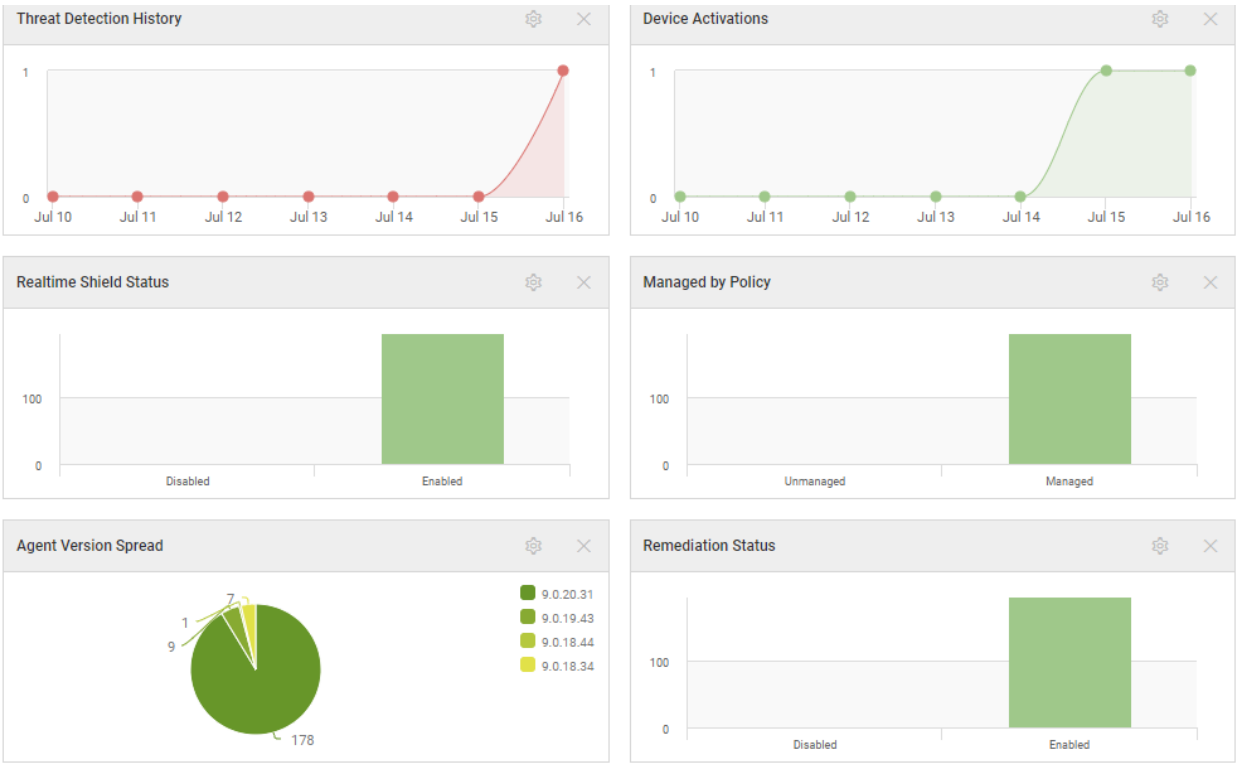

Figure 5 – RMM Anti-Virus Reporting

When combined with centralized management and full reportability, RMM anti-virus management truly ups InfoSec managers' games. Now, in seconds, a manager can generate an organization-wide report that outlines which machines are protected by anti-virus, which version

of the application is installed, whether or not the definitions are up-to-date, when the last scan was completed, etc. Before RMM, many InfoSec managers relied on a months old Microsoft Excel spreadsheet that was less than half accurate.

Data backups can cause InfoSec managers to lose sleep. Wondering if they have completed successfully, unsure if they will restore properly, many managers stress far more than is required over data backups. “The process of archiving information and electronic files is important in the event restoration is ever necessary. Information security managers must ensure that the process of recovering and restoring data files is outlined in the company policy and enforced. The importance of having offsite storage of backup media and system documentation is emphasized” (*Ransome & Rittinghouse 2005). With RMM centrally-managed data backups, those stressors are a thing of the past. Most modern RMM suites will integrate directly with industry-leading backup software and hardware, adding further capabilities to the systems. For example, today’s InfoSec managers can configure the following data backup scenario with RMM: Server/Data backups run hourly or nightly, according to the organization’s information security policy. Once the data has been backed up locally (perhaps to a SAN, NAS or tape drive), it will automatically synchronize off-site to protect against theft/fire/flood. If there are any problems or errors along the way, managers will be instantly notified via text message or e-mail correspondence. Data restore verification is also automated. Many RMM suites have the capability to automatically spin the backups into virtual machines, boot them, log in via a script, and send the InfoSec manager and appropriate staff verified data restore screenshots via SMS or e-mail. Truly, information security via data backup cannot currently get much simpler or more automated.

Which brings us to the third of the four primary areas that InfoSec managers use RMM: Automation. Information security managers have virtually endless automation capabilities via RMM, but several specific scenarios will be outlined here. Whether it is customizable scripts running automatically when a certain parameter is met, automated maintenance tasks such as deleting temp files or defragmenting disks, or streamlined system deployments via automatic application installation/configuration, RMM makes the lives of today's InfoSec managers far better. A manager may want an automation task configured through the RMM such that if the 'print spooler' service on any server were to switch to the 'stopped' state, the RMM would automatically start the print spooler service. Or, if the anti-virus on any workstation were to ever detect an infection, the manager could program the RMM to automatically scan/quarantine. Perhaps, if a virtualized server were ever to enter an 'offline' state not caused by a press of the "shutdown" or "restart" button, the InfoSec manager may wish that server to be automatically booted. Finally, asset management is almost completely automated for the InfoSec manager, making his/her job easier, their data more accurate, and their reporting capabilities far superior. "Complete visibility of your IT environment and a detailed inventory of all your assets is key for a strong security and compliance posture, because the things that pose the highest risk are the ones that you don't know are there. No wonder the CIS (Center for Internet Security) tops its 20 Critical Security Controls list with two asset inventories — one of all devices, the other of all software, said Qualys Director of Product Management Jimmy Graham" (Perez 2017).

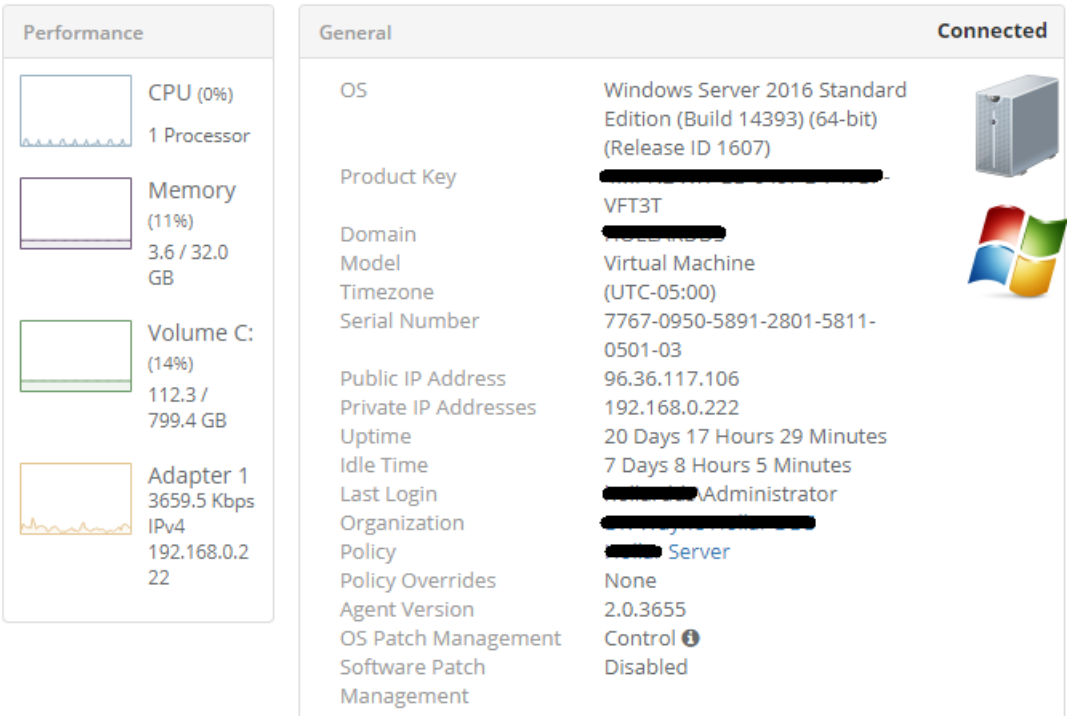

Figure 6 – RMM Device Visibility / Management

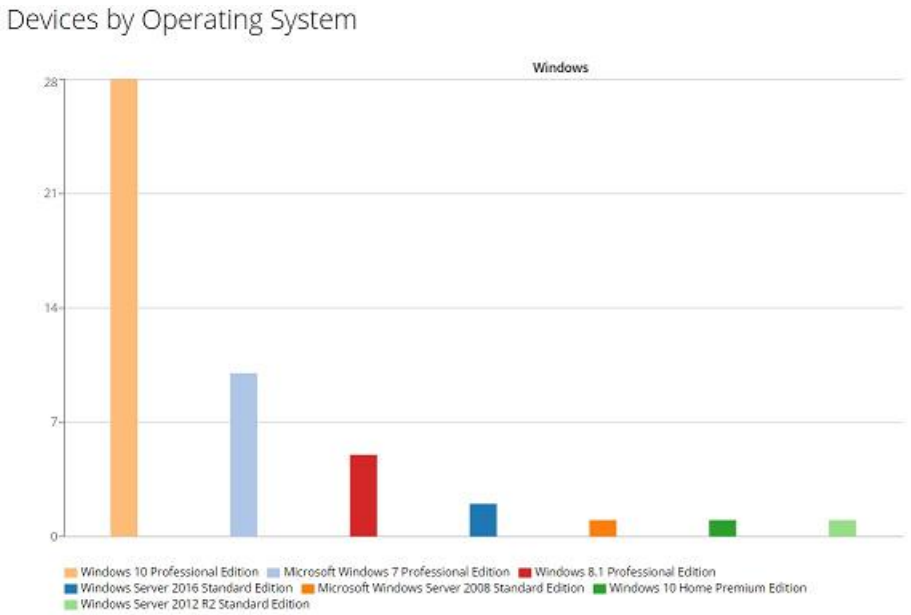

Figure 7 – RMM Asset Report

With RMM, a small light-weight agent is installed on each and every server/workstation. That agent transmits data to the RMM's web-based server. So, organizations will simply install this client on each and every computer they have, and the InfoSec manager will have 100% complete visibility of all hardware/software/statuses in real-time. Reports on these assets can be configured to run automatically, and instantly e-mail them to the proper upper management. This, and so much more, is all possible via today's modern RMM automation tasks.

The fourth and final primary area in which information security managers today use RMM to better perform their jobs is: Remote Access / Background Management. One of the most challenging aspects of information security management today is gaining access to workstations when staff are using their computers almost every minute of every day. Here, too, RMM helps to alleviate some of these challenges. Windows services can be stopped/started, processes can be killed, software uninstalled, custom scripts run and command prompts used all remotely and silently on the back-end without the end-user ever knowing. While this may seem minor to some, in practice it is a critical advantage. Having to ask an end-user to bring their laptop to your office, drop it off for an unknown amount of time, and pick it up once you call them (perhaps a new anti-virus application needs installed on all the organization's workstations) is very much a problem for all involved. Now, with the help of RMM, InfoSec teams can simply run the installer with the appropriate switches / command line values, on hundreds or thousands of an organization's workstations, with a few clicks of the mouse. For most, only once you've experienced the power of RMM for yourself do you truly understand just how powerful and helpful these newly available suites really are.

Conclusion

Confucius once said, “Life is really simple, but we insist on making it complicated.” RMM suites are making life simpler for today’s information security managers. Down time is greatly reduced by real-time notifications and alerts, the ability to correct problems before they arise (disk space beginning to fill up), and cross-platform monitoring. Policy enforcement and compliance is improved due to centrally-managed anti-virus, 3rd part application patching, windows operating system updates and data backups. Automation reduces the work hours required from today’s InfoSec managers by automatically taking action according to pre-configured parameters (i.e. automatically starting the ‘print spooler’ service if it ever enters the “stopped” state), streamlining repetitive maintenance tasks, and making organization-wide reports very easy to generate and modify. Remote access and background tasks help information security managers rectify problems more quickly while increasing end-user satisfaction via the ability to complete many tasks silently, without the user ever knowing it happened. RMM is the single-most important management tool in today’s busy InfoSec manager toolbox.

References

Donovan, K. (2018, May 29). 10 Cybersecurity Best Practices for IT. Retrieved July 13, 2018, from https://www.observeit.com/blog/10-best-practices-cyber-security-2017/

*Haufe, K., Colomo-Palacios, R., & Dzombeta, S. (2016). A process framework for information security management. *International Journal of Information Systems and Project Management*. doi:10.12821/ijispm4402

Information Security Incident Reporting | Standard Practice Guides - University of Michigan. (2016, June 29). Retrieved July 13, 2018, from http://spg.umich.edu/policy/601.25

*Kaur, G. (2016). Network security: Anti-virus. *International Journal of Advanced Research in Computer Science, 7*(6) Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1875134290?accountid=10639

Keall, B., & Mansfield, S. (2016, March). Ransomware Expands. *Network Security*.

Perez, J. C. (2017, September 25). For GDPR Readiness, You Need Visibility into Your IT Assets. Retrieved from https://blog.qualys.com/news/2017/05/17/for-gdpr-readiness-you-need-visibility-into-your-it-assets

Morgan, S. (2018, January 23). Top 5 cybersecurity facts, figures and statistics for 2018. Retrieved from https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

Ransome, J. F., & Rittinghouse, J. W. (2005). *Business Continuity and Disaster Recovery for InfoSec Managers*. Digital Press. doi:10.1016/b978-1-55558-339-2.x5000-1

*Rao, U. H., & Nayak, U. (2014). Key Concepts and Principles. *The InfoSec Handbook*, 29-61. doi:10.1007/978-1-4302-6383-8_3

*Waldbusser, S. (2006). Remote Network Monitoring Management Information Base Version 2.

doi:10.17487/rfc4502

What is Remote Monitoring and Management (RMM)? (n.d.). Retrieved from https://www.techopedia.com/definition/28529/remote-monitoring-and-management-rmm