Technical Review

Managing Risk, Complexity, and Cost with SanerNow Endpoint Security and Management Platform

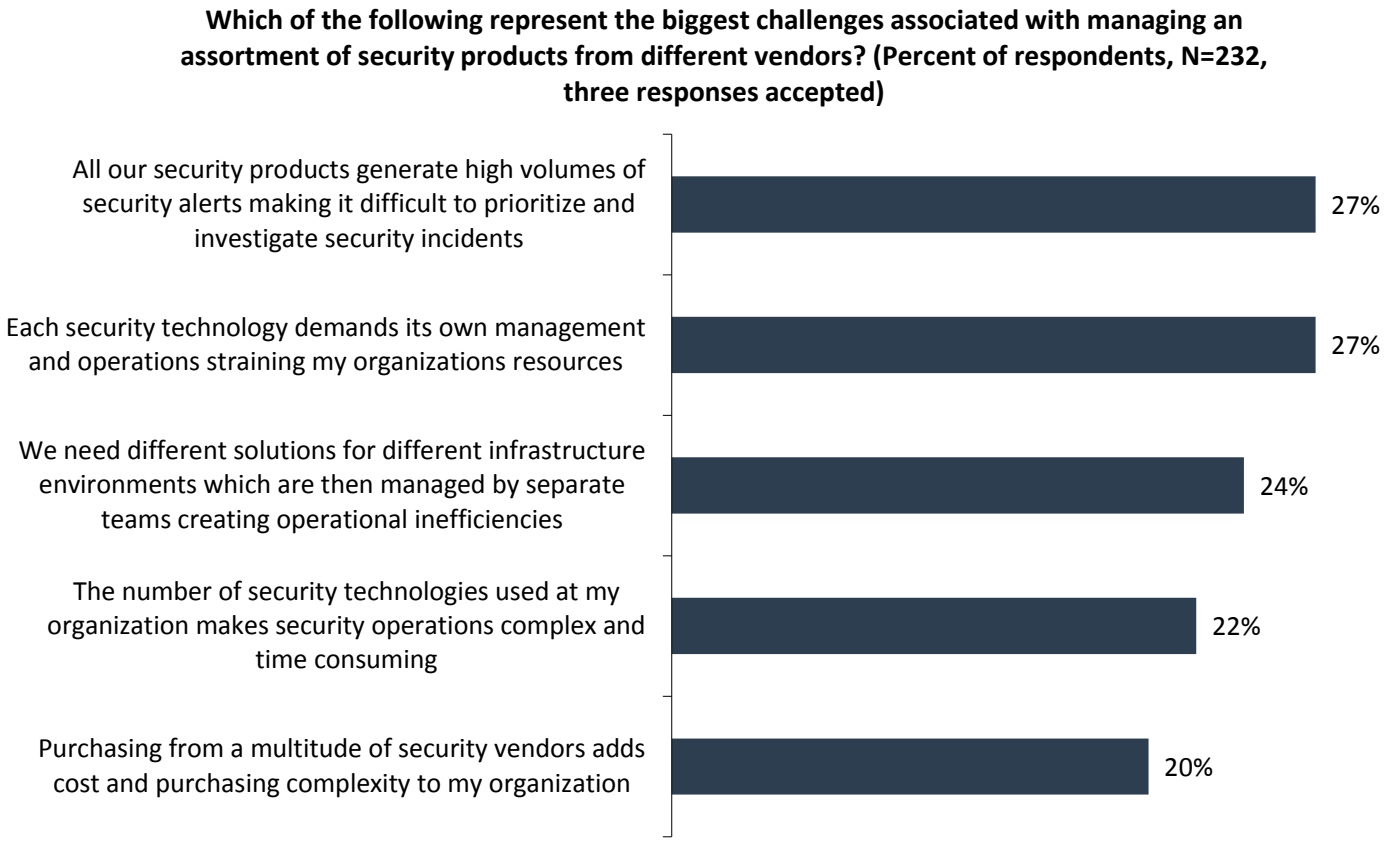
Date: October, 2018 **Author:** Jack Poller, Sr. Analyst

The Challenges

As organizations of all sizes embrace digital transformation and the shift to modern cloud architectures, their IT infrastructure is both growing and becoming more complex. Indeed, two-thirds (68%) of respondents to an ESG research survey said that their IT environment had become more complex in the last two years.[1]

Complex infrastructures have large attack surface areas, necessitating a variety of cybersecurity tools and techniques to protect them against ever-increasing volumes and sophistication of attacks. However, cybersecurity teams report numerous challenges managing an assortment of security products from different vendors, such as the inefficiencies created by having separate management and operations for each tool, cited by 27% of ESG research respondents as a challenge, or different tools for various parts of the IT infrastructure (24%), or the number of security tools making operations complex and time consuming (22%) (see Figure 1).[2]

Figure 1. Top Five Challenges Managing an Assortment of Security Products from Different Vendors



Source: Enterprise Strategy Group

[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.
[2] Source: ESG Master Survey Results, *Cybersecurity Landscape: The Evolution of Enterprise-class Vendors and Platforms*, October 2018.

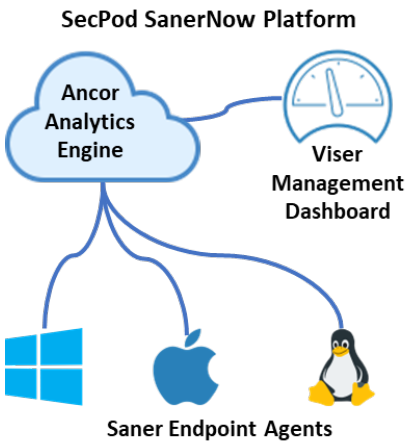
The Solution: SanerNow from SecPod

SecPod created SanerNow as an integrated platform to reduce the complexity, effort, and costs of managing and securing endpoints. The platform replaces multiple point tools, encompassing six endpoint security capabilities, including:

- Vulnerability Management—continuous risk assessment.
- Patch Management—risk reduction by automating the application of fixes to known vulnerabilities.
- Compliance Management—compliance with regulatory standards and industry benchmarks.
- Endpoint Management—automated endpoint management and system hardening.
- Asset Management—discovery and management of assets.
- Threat Detection and Response—detection and response to indicators of attack and indicators of compromise.

SecPod is developing additional modules to provide additional capabilities including file integrity monitoring, mobile device security, remote desktop sharing, and data loss prevention (DLP).

SanerNow comprises the Ancor scalable analytics and correlation engine, the Viser management dashboard, and Saner agents for Windows, Mac, and Linux endpoints. Organizations and managed services providers (MSPs) can deploy SanerNow as a software-as-a-service (SaaS) application, or the Ancor analytics engine can be deployed on-premises.



Security professionals use SanerNow to:

- Query—determine endpoint status and configuration.
- Monitor—determine endpoint changes as they occur.
- Analyze—determine endpoint risks and threats.
- Respond—fix endpoint issues.

Organizations and MSPs deploying SanerNow benefit from:

- Consolidated Platform—SanerNow incorporates all tools necessary for the most common and frequent endpoint security tasks including vulnerability and patch management, asset and endpoint management, regulatory and industry benchmark compliance, and endpoint detection and response. Organizations can simplify their cybersecurity toolbox, replacing many point products with the SanerNow platform.
- Accelerated Results—rapid visibility to risks and threats, and the automatable tools for remediation.
- SaaS—deployed as a SaaS solution, organizations leverage all the SaaS benefits including cloud-based self-provisioning, usage-based pricing, scalability, multi-tenancy, multi-user role-based access (RBAC), and accelerated deployment and upgrades.
- Single Agent—endpoint inventory and control, compliance checks, vulnerability, and endpoint detection and response (EDR) from a single lightweight agent.
- Automation and Orchestration—SanerNow includes a comprehensive set of APIs enabling automation and orchestration of the endpoint security system.
- Ease of Use—SecPod designed SanerNow to be deployed quickly, without requiring extensive user training.
- Cost Management—SanerNow replaces multiple vendors and point tools with a single tool and vendor, with usage-based pricing, enabling organizations to manage the cost of their cybersecurity toolbox.

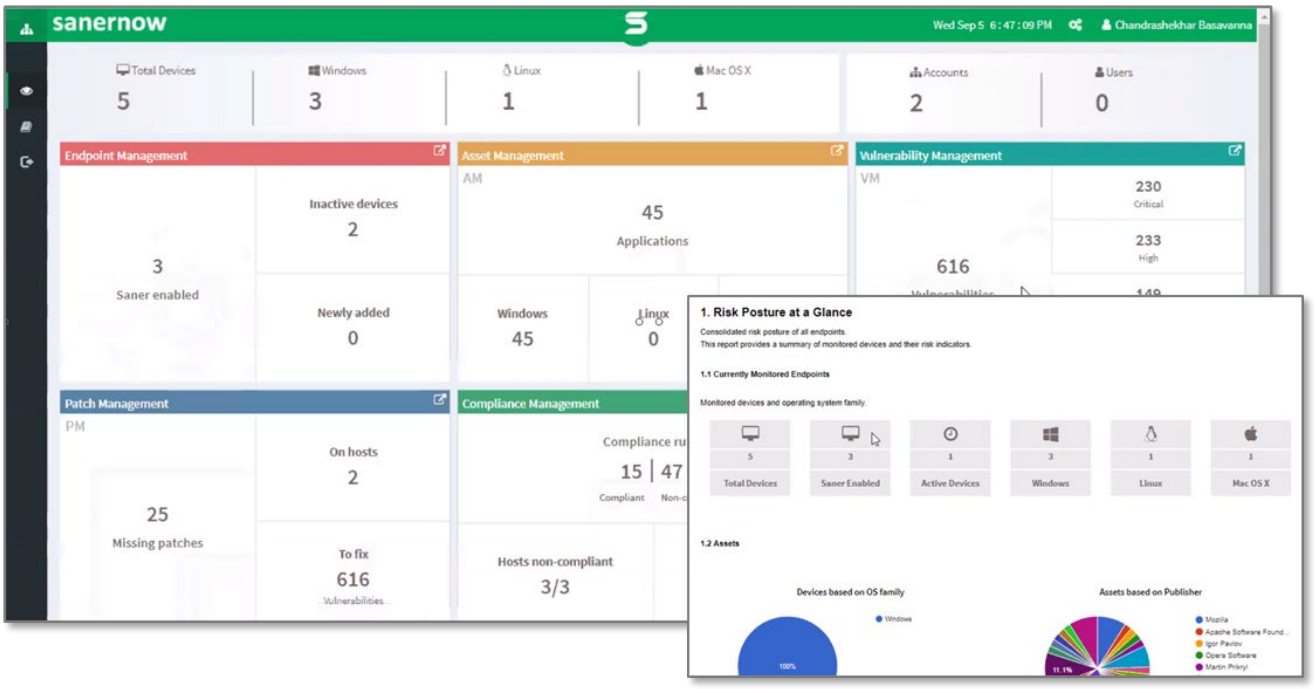
ESG Tested

This review used a demo environment representing a typical organization's IT architecture, with several deployed Windows, Mac, and Linux endpoints. ESG logged in to the web-based Viser management dashboard and was guided by a deployment wizard to create Accounts/Sites and deploy agents. Once the agents were deployed, within 5-6 minutes all the dashboard elements were populated with various findings. The Viser dashboard provides a comprehensive overview of the discovered

endpoints, as show in Figure 2. Below the discovered endpoint information is the summary data for each of the six modules: endpoint management, asset management, vulnerability management, patch management, compliance management, and EDR (endpoint detection and response).

From the menu, ESG Lab selected ***Reports*** to browse through the list of available reports and generate the risk posture report. Users can save reports as PDFs and can configure SanerNow to automatically email reports on a routine basis.

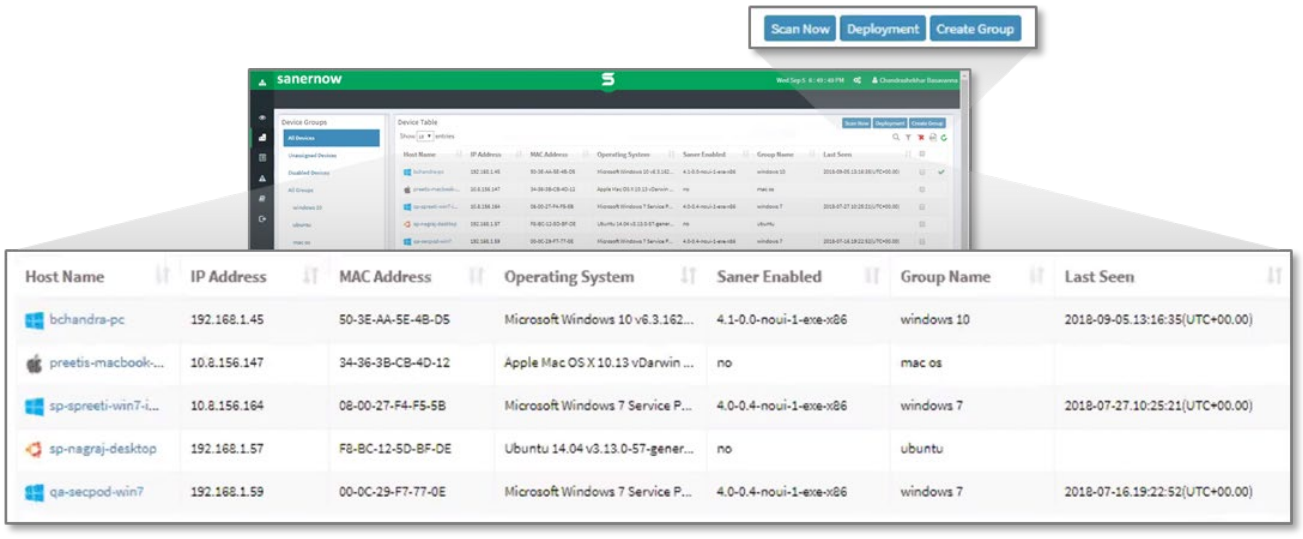
Figure 2. SanerNow Viser Dashboard



Source: Enterprise Strategy Group

As the typical next step for an initial deployment of SanerNow, ESG selected ***Device Manager*** from the menu to discover information about the endpoints in the environment. The device manager dashboard, shown in Figure 3, provided a comprehensive listing of devices, addresses, operating systems, and other critical information about all known endpoints.

Figure 3. Device Manager



Host Name	IP Address	MAC Address	Operating System	Saner Enabled	Group Name	Last Seen
bchandra-pc	192.168.1.45	50-3E-AA-5E-4B-D5	Microsoft Windows 10 v6.3.162...	4.1-0.0-noui-1-exe-x86	windows 10	2018-09-05.13:16:35(UTC+00.00)
preetis-macbook-...	10.8.156.147	34-36-3B-CB-4D-12	Apple Mac OS X 10.13 vDarwin ...	no	mac os	
sp-spreeti-win7-i...	10.8.156.164	08-00-27-F4-F5-5B	Microsoft Windows 7 Service P...	4.0-0.4-noui-1-exe-x86	windows 7	2018-07-27.10:25:21(UTC+00.00)
sp-nagraj-desktop	192.168.1.57	F8-BC-12-5D-BF-DE	Ubuntu 14.04 v3.13.0-57-gener...	no	ubuntu	
qa-secpod-win7	192.168.1.59	00-0C-29-F7-77-0E	Microsoft Windows 7 Service P...	4.0-0.4-noui-1-exe-x86	windows 7	2018-07-16.19:22:52(UTC+00.00)

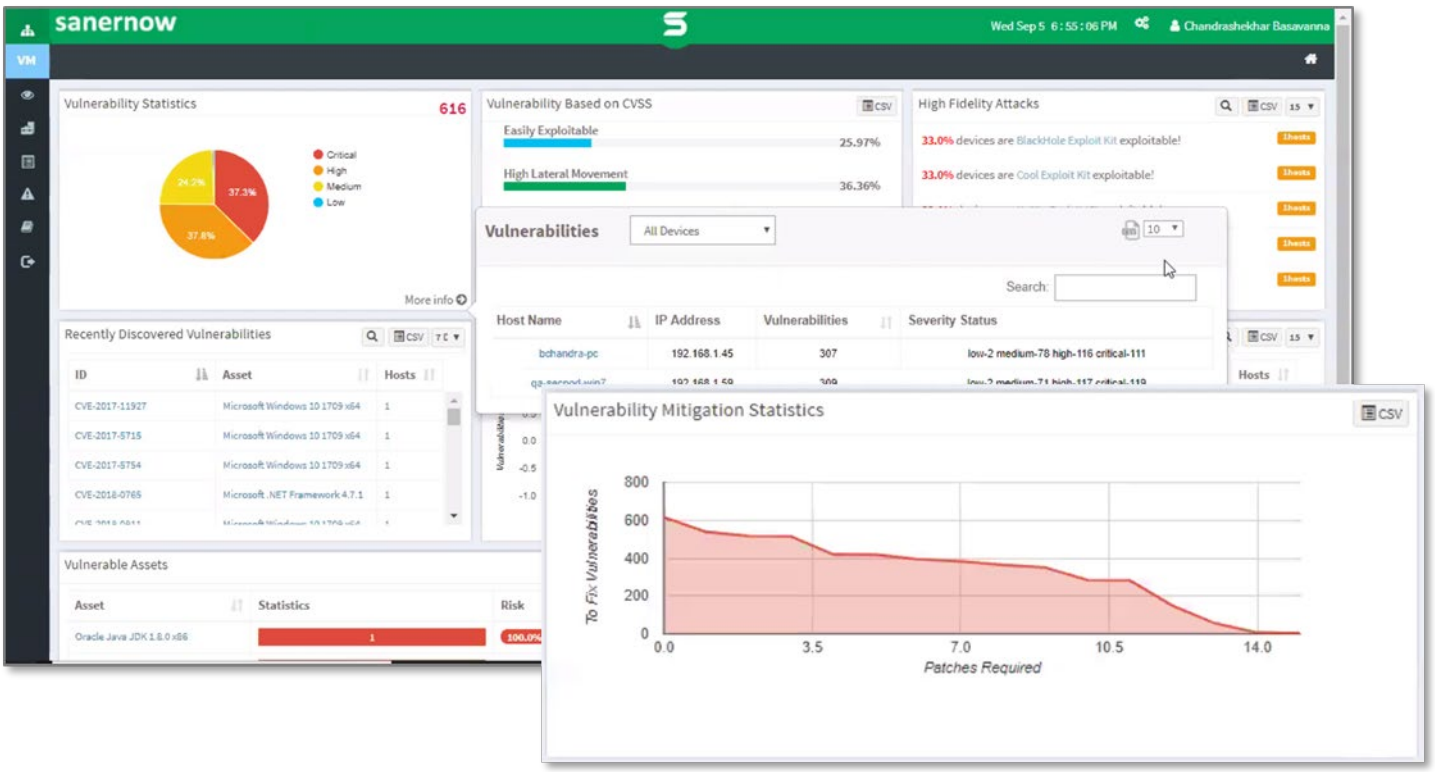
Source: Enterprise Strategy Group

Clicking on the *Create Group* action button brought up a grouping and filtering facility. SanerNow includes groups for each endpoint type (Windows, Mac, Linux), and administrators can group any arbitrary set of endpoints into a new group.

Clicking on the *Deployment* button opened a facility where we could deploy the Saner agent to selected unmanaged systems. Alternately, administrators can distribute a site-specific URL from which users can download and install the Saner agent. Once installed, the agent schedules a daily scan. Endpoints are scanned for inventory, configuration, vulnerability, patch, and other system details. By clicking on the *Scan Now* button, we could also send a command to the agent on selected endpoints to initiate a scan.

To explore the vulnerability of the managed endpoints in the environment, ESG selected the *Vulnerability Manager* from the menu. As shown in Figure 4, the vulnerability manager dashboard provided a comprehensive overview of the vulnerabilities discovered by the agent scan. The distribution of vulnerabilities by machine, type, criticality, and other factors was displayed. It also mapped malware and exploit kits to vulnerabilities that were being exploited in the wild. The dashboard included a panel detailing vulnerability mitigation statistics—the number of patches that needed to be applied to reduce or eliminate vulnerabilities.

Figure 4. Vulnerability Manager



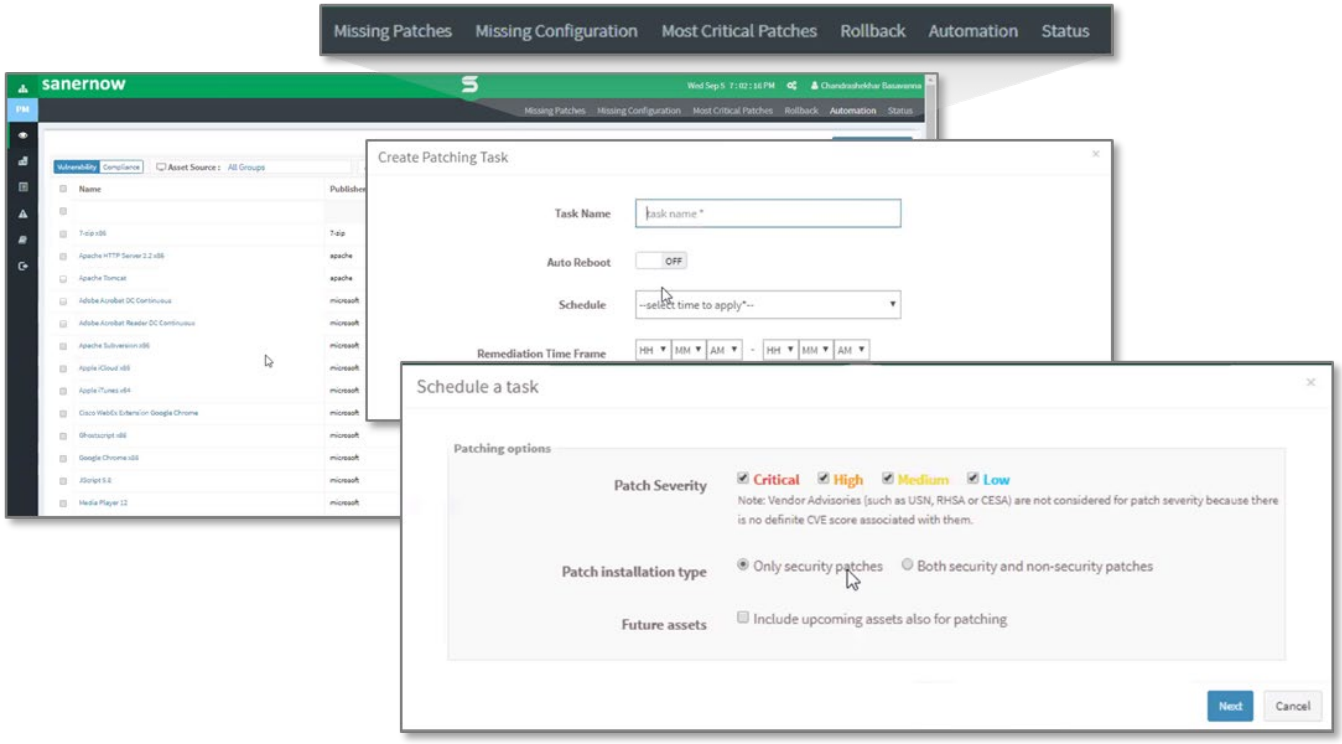
Source: Enterprise Strategy Group

The vulnerability manager enabled us to understand which endpoints were at risk, and what patches we needed to apply to reduce the risk. To apply the patches, we selected the *Patch Manager* from the menu. As shown in Figure 5, the patch manger provided a list of patches that could be applied to endpoints in the environment.

We selected a set of patches and then clicked ***apply selected patches.*** The ensuing pop-up enabled us to create and name the patching task, with options for when to apply the patches, and enable automatic reboot if necessary.

Using the top action item buttons, we were also able to create and schedule tasks to automatically patch systems as new patches were published, based on patch criticality and other factors. The top action item buttons also provided us the ability to monitor the status of patch tasks, and to roll back previously applied patches.

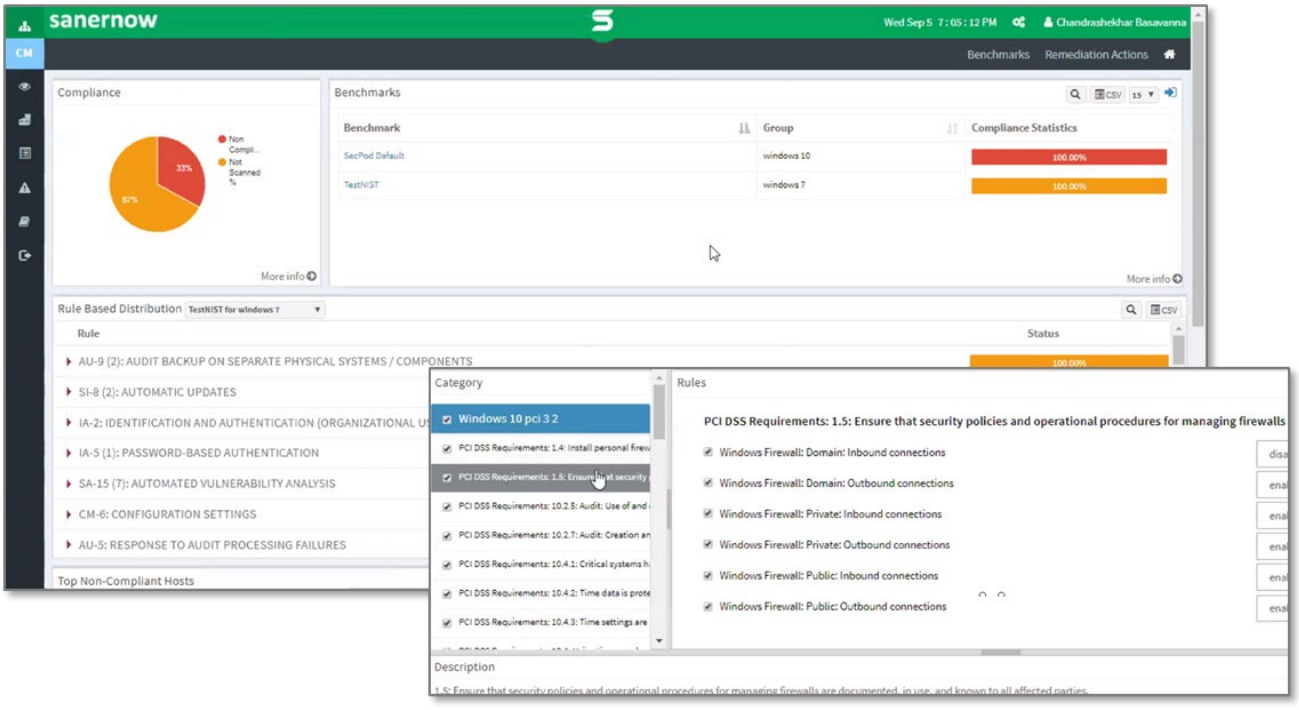
Figure 5. Patch Manager



Source: Enterprise Strategy Group

After applying patches to reduce endpoint risk, we selected the ***Compliance Manager*** from the menu to understand which endpoints were in compliance with regulatory standards and industry benchmarks. Shown in Figure 6, the compliance manager provided a display of compliance data gathered by the Saner agent during endpoint scans.

Figure 6. Compliance Manager



Source: Enterprise Strategy Group

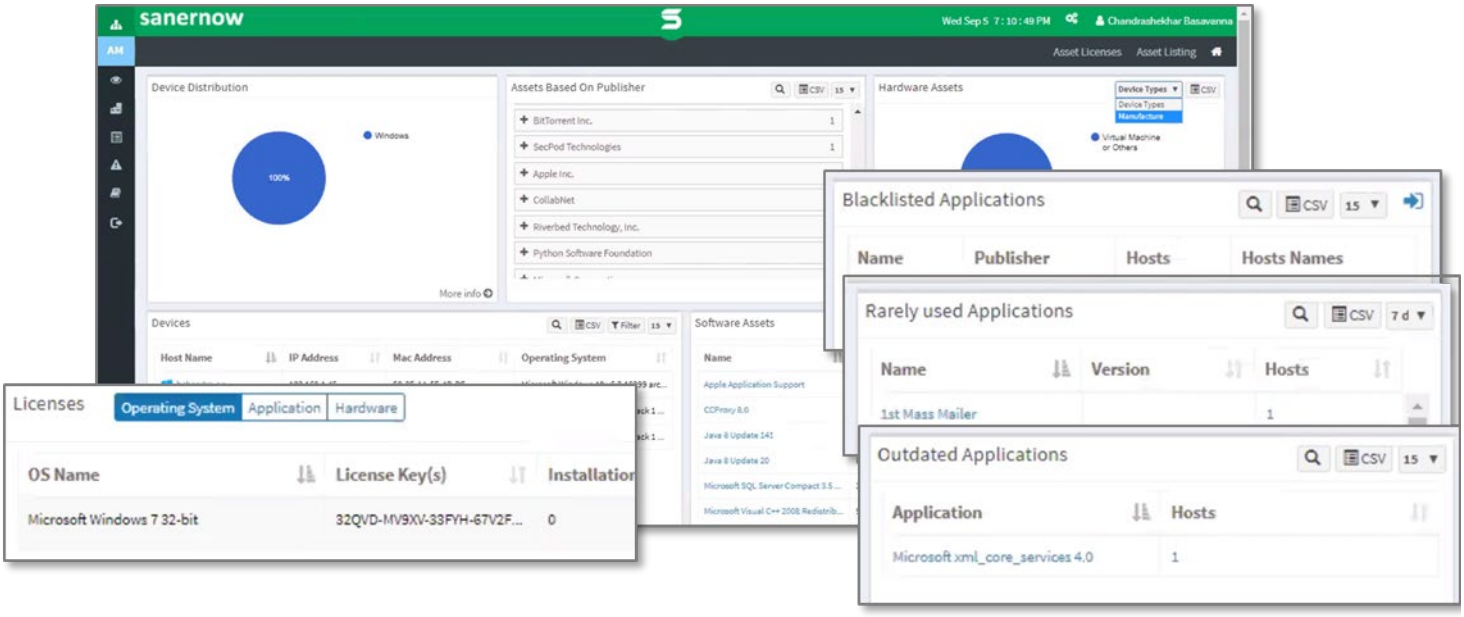
SanerNow comes with predefined checks for compliance with regulatory standards and industry benchmarks including PCI, HIPAA, NIST 800-53, and NIST 800-171. From the top action menu, ESG selected ***Benchmarks***, which brought up the benchmark editor, enabling us to create our own compliance benchmarks. We elected to customize a benchmark based on PCI 3.2 for Windows 10. Clicking on each item in the list brought up a description of the item, and the ability to edit the check for that item, as well as the ability to create our own checks.

Next, using the compliance manager dashboard, we reviewed the endpoints that were out of compliance. To fix those endpoints, we selected ***Remediation Actions*** from the top action menu. This brought us back to the patch manager, as shown in Figure 5. We then selected ***Missing Configuration*** from the top action menu. The ensuing pop-up enabled us to create and name the configuration remediation task which would modify the endpoint's configuration to bring it into compliance. As with patching tasks, SanerNow provides options for when to update the configuration and enable automatic reboot if necessary. These configuration remediations could be automatically applied to achieve continuous compliance through an Automation action menu item.

After bringing endpoints into compliance, we selected ***Asset Manager*** from the menu. Shown in Figure 7, the asset manager displayed comprehensive information on all software and hardware assets discovered by the Saner agent scans. Administrators can use SanerNow to track and manage OS, application, and hardware licenses. This provides cost management, enabling administrators to understand license usage, and reclaim resources when necessary.

The asset manager also listed installed blacklisted, rarely used, and outdated applications. Administrators can use this information to update or remove applications, thereby reducing the attack surface area of the endpoints in the environment.

Figure 7. Asset Manager



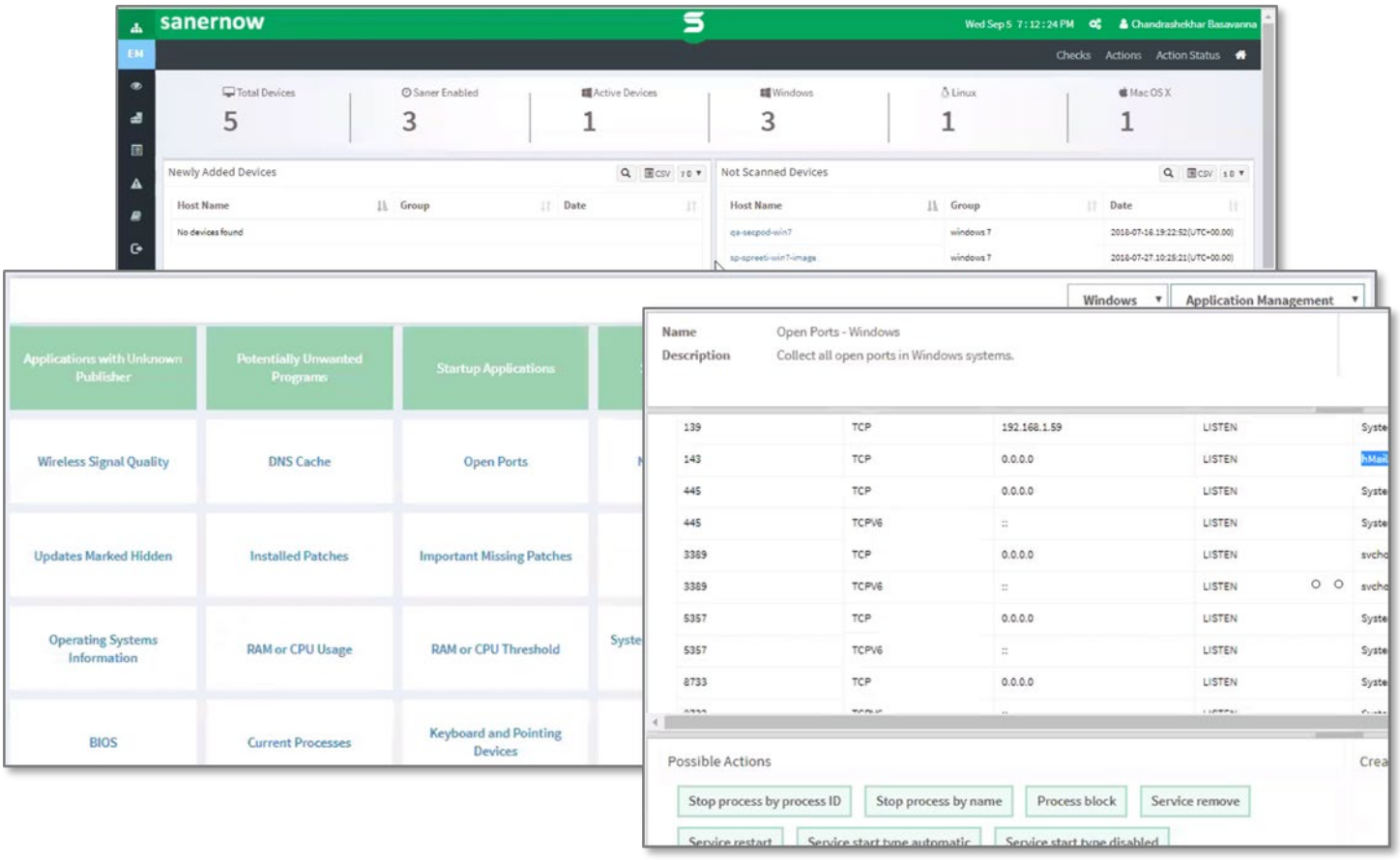
Source: Enterprise Strategy Group

Next, ESG selected ***Endpoint Manager*** from the menu. Shown in Figure 8, the endpoint manager provided summary information on the endpoints in the environment and provided facilities for the administrator to remotely manage the endpoint.

We clicked on ***Open Ports*** and SanerNow queried the selected endpoint for information on open network ports, displaying the results in a pop-up window. At the bottom of the window were action buttons that enabled us to manage the open ports by stopping or blocking processes, or starting, stopping, or disabling services.

The list of endpoint checks and actions is comprehensive, covering application, networking, OS, storage, BIOS, and other endpoint configurables.

Figure 8. Endpoint Manager



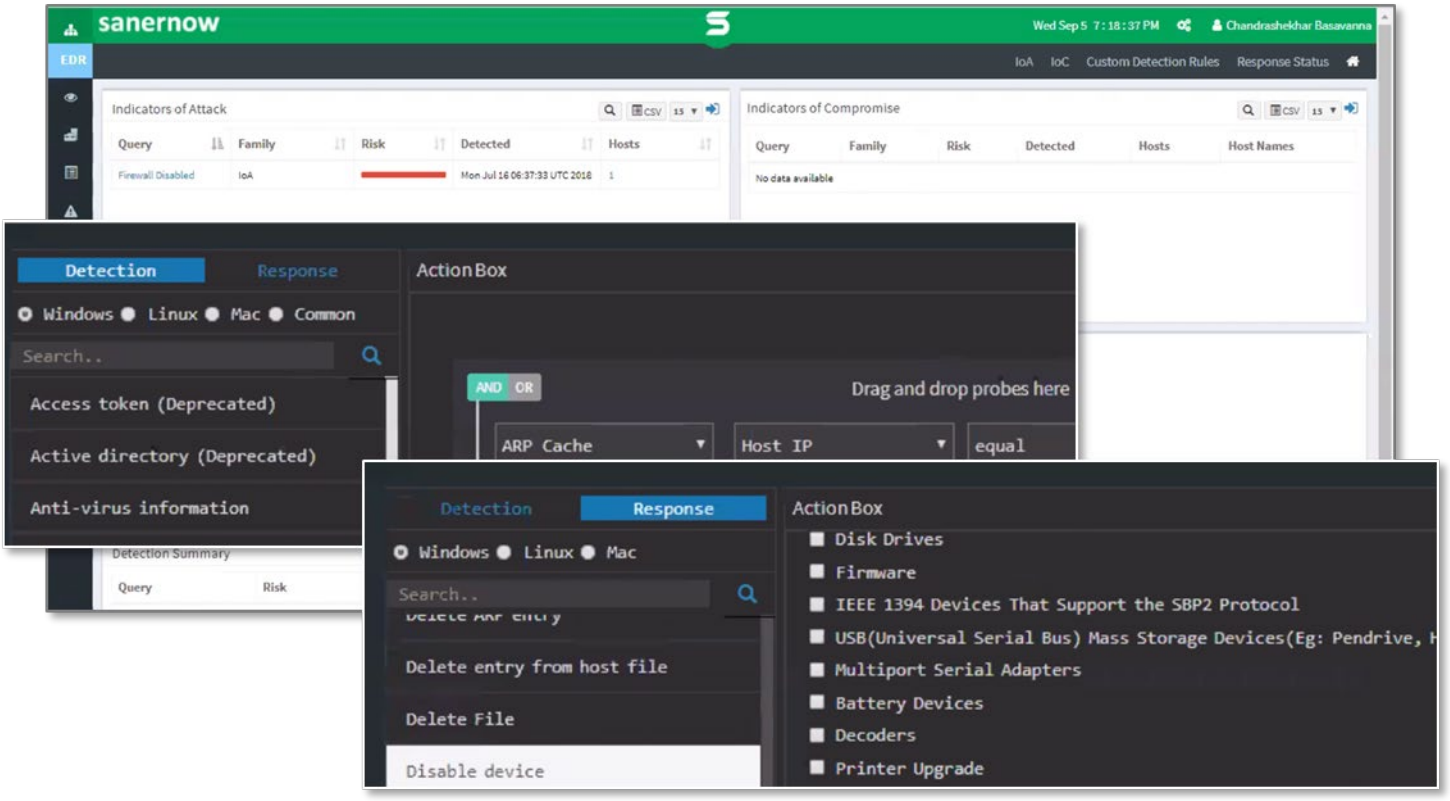
Source: Enterprise Strategy Group

As a final step in improving the security of the environment, we selected ***Endpoint Detection and Response*** from the menu. This brought up a summary detailing discovered indicators of attack (IoA) and indicators of compromise (IoC), as shown in Figure 9. Using the EDR screen, we set out to hunt existing threats in the environment.

We clicked on ***Detection*** to build our own custom IoC detection sequence. The simplicity of the detection builder enabled us to rapidly create a custom sequence by scrolling through the list of detectable items, clicking on ***ARP Cache***, and then providing a custom value to search. Clicking on the ***And/Or*** box enabled us to add another detectable item to the sequence, linking the detection criteria with and/or logic.

We then built a custom remediation sequence by clicking on ***Response***. Similar to the detection builder, the response builder enabled us to rapidly create a custom response sequence. In this case, we selected ***Disable Device*** to disable access to a device in response to our detection of compromise.

Figure 9. EDR



Source: Enterprise Strategy Group

Why This Matters

According to ESG research, 51% of surveyed organizations believe that their organizations have a problematic shortage of existing cybersecurity skills in their workforces.[3] When organizations deploy multiple point tools, each designed to address a specific endpoint problem, they exacerbate the skills gap.

SecPod designed SanerNow to address the challenges of multiple point tools with an integrated platform that reduces the complexity of endpoint security. ESG validated that the SanerNow platform incorporates the major features necessary to protect an organization's endpoints. Just a few mouse clicks are required to install the Saner agent on endpoints in the environment, after which the agent scans for vulnerability, inventory, configuration, patch, and other system details. We found it quick and easy to determine which endpoints were vulnerable to attack or out of compliance with regulatory and industry standards. A few more mouse clicks enabled us to manage the endpoints, reducing risk via patching, update configurations to bring systems into compliance, and remotely manage the systems. Integrated threat hunting and remediation features enabled us to rapidly find and fix compromised systems.

We observed that the SanerNow platform can replace multiple endpoint security point tools, simplifying the cybersecurity toolbox and obviating the need for a large staff of highly-skilled cybersecurity experts.

[3] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

The Bigger Truth

ESG asked IT executives and professionals to name the business initiatives that would drive the most IT spending at their organizations in 2018. Forty four percent cited strengthening cybersecurity, making it the most cited option in the list.[4] The traditional approach to achieving this goal is to acquire more tools to address perceived or existing weaknesses in the organization's cybersecurity strategy.

This approach is doomed to fail as it forces organizations to expend more scarce resources—time, money, effort, and, most importantly, staff—on acquiring and becoming experts in each new tool added to the cybersecurity toolbox. Instead of adding more tools, organizations need to look to integrated platforms that can reduce cybersecurity complexity.

SanerNow from SecPod is one such platform. Designed to meet the needs of organizations of any size, as well as MSPs and MSSPs, SanerNow is an integrated endpoint security platform that replaces multiple point tools and provides:

- Vulnerability management.
- Patch management.
- Compliance management.
- Endpoint management.
- Asset management.
- Threat detection and response.

During ESG's review of SanerNow, we were able to address a variety of risks and threats to endpoints quickly and simply. We installed the Saner agent on endpoints, and scanned for vulnerabilities, assets, configuration, and compliance. We used that information to determine which endpoints had exploitable vulnerabilities and addressed those vulnerabilities by applying the appropriate patches. Next, we determined which endpoints were out of compliance, and created tasks to update configurations, bringing the systems into compliance. Using SanerNow's threat detection and response engines, we quickly built complex queries for indicators of compromise and built remediation action scripts. We also used SanerNow to remotely manage endpoints, and to track hardware and software assets.

ESG Lab validated that SecPod's SanerNow endpoint security platform helps organizations overcome the cybersecurity skills gap with end-to-end endpoint security management, detection, analytics, response, and automation capabilities. For organizations that want to move beyond a large suite of point tools and leverage integrated platforms to reduce complexity and manage their costs, it would be worthwhile to take a closer look at SanerNow from SecPod.

[4] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.