AI Guided Security Management

Authors

Ashok Banerjee, Rudresha Murthy

Contributors

Mark Gentile, Archana Rajan

WHITE PAPER

Contents

The Security World Runs on Default

The endpoint security landscape is rapidly changing. *Attacks are evolving* – the number of ransomware variants and coin mining detections increased 46% and 8,500% respectively in 2017.[1] *Attack frequency is escalating* – 63 percent of organizations indicated they have seen an increase in attack frequency on their endpoints over the past year.[2] *Attack success rates are going up* – the number of companies that have been compromised by an attack that originated from an endpoint went up 20 percent over a 12-month period.[3] And the *costs of these attacks are rising* – the average cost of an endpoint attack is $440 per endpoint.[4]

Something needs to change. Given the reality that *resources available to combat all these risks are becoming scarcer* – it's expected there will be 3.5 million unfilled cybersecurity positions by 2021[5] – that change will likely have to be initiated by the technology used to manage security. On a daily basis, most security teams within most organizations are fighting an uphill battle – stretched to the breaking point trying to keep the lights on. This means, if your organization is like most, your security runs on default.

This means controls are not optimized or tuned to meet the real needs of the enterprise. Instead, rules and policies are typically set and then left. Administrators need to move on to the next thing. There is no time to come back to ensure everything remains effective in the face of new vulnerabilities and threats. No time to analyze what impact a configuration has on everything around it. No time to evaluate what should be changed based on current conditions to strengthen the organization's security posture. No time to address new vulnerabilities when they are identified – the average time to test and roll out a patch to endpoints is 102 days.[6]

Your organization probably barely has time to react. When you see something's happening it's usually too late - your organization has already been compromised. This sets in motion another whole set of tasks that consume a lot of your time, as you complete steps to investigate, analyze, remediate, and close out an incident. 70% of cybersecurity professionals claimed their organization was spending most of their time dealing with the emergency of the day.[7] This leaves little time for training, planning, or strategy and it makes it virtually impossible to be proactive in your security measures.

The Symantec Cyber Defense Manager fixes this broken security management paradigm, automating security analysis and tasks to give you back precious time and allow you to take charge and create consistent security practices. This paper describes how Symantec Cyber Defense Manager introduces autonomous self-driving security, with an engine guided by Artificial Intelligence (AI) that can evaluate current conditions, recommend appropriate actions, which can be executed via automated workflows, when necessary, apply fixes, and continue to learn to identify ways to help your organization improve the efficiency and effectiveness of your defenses.

Dynamic Defenses Are Needed to Protect Against Dynamic Attackers

Deploying static security against dynamic adversaries is a losing battle. Default, set and forget policies are not going to protect your ever-changing environment from the ever-evolving threats targeting it. You need near real-time, dynamic defenses to protect against the dynamic landscape you are facing. This takes security management that can automatically analyze current conditions, spot vulnerabilities and threats, and modify policies and take necessary steps to shut them down.

To accomplish requires a security management platform that can automate the following stages of the security management lifecycle:

- **Deep Insights** – highlighting and prioritizing issues and threats based on the potential impact they can have on your organization's data, resources and operations. The solution should continuously correlate and analyze information generated by all the different security solutions in the environment, using advanced analytics and machine learning (ML), to be able to identify what's normal behavior and what's suspicious and indicative of a potential attack.
- **Recommendations** – providing the actions and workflows that will effectively address the threat or issue facing your organization. The solution should present recommendations in context and include the impact any action will have on your environment, so you can determine which course will be best for your organization.
- **Remediation** – managing the workflow to execute the tasks that will not only completely remove the threat, but also enhance the overall security of the environment. The solution should ensure your organization can not only fully recover from an incident, but also institute policy changes that create a stronger security stance, by implementing more robust controls that can automatically apply to subsequent detections to head off similar risks in the future.
- **Learning** – continuously learning about security events, threats, device profiles and the environment, so recommendations can be tuned to better meet the needs and risk tolerance levels of your organization. The solution should consider general user behaviors and administrative tendencies when it makes recommendations or automatically applies actions.

Symantec designed its Cyber Defense Manager with these capabilities in mind to give you a security management platform that can automatically learn, analyze, recommend and apply actions to proactively address vulnerabilities and speed responses to security events.

[1] *"Internet Security Threat Report, Volume 23" Symantec, March 2018.*
[2] *"The 2018 State of Endpoint Security Risk," Ponemon Institute LLC, October 2018.*
[3] *"The 2018 State of Endpoint Security Risk," Ponemon Institute LLC, October 2018.*
[4] *"The 2018 State of Endpoint Security Risk," Ponemon Institute LLC, October 2018.*
[5] *"Cybersecurity Jobs Report 2018-2021," Cybersecurity Ventures, Steve Morgan, May 31, 2017, https://cybersecurityventures.com/jobs/.*
[6] *"The 2018 State of Endpoint Security Risk," Ponemon Institute LLC, October 2018.*
[7] *"ESG Research Suggests Cybersecurity Skills Shortage is Getting Worse," by Jon Oltsik, Jan. 11, 2018, https://www.esg-global.com/blog/esg-research-suggests-cybersecurity-skills-shortage-is-getting-worse.*

Symantec Cyber Defense Manager

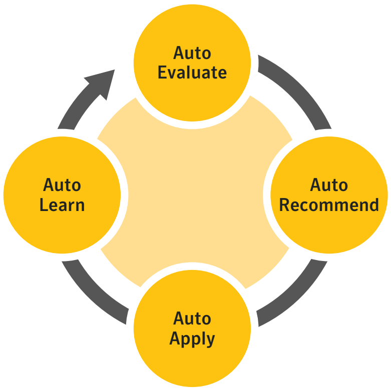
Symantec Cyber Defense Manager introduces the concept of autonomous, self-driving security with its AI-guided Engine that automates, end-to-end, your daily security management and operations. Cyber Defense Manager helps you improve your security practices and bring consistency across your organization, via automated standard workflows to adapt and strengthen your overall security posture.

The Cyber Defense Manager uses advanced AI and ML to improve prevention through policy recommendations and automation – uniquely combining admin and user behavior intelligence, indicators of compromise (IoC) and historical anomalies to identify threats. It then adapts endpoint policies to keep them up to date and aligned with the current risk profile of your organization.

The Full Security Lifecycle

The Cyber Defense Manager frees up your precious resources by automating each and every phase of the security management lifecycle:

- **Auto Evaluate** – Cyber Defense Manager correlates and analyzes events, device configurations, device locations, discovered files & applications, accessed URLs, agent operational states, and connected networks. This data, along with reputation, prevalence, and known vulnerabilities are then fed into the AI/ML classification and recommendation engine to adapt policy and strengthen prevention.
- **Auto Recommend** – Cyber Defense Manager will make recommendations, in prioritized order, how best to address the vulnerabilities or threats in your environment, based on the types of devices involved (workstation, fixed function, satellite, etc.) and potential risk it poses to sensitive data and business operations.
- **Auto Apply** – Cyber Defense Manager can automatically complete part or all of the recommended workflow, based on your input, to ensure the incident is resolved to your satisfaction. It can automate workflow execution including escalation flow, all without manual intervention.

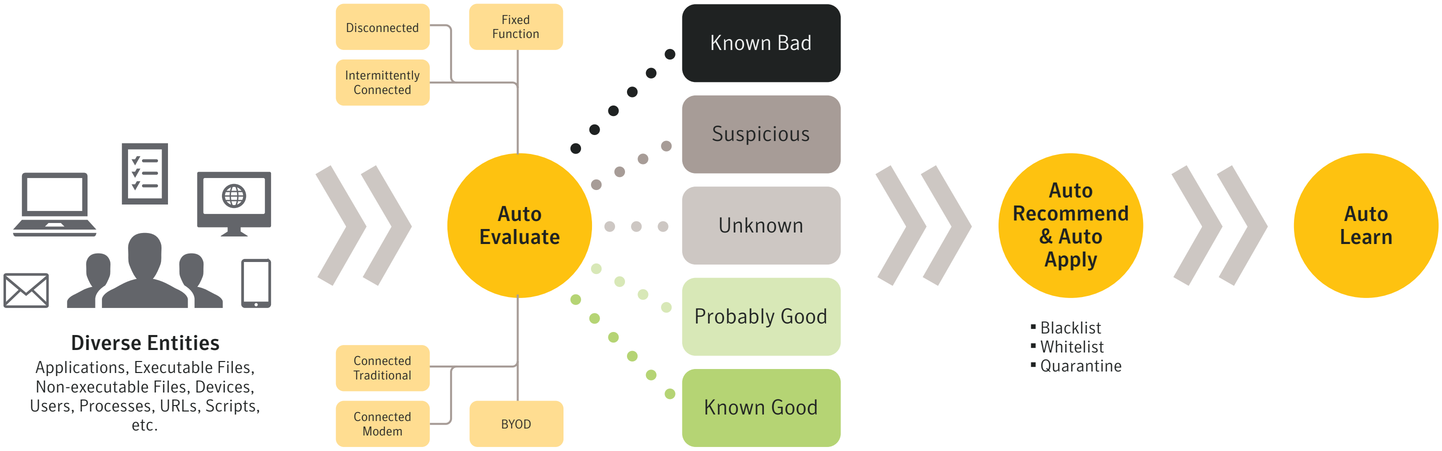


- **Auto Learn** – Cyber Defense Manager applies artificial intelligence and machine learning to continuously improve recommendations and auto apply. For example, it can automatically determine thresholds or rules, based on the historical sequence of events in your environment.

There is no more guesswork, no more manual to-do-lists – Symantec Cyber Defense Manager lays it all out for you and then applies the changes necessary to keep your security policies current.

The Most Complete AI-Guided Security Management

Auto Evaluate → Auto Classify → Auto Recommend → Auto Apply → Auto Learn

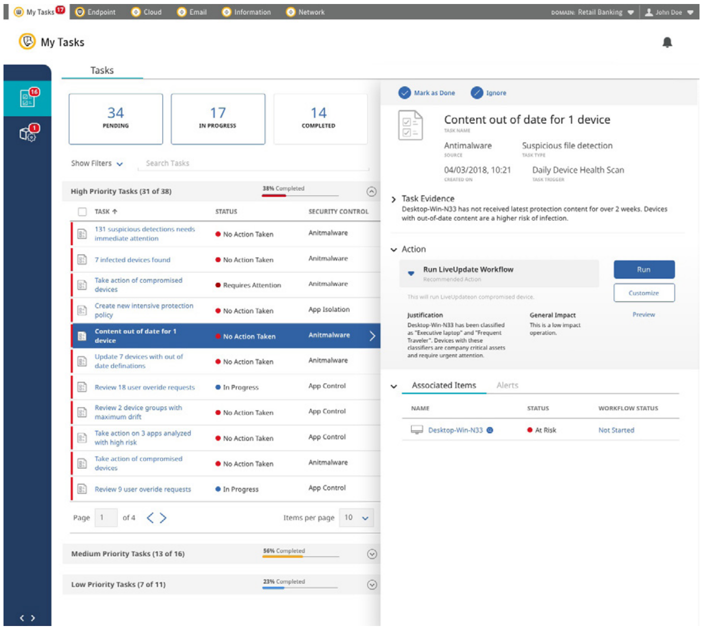


You determine which course of action you want to take, and Symantec orchestrates its execution. This enables you to proactively **improve your compliance hygiene, strengthen your security stance, and drastically reduce your total cost of ownership (TCO)**.

How Symantec Cyber Defense Manager Works

Cyber Defense Manager closes the loop between suspicious activity, threats, vulnerabilities and security incidents and the policies in place to prevent and shut them down.

Within the "My Tasks" section of your dashboard, Cyber Defense Manager provides analysis on all the logs and events from the Symantec solutions you have deployed, such as Symantec Endpoint Protection (SEP). It uses advanced artificial intelligence and machine learning technologies, which are augmented by the Symantec Threat Intelligence Feed, to understand the context and level of urgency of the event – What type of device is it targeting? What is it trying to do? How many other devices are potentially impacted? Based on the analysis, Cyber Defense Manager will prioritize the events for you, so you know exactly where to focus first.



34	17	14
PENDING	IN PROGRESS	COMPLETED

High Priority Tasks (31 of 38) 38% Completed

TASK	STATUS	SECURITY CONTROL
131 suspicious detections needs immediate attention	● No Action Taken	Anitmalware
7 infected devices found	● No Action Taken	Anitmalware
Take action of compromised devices	● Requires Attention	Anitmalware
Create new intensive protection policy	● No Action Taken	App Isolation
Content out of date for 1 device	● No Action Taken	Anitmalware
Update 7 devices with out of date definations	● No Action Taken	Anitmalware
Review 18 user overide requests	● In Progress	App Control
Review 2 device groups with maximum drift	● No Action Taken	App Control
Take action on 3 apps analyzed with high risk	● No Action Taken	App Control
Take action of compromised devices	● No Action Taken	Anitmalware
Review 9 user overide requests	● In Progress	App Control

Page 1 of 4 Items per page 10

Medium Priority Tasks (13 of 16) 56% Completed

Low Priority Tasks (7 of 11) 23% Completed

Content out of date for 1 device
TASK NAME

Antimalware
SOURCE

Suspicious file detection
TASK TYPE

04/03/2018, 10:21
CREATED ON

Daily Device Health Scan
TASK TRIGGER

Task Evidence
Desktop-Win-N33 has not received latest protection content for over 2 weeks. Devices with out-of-date content are a higher risk of infection.

Action

Run LiveUpdate Workflow
Recommended Action

This will run LiveUpdateon compromised device.

Justification
Desktop-Win-N33 has been classified as "Executive laptop" and "Frequent Traveler". Devices with these classifiers are company critical assets and require urgent attention.

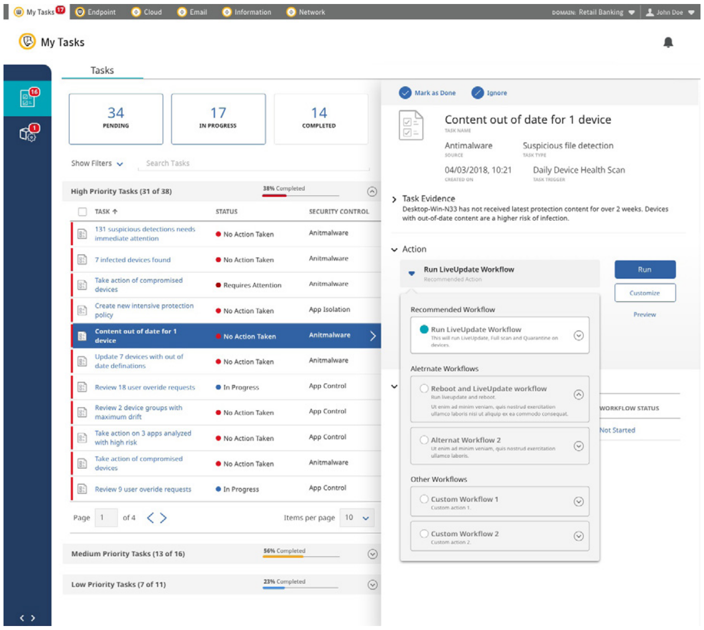
General Impact
This is a low impact operation.

NAME	STATUS	WORKFLOW STATUS
Desktop-Win-N33	● At Risk	Not Started

Figure 1. "My Tasks" in Cyber Defense Manager Prioritizes Events, Recommends Actions & Automates Responses

Cyber Defense Manager lays out what next steps could be, based on best practices followed by peers in the same domain or with a similar profile or, learned from your environment, over time. Cyber Defense Manager provides the potential impact of each action, so you know beforehand what it will do to the environment – How many devices it impacts, which policies it affects, etc.

You can take all or some of the actions Cyber Defense Manager recommends. Based on what you choose, Cyber Defense Manager will automate the coordination and execution of those actions to close out the incident.



34	17	14
PENDING	IN PROGRESS	COMPLETED

High Priority Tasks (31 of 38) 38% Completed

TASK	STATUS	SECURITY CONTROL
131 suspicious detections needs immediate attention	● No Action Taken	Anitmalware
7 infected devices found	● No Action Taken	Anitmalware
Take action of compromised devices	● Requires Attention	Anitmalware
Create new intensive protection policy	● No Action Taken	App Isolation
Content out of date for 1 device	● No Action Taken	Anitmalware
Update 7 devices with out of date definations	● No Action Taken	Anitmalware
Review 18 user overide requests	● In Progress	App Control
Review 2 device groups with maximum drift	● No Action Taken	App Control
Take action on 3 apps analyzed with high risk	● No Action Taken	App Control
Take action of compromised devices	● No Action Taken	Anitmalware
Review 9 user overide requests	● In Progress	App Control

Page 1 of 4 Items per page 10

Medium Priority Tasks (13 of 16) 56% Completed

Low Priority Tasks (7 of 11) 23% Completed

Content out of date for 1 device
TASK NAME

Antimalware
SOURCE

Suspicious file detection
TASK TYPE

04/03/2018, 10:21
CREATED ON

Daily Device Health Scan
TASK TRIGGER

Task Evidence
Desktop-Win-N33 has not received latest protection content for over 2 weeks. Devices with out-of-date content are a higher risk of infection.

Action

Run LiveUpdate Workflow
Recommended Action

Recommended Workflow

● Run LiveUpdate Workflow
This will run LiveUpdate, Full scan and Quarantine on devices.

Aletrnate Workflows

○ Reboot and LiveUpdate workflow
Run liveupdate and reboot.
Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

○ Alternat Workflow 2
Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris.

Other Workflows

○ Custom Workflow 1
Custom action 1.

○ Custom Workflow 2
Custom action 2.

WORKFLOW STATUS
Not Started

Figure 2. Best Practice Recommendations Are Presented to Help You Close Out an Incident, Fast

It will then take cues from your decisions over time and incorporates your preferences into future recommendations and remediation actions. For example, it will incorporate whether you are conservative or aggressive in the measures you take to protect certain types of devices into its logic to continually improve its efficacy and smooth your path to self-driving security management.

Events Cyber Defense Manager Evaluates

The goal of Cyber Defense Manager is to make recommendations and auto-tune policies in response to security events to strengthen your security stance and improve your overall security and compliance hygiene. There are generally three types of events – product, enterprise, global - that trigger evaluation:

Product Events

Cyber Defense Manager will look for events of significance generated by one of Symantec's solutions, such as SEP, that warrants an instantaneous change in policy. It may look for policy violations, micro-segmentation violations, file integrity monitoring violations, deceptors that were touched or triggered, the number of detections, the frequency of the detections, as well as any information gathered by App Isolation, which isolates suspicious apps, based on the threat levels they pose, and allows them to run certain capabilities within a safe, contained environment. Cyber Defense Manager will determine whether these events are a violation or indicator of attack (IoA), in which case a policy may need to be tuned to bolster protections to ensure it doesn't become a compromise (IoC), or a false positive, in which case a policy may need to be adjusted to reduce the noise.

Organization-wide Attack

Cyber Defense Manager will look for events that, when correlated with other events across the organization, indicate an attack. It will look for the breadth and frequency of detections to determine if they are isolated to a specific group or department or organization-wide. This will determine whether the attacks are likely coming from an internal or external attacker, which has significantly different policy implications. It will also look for behaviors that indicate an imminent attack. To ensure your data remains private and operations uninterrupted, Cyber Defense Manager will evaluate your policies in light of targeted attacks and recommend changes that will improve your defensive posture.

Global Attacks

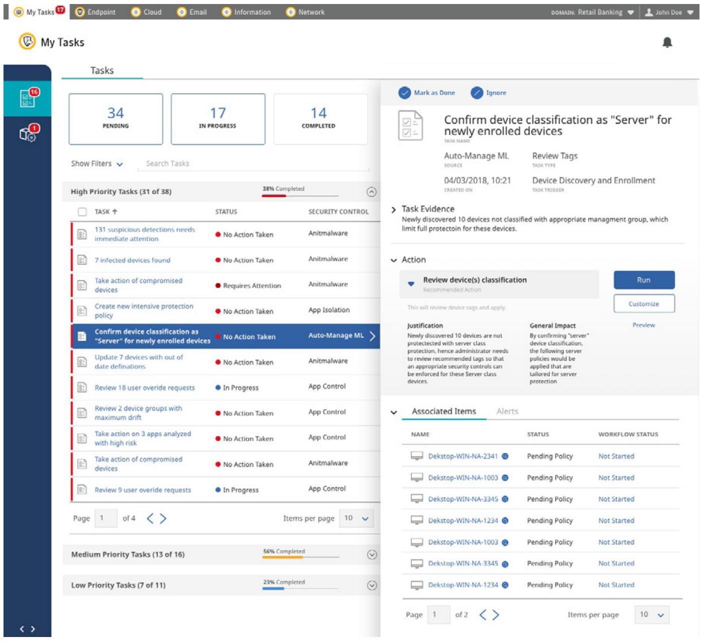
Cyber Defense Manager will look for attacks that are present on a global scale and identify policy changes that will help you minimize their impact. This refers to the large-scale attacks, such as WannaCry or Petya, that cause wide-scale disruption. Threat intelligence from the Symantec Global Intelligence Network, which monitors and analyzes billions of endpoints worldwide, often gives Symantec visibility into threats as soon as they emerge. When identified, Cyber Defense Manager will likely recommend updating your intrusion prevention systems (IPS) or technologies to provide coverage for the attack. When it's in outbreak mode, Cyber Defense Manager may give more aggressive recommendations, which customers may be more apt to take, to ensure the organization is not compromised.

A Look at Cyber Defense Manager in Action

Let's look at a few use cases for Symantec Cyber Defense Manager:

Strengthening Security Stance Use Case

Cyber Defense Manager can help you stay on top of the constant changes within your environment to maintain and strengthen your security stance. For example, when a new device is added to your network, Cyber Defense Manager can automate its classification and recommend security policy configurations to ensure it is appropriately protected, based on the inventory, traffic patterns and threats that have been seen against those kinds of devices. You can determine which policies you want to apply to ensure your security remains in force through all the changes taking place in your environment.



34 PENDING | 17 IN PROGRESS | 14 COMPLETED

High Priority Tasks (31 of 38) — 38% Completed

TASK	STATUS	SECURITY CONTROL
131 suspicious detections needs immediate attention	No Action Taken	Anitmalware
7 infected devices found	No Action Taken	Anitmalware
Take action of compromised devices	Requires Attention	Anitmalware
Create new intensive protection policy	No Action Taken	App Isolation
Confirm device classification as "Server" for newly enrolled devices	No Action Taken	Auto-Manage ML
Update 7 devices with out of date definations	No Action Taken	Anitmalware
Review 18 user overide requests	In Progress	App Control
Review 2 device groups with maximum drift	No Action Taken	App Control
Take action on 3 apps analyzed with high risk	No Action Taken	App Control
Take action of compromised devices	No Action Taken	Anitmalware
Review 9 user overide requests	In Progress	App Control

Page 1 of 4 — Items per page 10

Medium Priority Tasks (13 of 16) — 56% Completed

Low Priority Tasks (7 of 11) — 23% Completed

Confirm device classification as "Server" for newly enrolled devices
TASK NAME

Auto-Manage ML
SOURCE

Review Tags
TASK TYPE

04/03/2018, 10:21
CREATED ON

Device Discovery and Enrollment
TASK TRIGGER

Task Evidence
Newly discovered 10 devices not classified with appropriate managment group, which limit full protectoin for these devices.

Action
Review device(s) classification
Recommended Action
This will review device tags and apply.

Justification
Newly discovered 10 devices are not protectected with server class protection, hence administrator needs to review recommended tags so that an appropriate security controls can be enforced for these Server class devices.

General Impact
By confirming "server" device classification, the following server policies would be applied that are tailored for server protection

NAME	STATUS	WORKFLOW STATUS
Dekstop-WIN-NA-2341	Pending Policy	Not Started
Dekstop-WIN-NA-1003	Pending Policy	Not Started
Dekstop-WIN-NA-3345	Pending Policy	Not Started
Dekstop-WIN-NA-1234	Pending Policy	Not Started
Dekstop-WIN-NA-1003	Pending Policy	Not Started
Dekstop-WIN-NA-3345	Pending Policy	Not Started
Dekstop-WIN-NA-1234	Pending Policy	Not Started

Page 1 of 2 — Items per page 10

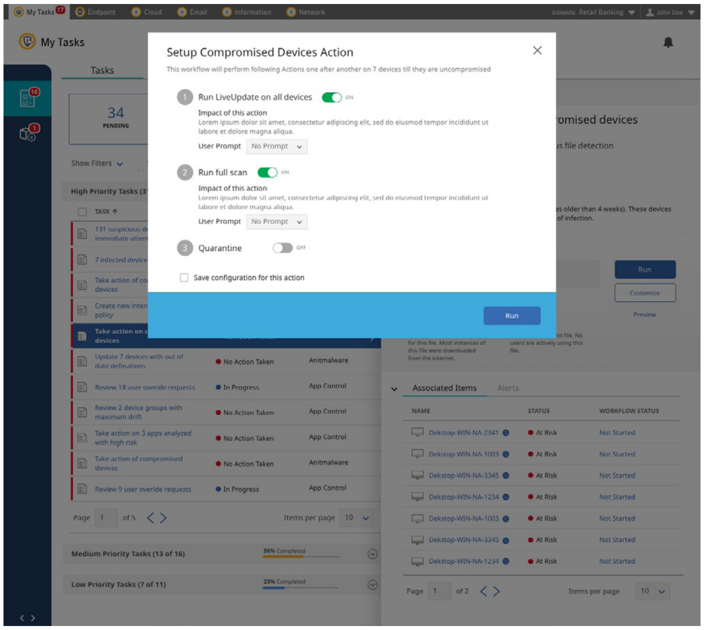
Figure 3. Keep Up with Your Dynamic Environment – Defense Manager Automates Device Classification & Policy Recommendations

Improving Compliance Hygiene Use Case

Cyber Defense Manager can help you apply best practices and ensure ongoing enforcement that aligns with your compliance requirements. For example, it can help you identify data exfiltration that indicates sensitive, regulated information is leaving your organization or out of your control. It could look at historical outbound patterns and, using AI and ML, automatically determine which outbound connections are suspicious and could be compromising the privacy and integrity of your data. Cyber Defense Manager can identify anomalous behavior at an individual device-level or organization-wide. Based on the detection, it will recommend appropriate actions to close the vulnerability and keep you in compliance.

Reduce Total Cost of Ownership Use Case

Identifying and then fixing compromised devices in your environment can be labor-intensive and time-consuming. Symantec Cyber Defense Manager can drastically reduce this workload, automating the identification of all impacted devices, recommending the appropriate fixes and then implementing them – e.g. remove file, reboot device, quarantine device, etc. Cyber Defense Manager tells you exactly what the incident entails and what it means for your organization, detailing the impact of the threat and the potential remediation actions. You can customize the implementation of the remediation workflow – dictating exactly which steps you want to complete for which devices, or even excluding some devices altogether. You can even determine if or how you want to involve the user in the remediation.



Setup Compromised Devices Action

This workflow will perform following Actions one after another on 7 devices till they are uncompromised

1. Run LiveUpdate on all devices — ON
   Impact of this action
   Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.
   User Prompt: No Prompt
2. Run full scan — ON
   Impact of this action
   Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.
   User Prompt: No Prompt
3. Quarantine — OFF

☐ Save configuration for this action

Run

TASK ↑		
131 suspicious d immediate attent		
7 infected device		
Take action of co devices		
Create new inten policy		
Take action on c devices		
Update 7 devices with out of date definations	● No Action Taken	Anitmalware
Review 18 user overide requests	● In Progress	App Control
Review 2 device groups with maximum drift	● No Action Taken	App Control
Take action on 3 apps analyzed with high risk	● No Action Taken	App Control
Take action of compromised devices	● No Action Taken	Anitmalware
Review 9 user overide requests	● In Progress	App Control

Page 1 of 5 — Items per page 10

Medium Priority Tasks (13 of 16) — 56% Completed

Low Priority Tasks (7 of 11) — 23% Completed

omised devices

s file detection

es older than 4 weeks). These devices of infection.

for this file. Most instances of this file were downloaded from the internet.

is file. No users are actively using this file.

NAME	STATUS	WORKFLOW STATUS
Dekstop-WIN-NA-2341	● At Risk	Not Started
Dekstop-WIN-NA-1003	● At Risk	Not Started
Dekstop-WIN-NA-3345	● At Risk	Not Started
Dekstop-WIN-NA-1234	● At Risk	Not Started
Dekstop-WIN-NA-1003	● At Risk	Not Started
Dekstop-WIN-NA-3345	● At Risk	Not Started
Dekstop-WIN-NA-1234	● At Risk	Not Started

Page 1 of 2 — Items per page 10

Figure 4. Defense Manager Makes It Easy to Customize Remediation Implementations

Summary

Default security is all most organizations can handle. They are treading water, tackling daily fire-drills and an ever-growing threat landscape, with no real way to get ahead. Symantec Cyber Defense Manager changes that, introducing autonomous, self-driving security with an AI-guided Engine that automates complex workflows, so you can quickly address current issues and improve your overall security posture. Cyber Defense Manager automates every step of the security management lifecycle – analysis, recommendation, remediation, and policy tuning – to allow you to easily customize business and security rules to ensure enforcement is in line with your company's risk profile and security objectives.

With Cyber Defense Manager, you can execute sophisticated workflows with a click of a button to quickly and effectively address threats and close vulnerabilities to strengthen your defenses. The Cyber Defense Manager can perform daily security operations and automate decision-making and execution to eliminate your time-consuming processes and to-do-lists.

It continuously learns about your administrative tendencies, using AI and ML, to ensure, it can match priorities, recommendations, and responses to your organization's specific needs and tolerance to risk. You can also easily build custom workflows to meet your organization's unique needs. This allows you to easily and effectively scale your defenses to maintain compliance and meet growing demands and threats.

More Information

For more information, please visit the Symantec Endpoint Security website at **https://www.symantec.com/products/endpoint**.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec.
350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | **www.symantec.com**