SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

# Avert Cyber Attacks With Proactive Endpoint Hardening

A guide to achieve the speed you need to stay secure

A vulnerability has been exposed.
Attackers will need only seven days to weaponize it.

Your secret to averting cyber attacks?

# Powerful, Proactive Endpoint Hardening

That remediates zero-day vulnerabilities within 24 hours and critical vulnerabilities within 72 hours.

# Contents

# Introduction

# Increasing the Velocity of Your Cyber Defense

**Patch management, configuration drift, software deployment — these challenges bleed organizations of resources, take mind-numbing amounts of time to handle, and distract IT leaders from the strategy and innovation they should be focusing on.**

These factors (particularly patch management) are among the biggest sources of risk a company faces.

**When adversaries need just seven days to weaponize a vulnerability, the clock effectively starts the moment the vulnerability is disclosed.**

Now more than ever, IT organizations need to consider how to increase the velocity and agility of their operations to manage these risks.

The correct response to these challenges is cyber hygiene, with an emphasis on endpoint hardening. The Center for Internet Security (CIS) defines cyber hygiene as a set of baseline practices that preemptively protect organizations from cyber threats. Cyber hygiene has to cover every device in your ecosystem, whether it's on-premises or remote, so the implementation can be more difficult than the theory.

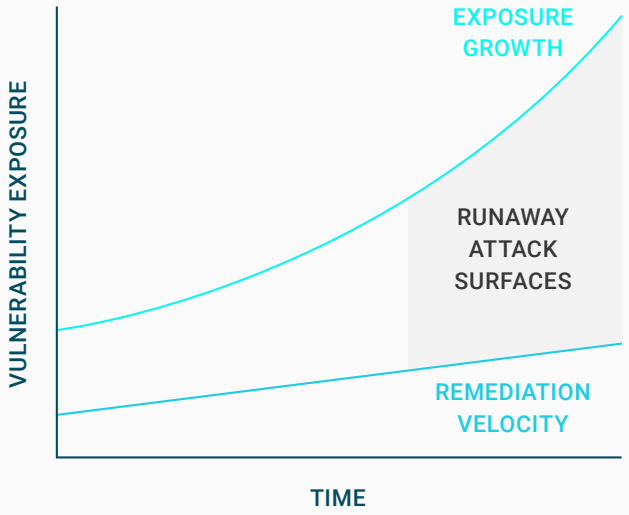
To help, CIS has provided an authoritative set of controls to assist organizations with evaluating and planning their cyber hygiene. This gives us all a clear set of guidelines, though the specific tools for putting these concepts into place are up to companies to source.

## Inconvenient math

**22K** vulnerabilities disclosed per year

**7** days on average to weaponize

**102** days on average to deploy critical patches



**6 in 10** security practitioners lack context on the business impacts of a breach.[1]

**44%** of cybersecurity professionals are not confident that their organization can avoid a breach.[1]

**More than 2/3** of security teams admit taking a month or more to fix known software vulnerabilities.[1]

**74%** of companies feel that they can't patch fast enough because they lack the staff resources.[1]

1. Ponemon Institute. (February 2019). Challenging State of Vulnerability Management: Gaps in Resources, Risk and Visibility Weaken Cybersecurity Posture. Commissioned by Balbix.

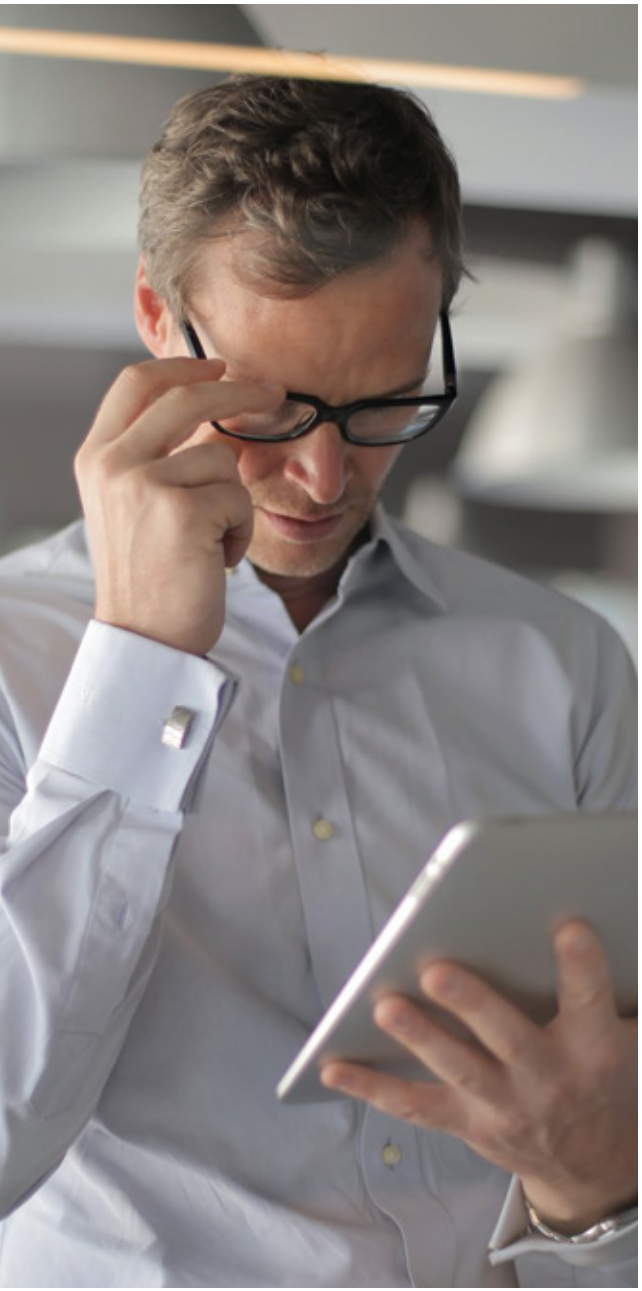
## IN THIS GUIDE

Automox has stepped in with a new Endpoint Hardening Maturity Matrix, which helps companies understand their path to be able to act faster than their adversaries. It is a natural complement to Automox's endpoint hardening cyber hygiene platform, which addresses several of the most important CIS Controls® and gives organizations a complete, cloud-native solution.

We also introduce new guidance on the velocity required for organizations to proactively harden their systems — what we refer to as a 24/72 threshold to harden your corporate endpoints once a vulnerability is disclosed. This clearly defines what SecOps and IT organizations should be working toward.

Throughout, our principles integrate the best practices offered by the CIS (and others), as well as our own firsthand data and client experiences.

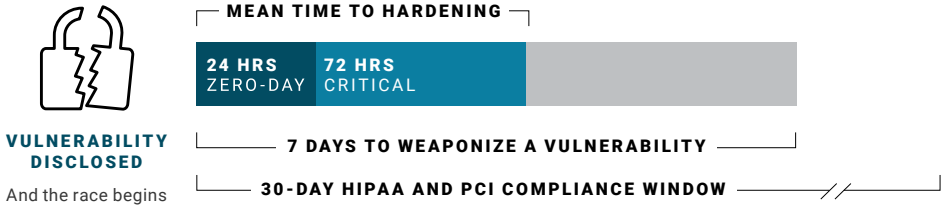
**By the end, you'll see your way to impactful cyber hygiene, with the emphasis on endpoint hardening, and you'll have the necessary tools in front of you to implement it.**



# Rethinking IT velocity

# How Fast Do You Really Need to Move?

Data shows that adversaries weaponize vulnerabilities within seven days — typically, that is roughly 15 times faster than organizations are acting.




Clearly, to achieve a sustainable cyber hygiene posture, organizations need to focus on the velocity of their endpoint hardening. Speed is essential to a proactive stance.

Bottom line: Zero-day vulnerabilities need to be patched within 24 hours and all other critical vulnerabilities within 72 hours. This is the 24/72 endpoint hardening threshold. Outside this threshold, hardening increasingly becomes a reactive exercise with little to no pre-incursion value.

### THE ALL-OUT DRAG RACE OF ZERO-DAYS

Zero-day incursions are the statistical exception rather than the rule, since they account for less than one-tenth of 1% of the 20,000-plus vulnerabilities that we see accumulating year over year. But when they do occur, the response window is 24 hours from the time of disclosure.

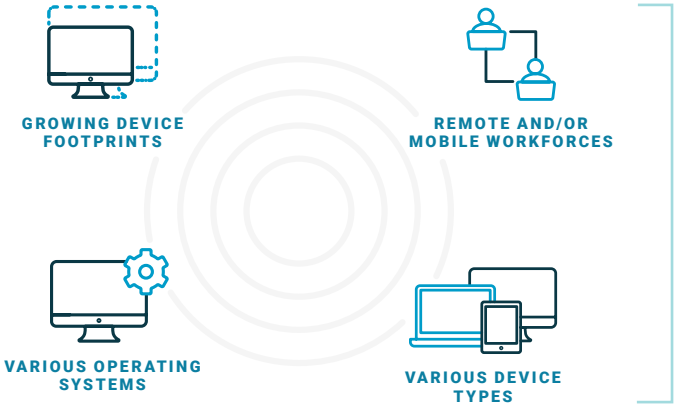
**This 24-hour threshold for zero-day vulnerabilities is the new norm for establishing a true, all-encompassing cyber hygiene practice.**

## WHY ARE WE TALKING ABOUT THIS NOW?

Today, the rise of patch management and related challenges coincides with many companies' broader adoption of digital transformation plans. This is both an opportunity and a problem. On one hand, many companies are (rightly) disposed to adopting cloud-native solutions, automating legacy processes, and rethinking their IT ecosystems; on the other, they are often so strapped for resources during this time of transition that cyber hygiene gets pushed down to a secondary priority — until it comes back to haunt them.

This is why Automox talks so much about how cyber hygiene makes you a smaller, faster target: You don't have to invest in so much cumbersome armor, which lightens your security load. In our experience, organizations can sidestep up to 80–90% of cyber threats with good cyber hygiene — allowing them to focus on the strategy and transformations that will help their business thrive.

### It might help to think of this the other way around and ask, "What are the factors that make us a bigger target?" Here are some notable ones:




**Cyber hygiene can address each of these factors,** effectively shrinking your vulnerability potential so it's even smaller than the old days when everything could be handled and protected on-premises.

# Benefits On Top of Benefits

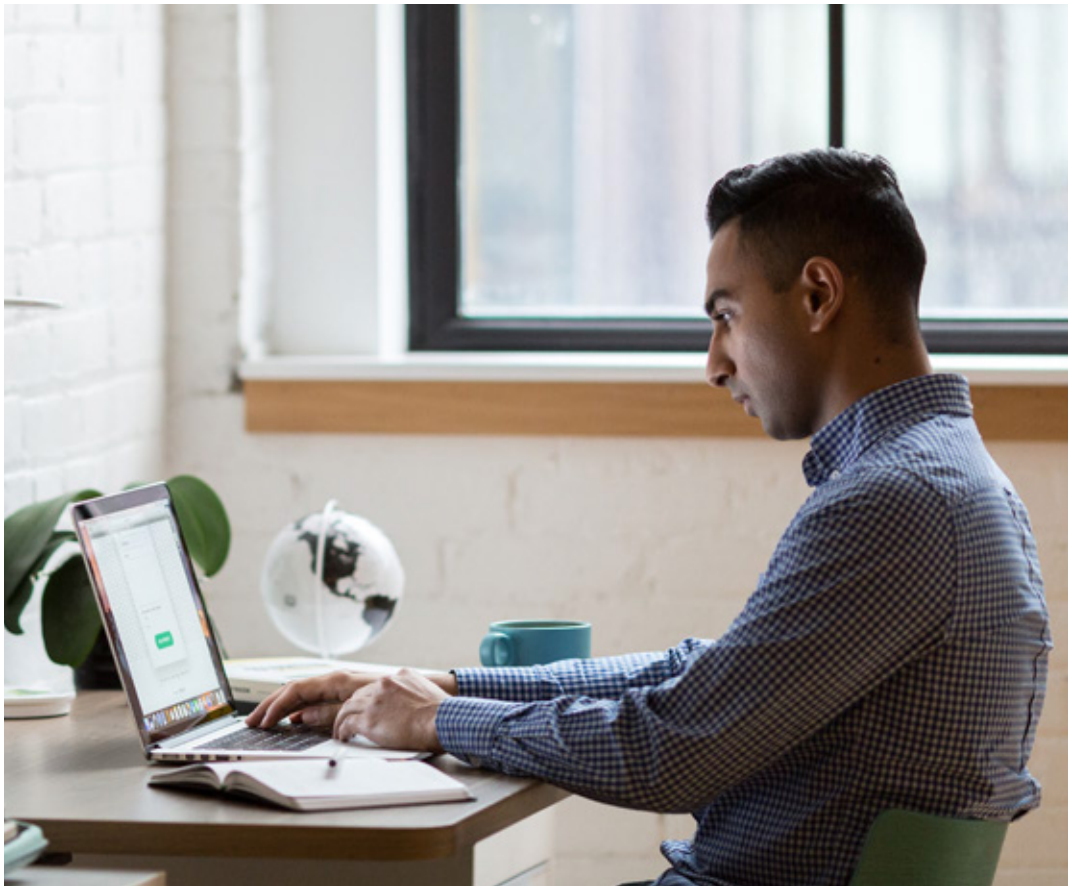
Important organizational benefits — beyond security — come along with good cyber hygiene. First of all, it creates automation and labor savings that can drive efficiency and free up precious internal resources.

**The labor needed to manage Automox's solution, for example, is on average one-fifth the labor needed to manage existing security models.**

Your organization will likely see drastic staff and operational efficiencies, depending on how you're currently organized.

Then there are the outright cost savings, which can be surprising. We don't need to tell you what you can do with thousands of extra dollars every month.

# Introducing the Center for Internet Security Cyber Hygiene Controls



**In any context of technological change, one challenge is identifying a dependable set of standards to judge your progress and tools.**

Until recently, the principles of cyber hygiene were new enough that companies were essentially on their own. But they aren't now. The CIS is the authoritative body responsible for the most complete and useful guidelines for cyber hygiene. Their Cyber Hygiene Controls, which have seen several iterations, begin with six fundamental principles that focus heavily on endpoint hardening. These principles are practical and actionable, and they're relevant to almost any organization's IT ecosystem.

## 1 INVENTORY AND CONTROL OF HARDWARE ASSETS

**Our take:**

A company's endpoints, servers, and other hardware assets are where attackers establish initial footholds. This makes it crucial for companies to track and update their assets and control network access as needed.

Endpoints that are not permanently attached to the network (such as BYOD and remote workers) are especially vulnerable, since they're often out of sight and typically fall behind with scheduled patching and updating tasks.

## 2 INVENTORY AND CONTROL OF SOFTWARE ASSETS

**Our take:**

Companies need to know that only authorized and properly installed software is running on their machines (real and virtual). This is harder than it seems, and the rapid versioning of many applications and other tools makes it difficult to stay compliant, protected, and optimized.

Unwanted or outdated third-party software is, of course, a primary point of exposure to attackers who exploit the resulting vulnerabilities. Any cyber hygiene framework must inventory desired software installations, such as productivity tools and databases, as well as infiltrations of undesired types to capture a full ecosystem view.

## 3 CONTINUOUS VULNERABILITY MANAGEMENT

**Our take:**

It's no longer enough to rely solely on human interventions to keep pace with the scale and velocity of remediating patches, configurations, etc., required to effectively reduce an organization's exploitable attack surface. Adversaries are usually faster than their targets and will seize on publicized security vulnerabilities before most companies can remedy them.

In fact, the average time to weaponize a newly disclosed critical vulnerability is seven days, while the average organization takes 102 days to remediate. Organizations simply can't scale their efforts fast enough if they rely entirely on human memory and follow-through.

## 4 CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES

**Our take:**

Admin rights are the keys to the kingdom, and they are a primary method for attackers to spread laterally inside a target. The more an organization can enforce a least privilege strategy (providing only those privileges needed for users to do their jobs), the less likely they are to fall victim to malicious software or social engineering tactics.

If administrative privileges and use practices are loosely controlled, a company's most critical data, applications, and security functions are exposed because attackers have a ready-made (and often publicly identifiable) group of targets. Companies should audit their use of admin rights and reset those rights at regular intervals.

## 5 SECURE CONFIGURATION FOR HARDWARE AND SOFTWARE ON MOBILE DEVICES, LAPTOPS, WORKSTATIONS, AND SERVERS

**Our take:**

Patches, updates, and configurations are only useful to the extent that they are evenly applied across devices, software, and the rest of a company's infrastructure. Furthermore, the default settings for business hardware and software usually prioritize ease of use — not security.

Consequently, there is work involved on a company's part to ensure proper settings and configuration. It usually isn't enough to expect individual users to manage this on their own, and configuration drift remains a critical — often unseen — vulnerability for many teams.

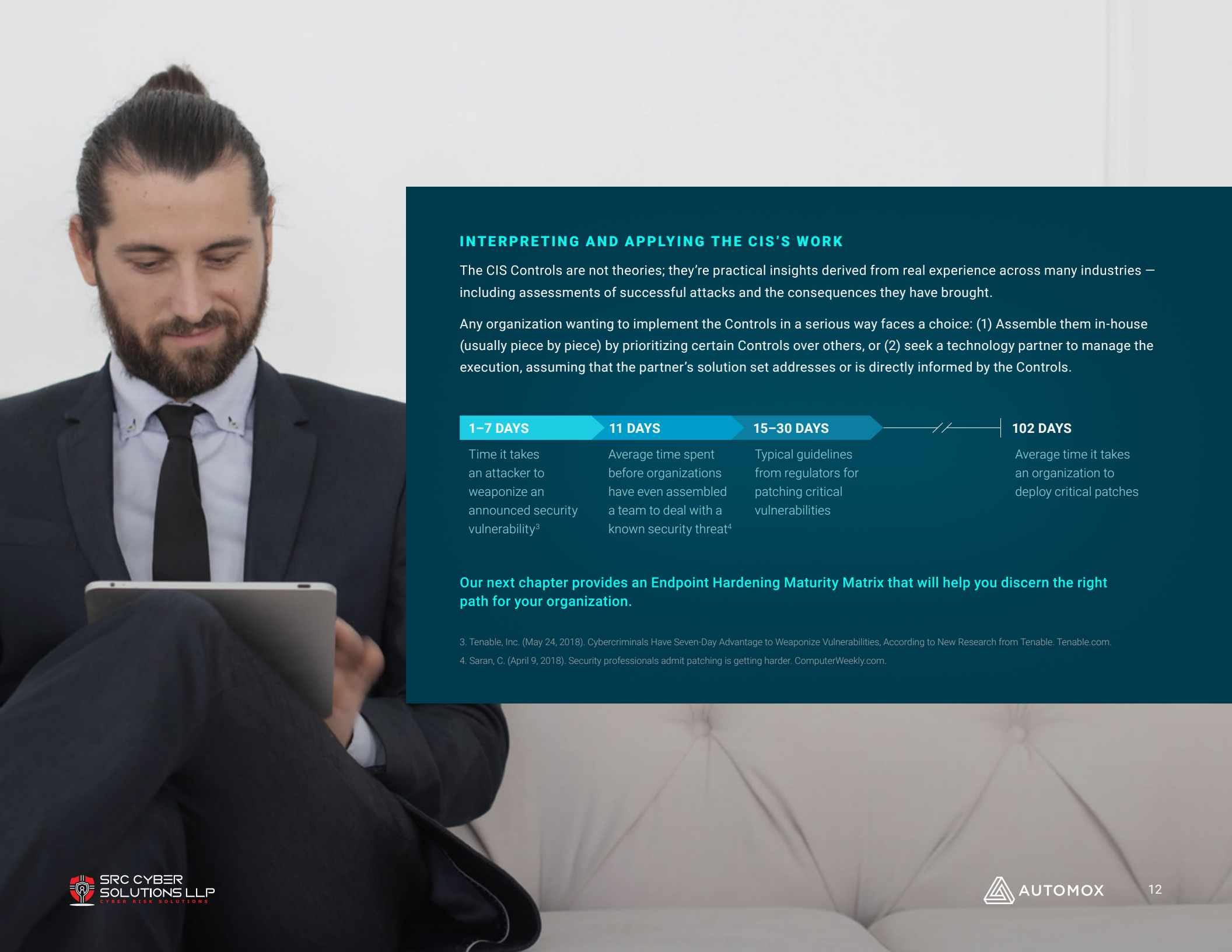
## 6 MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS[2]

**Our take:**

Logging and analysis are the means through which companies can discover threats or breaches. If you're not seeing what's going on, you're certainly not fixing it.

Many auditing practices exist mostly for obligatory compliance reasons and are infrequently analyzed for security insights or warnings. This is usually a human labor issue. Given the work involved and the traditional lack of automation opportunities, most companies cut these processes short.

[2] *Center for Internet Security. (April 1, 2019). CIS Controls V7.1. http://www.cisecurity.org/controls/. License at https//creativecommons.org/licenses/by-nc-nd/4.0/legalcode.*



## INTERPRETING AND APPLYING THE CIS'S WORK

The CIS Controls are not theories; they're practical insights derived from real experience across many industries — including assessments of successful attacks and the consequences they have brought.

Any organization wanting to implement the Controls in a serious way faces a choice: (1) Assemble them in-house (usually piece by piece) by prioritizing certain Controls over others, or (2) seek a technology partner to manage the execution, assuming that the partner's solution set addresses or is directly informed by the Controls.

**1–7 DAYS**

Time it takes an attacker to weaponize an announced security vulnerability[3]

**11 DAYS**

Average time spent before organizations have even assembled a team to deal with a known security threat[4]

**15–30 DAYS**

Typical guidelines from regulators for patching critical vulnerabilities

**102 DAYS**

Average time it takes an organization to deploy critical patches

**Our next chapter provides an Endpoint Hardening Maturity Matrix that will help you discern the right path for your organization.**

3. Tenable, Inc. (May 24, 2018). Cybercriminals Have Seven-Day Advantage to Weaponize Vulnerabilities, According to New Research from Tenable. Tenable.com.

4. Saran, C. (April 9, 2018). Security professionals admit patching is getting harder. ComputerWeekly.com.

# Where do you stand?

# An Endpoint Hardening Maturity Matrix

**Automox has built the following Endpoint Hardening Maturity Matrix to help companies assess their cyber hygiene practices as they relate to proactive endpoint hardening.**

It's rooted in our experience across industries and with organizations of drastically different levels of maturity.

Regardless of whether you choose Automox's solution, a positive trajectory along these maturity stages will protect your core business functions.

**Achieving mature cyber hygiene is not a "nice to have" — it's a matter of preserving what's most important to your organization.**

# Endpoint Hardening Maturity Matrix

| | 1 Undeveloped | 2 Starting out | 3 Maturing | 4 Optimizing | 5 Operational excellence |
|---|---|---|---|---|---|
| **Management** | • Lack formal cyber hygiene practice<br>• Unclear ownership<br>• Extensive human labor | • Some formal cyber hygiene practices<br>• Scaling is slow/ labor-intensive | • Some convergence on tooling and best practices<br>• Scaling still difficult | • Clear ownership<br>• Cyber hygiene understood and given priority as a security pillar | • Clear protocols and priority<br>• Patching/management with velocity and agility |
| **Tools** | • Ad hoc patching/config<br>• Manual implementations<br>• Spreadsheet-based organization<br>• Little or no holistic visibility | • Some fragmented tools in place (or in progress)<br>• Lack coordination among tools<br>• Lack single-pane visibility | • Still lack single-pane visibility<br>• In-house architectures and old on-premises systems<br>• Some automation<br>• Little or delayed visibility into remote assets | • Moving beyond on-premises architectures and legacy practices<br>• Viable automation and cloud-native cyber hygiene<br>• Visibility of on- and off-premises assets | • Cloud-native tools<br>• Free of obsolete architectures<br>• Extensive automation<br>• Single-pane visibility of all endpoint operating systems (OSs) |
| **Time to REMEDIATE** | 100+ days | 60+ days | 30+ days | < 15 days | < 7 days |
| **Posture** | Reactive | Reactive | Reactive | Proactive | Proactive |

# Next steps

# Where Do You Go From Here?

**It's possible that you've flipped to this page with a sense of assurance… or worry. Either way, your mission is simple: Wherever you are on the Endpoint Hardening Maturity Matrix, move up.**

### IF YOU OCCUPY STAGES 1–2

At this point, the most important changes you need to confront might be organizational, not technological. In our experience, companies' initial barriers to cyber hygiene maturity are cultural — they're locked in old ways of thinking and managing risk.

Put it another way: Many businesses, especially ones that have invested in on-premises IT architectures, resist "throwing it all out" by moving to cloud-native cyber hygiene. However, the modern business isn't run on-premises. Expecting so creates barriers to productivity and substantial risk exposure.

Some leaders hesitate because they don't want to experience hiccups or disruption during a transition — or they fear that automated patching is going to break something along the way. These concerns are usually for naught. Ask yourself: Is it better to iron issues out in a test environment under the guidance of your technology partner, or witness the failure of your current setup without a partner?

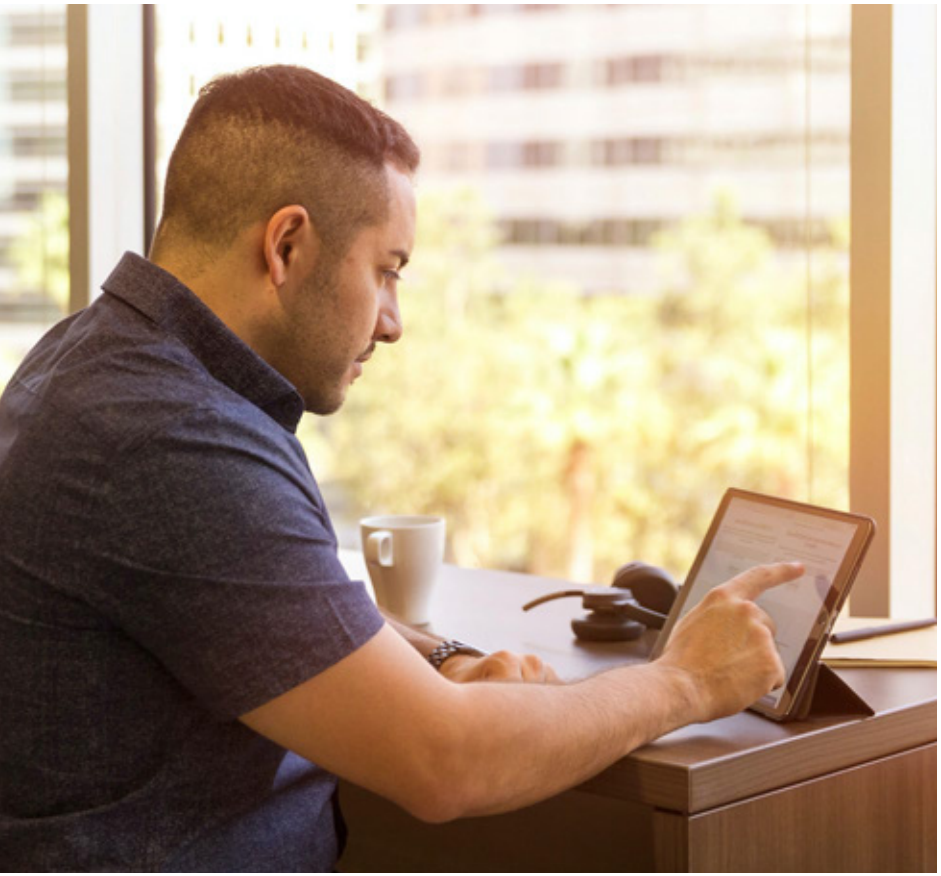
### IF YOU OCCUPY STAGES 3–4

You have some momentum, but your patch and configuration response times are likely inadequate. Somewhere in your IT environment, there are probably still legacy systems and practices that no longer serve you. Consider letting go.

Focus on automating out any obsolete practices, and question any cyber hygiene practices that require substantial human labor. Prepare your leadership and organization for sustained prioritization of cyber hygiene by assessing the efficiencies it has created and the improved response it already allows.

### IF YOU OCCUPY STAGE 5

Go take a vacation. Then get back to work, because cyber hygiene is never static. It takes constant development, optimization, and learning.

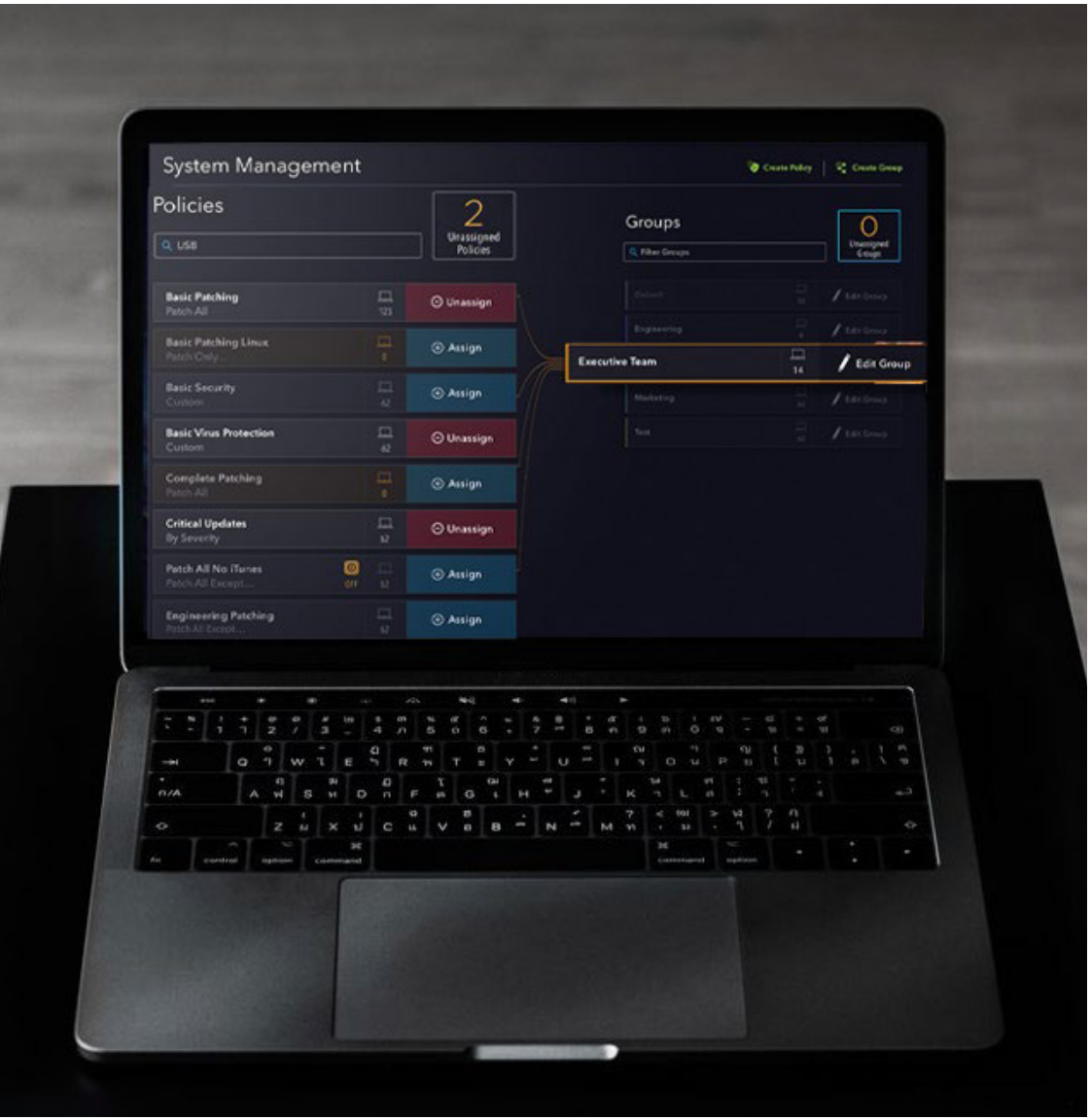


## HOW CYBER HYGIENE AFFECTS ORGANIZATIONS

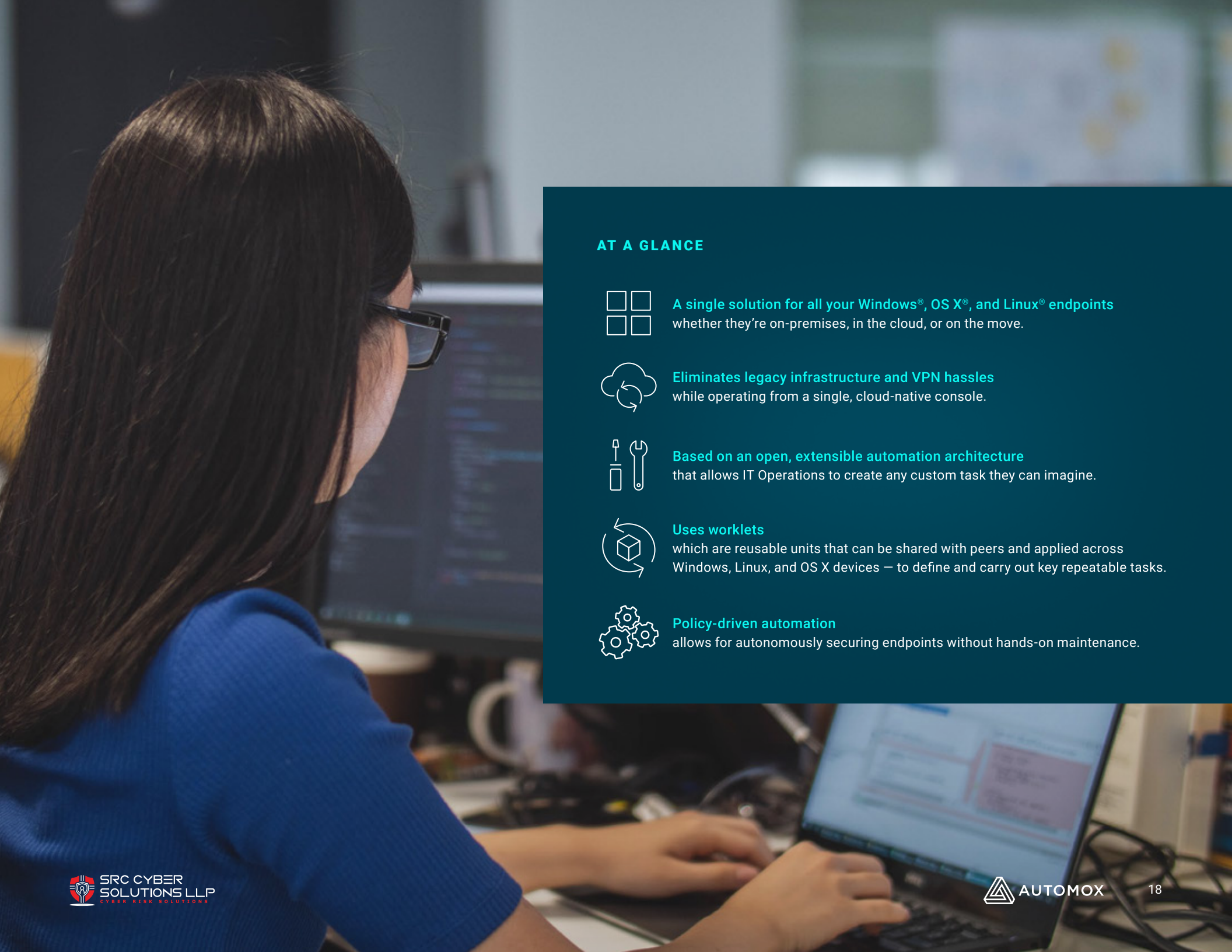
One of the most productive things about cyber hygiene is that it forces important conversations at both the leadership and operational levels. For example:

- Has the organization proclaimed its enthusiasm for digital transformation but failed to enact it?
- Is the organization coasting on a “It’s never happened to us” security mindset?
- Do your leaders really understand cloud-native tools and their inevitability?
- Is your security operation secretly loaded with labor-intensive, expensive practices?

Alongside the business benefits mentioned in Chapter 1, these organizational conversations can expose all sorts of antiquated practices, opportunities to cut costs, and new chances to embrace the cloud and automation.




# Achieving the 24/72 Endpoint Hardening Threshold With Automox



## AT A GLANCE

**A single solution for all your Windows®, OS X®, and Linux® endpoints**
whether they're on-premises, in the cloud, or on the move.

**Eliminates legacy infrastructure and VPN hassles**
while operating from a single, cloud-native console.

**Based on an open, extensible automation architecture**
that allows IT Operations to create any custom task they can imagine.

**Uses worklets**
which are reusable units that can be shared with peers and applied across Windows, Linux, and OS X devices — to define and carry out key repeatable tasks.

**Policy-driven automation**
allows for autonomously securing endpoints without hands-on maintenance.

## Automox-specific business outcomes

80% **Percentage potentially reduced of vulnerable exposure** with minimal effort or impact on employees.

50% to 90% **lower total cost of ownership** over traditional on-premises patch management solutions.

**Gives businesses built-in cyber hygiene fundamentals,** including OS, software, and third-party patching, system inventory, software deployment, and secure configurations.

**Provides a single platform of record** drastically reducing complexity, staff time, and management fatigue.

**Compliance reporting and other minutia are managed entirely by Automox,** freeing IT departments and management to focus on more strategic jobs.

## OUR APPROACH TO SECURITY

### You have enough IT horror stories in your life.

Automox operates on the philosophy that it's better to calmly and steadily solve people's security problems than it is to scare them into a frenzy. We devote ourselves to cyber hygiene because we know it's one of the most practical and influential practices any company can adopt.

## About SRC Cyber Solutions LLP

**At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.**

**Contact SRC Cyber Solutions LLP**

// www.srccybersolutions.com
// +91 120 232 0960 / 1
// sales@srccybersolutions.com


SRC CYBER
SOLUTIONS LLP
CYBER RISK SOLUTIONS