



Manage, Automate and Prioritize (M.A.P) Your Cybersecurity Journey

Six steps for a comprehensive approach to
cybersecurity for the Everywhere Workplace

Table of Contents

Why read this eBook?	2
Introduction	3
It's time to M.A.P. your cybersecurity journey	4
Step 1: Get complete asset visibility	5
Step 2: Modernize device management	6
Step 3: Establish device hygiene	7
Step 4: Secure your users	9
Step 5: Provide secure access	10
Step 6: Manage your compliance and risk	11
M.A.P your cybersecurity journey	12
About Ivanti	13

Why read this eBook?

Attacks stemming from software vulnerabilities, malware, credential theft and a host of other threat vectors have grown exponentially in both frequency and sophistication. Further exacerbating the problem: the rise of the Everywhere Workplace, with the rapid shift to remote work, as well as the substantial limitations in both budgets and the number of available skilled security personnel. Keeping up with every vulnerability, while previously difficult, has now become virtually impossible.

For businesses, and ultimately IT, the circumstances demand a comprehensive security strategy that enhances security posture, ensures continuous cyber risk management and reduces disruption. That means moving beyond solutions designed for a world dominated by PCs and datacenters and toward solutions built for the Everywhere Workplace, where mobile-cloud technologies are paramount.

This guide serves as a starting point and framework of steps to help you advance that cybersecurity journey. By following the recommendations in this guide, you can move toward protecting users, devices, networks, applications and data against increasing threats in the Everywhere Workplace.

Introduction

The cybersecurity landscape today

The threat isn't looming. It's here.

How did we get to this point?

The rapid rise of the Everywhere Workplace led to an extraordinary increase in vulnerable exposure points. While the abrupt shift to a remote, digital business landscape was initially assumed to be temporary, the Everywhere Workplace is now here to stay. According to Gartner¹, 82% of organizations intend to permit remote working some of the time, and 47% intend to allow employees to work remotely full-time going forward. Clearly, the PC and database-centered security solutions that were relied upon prior to the pandemic are no longer adequate in the face of distributed workforces and the widespread use of personal mobile devices and cloud applications.

For a good example, look no further than QR codes. They've sprung up everywhere, from restaurants to doctors' offices, and are often scanned with the same mobile devices employees use for their work. But the ubiquity and ease of use of QR codes has also made them an ideal vehicle for phishing attacks. With only email phishing solutions in place, the user – and the enterprise – are vulnerable to attacks.

Making matters worse, threats of all types have grown in sophistication – often specifically targeting remote work-generated vulnerabilities – and are taking place at an alarming rate. Phishing attempts, for example, are up 85% year-over-year (with 74% of organizations falling victim), and 59% of organizations have reported being victimized by ransomware in 2021. Factor in a global shortage of security experts, combined with tight budgets everywhere, and now the simple act of organizing and prioritizing vulnerabilities consumes the lion's share of security and IT time – as much as 53%².

This is a perfect storm: a changing workplace, too much to secure, and not enough resources to act. Staying the course is not an option. Businesses that fail to act are likely to experience more data breaches, including ransomware, phishing, hacks, and vulnerabilities caused by internal employees (intentional or unintentional), and potentially run afoul of ever-changing compliance mandates. The brand impact is astronomical, with unanticipated downtime, compliance issues, loss of reputation and customers, and an estimated cost of \$4.24 million per data breach³. Ransomware attacks cause an interruption lasting an average of 22 days⁴. And compliance violations have cost companies more than \$1.3 billion...and counting.⁵

“This is a perfect storm: a changing workplace, too much to secure, and not enough resources to act.”

It's time to M.A.P your cybersecurity journey

M.A.P, an acronym standing for Manage, Automate, and Prioritize, is a three-phased journey to building a comprehensive, scalable and framework-aligned cybersecurity strategy for the Everywhere Workplace.

Manage, the first phase, is about establishing your cybersecurity foundation. In it, your goal is to move from an unknown state to a known one. That means gaining visibility into who your users are, and the devices and applications they're using, to better understand where your vulnerabilities lie. It also means doing away with practices that could put your organization at risk, such as having unmanaged devices accessing business resources (especially those in the cloud) or not keeping up to date with the latest patches.

Automate, the second stage, is about alleviating burdens. Once you've arrived at a known state, the next step is to free up resources by automating repetitive, manual processes like maintaining inventory, onboarding devices and deploying workspaces and applications. You can also add self-healing and self-service solutions to further reduce the need for IT intervention.

Finally, **Prioritize** is about getting to a state where IT has the information and ability to identify and address the top areas of risk. Despite automation, there will still be areas that require IT intervention.

Rather than taking a non-strategic, guesstimate approach to addressing risk, Prioritization empowers IT with the right data and risk scores to take an intelligent, strategic approach to risk response and remediation.

M.A.P looks different for every organization, but in every instance should span the key pillars of users, devices, network, applications and data, and include consistent factors, such as:

- Discovery.
- Management.
- Enforcement and verification of secure configuration.
- Updated, risk-based patching systems.
- Reduction of employee-introduced risk through methods including verified credentials.
- Adaptive control and lifecycle management.

While this approach can't prevent every attack, it minimizes attack surface and enables proactive intelligent risk management, allowing you to be as prepared as possible. And when threats do crop up, continuous cyber risk management designed to accelerate into action reduces security exposure and limits business disruption.

Potential benefits also include better visibility, fewer non-managed and non-compliant devices accessing business systems, less time spent patching, a lower risk of audit failures, and financial savings. With the right tools, all of this is possible with less manual intervention – not more.

The dilemma that keeps businesses stuck – and six steps to get unstuck

While the above sounds great, we understand it can also feel daunting. At first, it reads like a dilemma with no clear answer. We need to enhance security, reduce threats, improve productivity and conserve resources, but because we're spread so thin and face an expanding threat landscape and attack surface, we don't have the bandwidth to implement new programs right now.

That's why we've mapped out six steps to help guide organizations on their journey. Each covers a component critical to effective cybersecurity today, and, taken together, forms the basis of a comprehensive and scalable cybersecurity management strategy.

Step 1

Get complete asset visibility

You can't manage what you don't know about. Lack of accurate and consolidated cloud and asset inventory (hardware and software) leaves your organization vulnerable to security risks, compliance shortcomings, overly complex tracking and confusing data.

With IT resources strained globally, now is the time to invest in an automated platform that makes the highest and best use of your team's capabilities. A comprehensive discovery initiative finds all assets on your network, both corporate-owned and BYOD, and maps them along with context so you know who is using what device, how and when they're using that device as it interacts with your organization, and what they have access to.

The benefits of discovery include:

- Gather complete and real-time visibility from all connected devices and software and their context.
- Enable efficient management, protection and service of assets everywhere.
- Streamline and organize all data from each source.
- Track and reclaim software licenses.
- Optimize the overall spend of IT assets (hardware, software, cloud).

What to look for in your discovery solution:

- The ability to discover, manage and secure devices that are on and off the network. This includes devices connecting to cloud services.
- Automatically discover and M.A.P the linkages between key hardware and software assets with the services and applications that depend on those assets.
- A consolidated asset database that can pull information from a variety of systems such as unified endpoint management (UEM), network gateways, Cloud Services, and ITSM.
- Reconciliation between what is procured by IT and what is actively connecting to business services.
- Connectors to data sources (vendor, contract databases, hardware warranty, etc.)
- Integration with ITSM and security processes for proactive remediation of IT issues and security vulnerabilities.



Step 2

Modernize device management with unified endpoint management

As more organizations continue moving to hybrid work environments, endpoint security and management have never been more critical to both IT staff and employees. Modern device management is necessary for increasing user and IT productivity, empowering IT administrators to automate provisioning of devices and software deployments, and fixing user issues quickly.

To cut down on support time and ensure that all devices are managed to the same standards, choose a UEM solution with management capabilities for a wide range of operating systems including iOS, Android, Windows, macOS, Linux, ChromeOS, special-purpose frontline worker devices, wearables and IoT devices, with support for both modern management and client-based management.

A unified endpoint management solution should be available both on-premises and as a SaaS offering to meet the deployment requirements of your business. UEM helps protect employee privacy through the separation of business and personal data on endpoints. UEM also fully supports BYOD initiatives while maximizing user privacy and securing corporate data at the same time.

Benefits of managing devices using a unified endpoint management approach include:

- Consistent management and security across all your devices.
- Easy onboarding, provisioning of applications and configuration of device settings at scale, improving both IT productivity and the user experience.
- Monitor device posture and ensure compliance at all times.
- Remediate issues quickly and remotely.
- Automate software updates and OS deployments.
- Provide comprehensive dashboards and real-time intelligence to improve IT decision-making.
- Detect and remediate OS and third-party app vulnerabilities.
- Reduce end user interruption and provide a seamless onboarding experience.

Features to watch for in your device management solution:

- Simple onboarding and provisioning process for IT by leveraging services such as Apple Business Manager (ABM), Google Zero-Touch Enrollment and Windows AutoPilot to provide users with automated device enrollment.
- The ability to discover, manage and secure any endpoints running iOS, Android, macOS, Windows, Linux and ChromeOS devices as well as other immersive and rugged devices such as HoloLens, Oculus and Zebra.
- Support for multiple device ownership models so you can manage, configure, and secure corporate-owned, BYOD and shared devices.
- The ability to empower frontline workers and secure business apps on their devices without requiring device management.
- Enablement of secure access to data and apps on any devices.
- In-depth visibility and control across all managed devices via custom reports and automated remediation actions.

Step 3

Establish device hygiene

Good device hygiene involves taking a proactive approach to ensuring only devices that meet defined security requirements are allowed to access business resources. This includes having systems in place that can either automatically patch devices or quarantine devices with software vulnerabilities, both in the operating system and/or applications. Establishing good device hygiene requires the use of reputable solutions to reduce digital attack surface.

On the other hand, poor device hygiene can leave your organization susceptible to cyberattacks such as ransomware. For organizations with poor device hygiene, the onus is on IT, rather than purpose-built solutions, to actively track vulnerabilities and protect the organization from cyberattacks.

Hygiene for mobile devices

While 71% of professionals feel that mobile devices are essential to their work, security leaders nearly unanimously agree that remote workers are exposed to more risk than in-office workers. And yet, three in four security professionals have succumbed to the pressure to sacrifice the security of mobile devices for the sake of expediency.⁶

That's a big problem. Solid mobile device hygiene is critical to combat device vulnerabilities (e.g., jailbreak, root detection, vulnerable OS versions, etc.), network vulnerabilities (e.g., man-in-the-middle attacks, malicious hotspots, unsecured Wi-Fi, etc.) and application vulnerabilities (high security risk assessment, high privacy risk assessment, suspicious app behavior, side-loaded app, etc).

Benefits of establishing mobile device hygiene include:

- Limit both human error and IT investment with automated, actionable risk-based intelligence.
- Zero-day detection and remediation so you don't have to guess what's coming.
- Detect and remediate issues even on devices that are turned off or not connected.
- Preserve your data, your resources and your brand by reducing attack surface.

Features to watch for in your mobile threat defense solution:

- Prioritize software that protects against all mobile attack types, including phishing attacks plus attacks at the device, network and application levels.
- Protection for both Android AND iOS devices is key. Seek a single application with an on-device machine learning engine bundled with a UEM client. Users are far more likely to adopt a single application rather than two—or more.
- Look for multilayered protection from a solution that defends against threats at the device, network and application levels – plus phishing threats – with both on-device and cloud-based threat detection capabilities. On-device protection does not require an internet connection to still detect and remediate threats.
- A tiered compliance policy that can be applied to alert the end user and admin that their device is out-of-compliance is essential. Non-compliance is met with graduated actions, from blocking access to corporate resource to quarantining, to retiring the device and removing all UEM-provisioned apps, content, settings, etc.

Hygiene for desktop/laptop devices

Until ransomware attacks and other data breaches are a thing of the past – a day that may never come based on their current trajectory – organizations must take steps to protect against them. Patching to fix Common Vulnerabilities and Exposures (CVEs) is one of the best things an organization can do to counter ransomware attacks. Unfortunately, research from Ivanti⁷ shows 71% of IT and security professionals find patching to be overly complex and time-consuming. That may be due to the overwhelming volume of vulnerabilities that exist.

There are well over 100,000 vulnerabilities listed in the U.S. National Vulnerability Database (NVD). While only a small percentage of those vulnerabilities are tied to ransomware, and an even smaller percentage are trending/active exploits, identifying which ones pose the most risk to an organization can be tricky. A report from Ivanti shows⁸ that from 2018-2020, using CVSS v3 scoring, if an organization were to patch only critical vulnerabilities, its coverage against ransomware would only be about 35%. Automated, risk-informed patching is essential to desktop/laptop device hygiene.

Benefits of establishing desktop/laptop device hygiene include:

- As with mobile device hygiene, limit both human error and IT investment with automated, actionable risk-based intelligence.
- Reduce the likelihood of ransomware attacks by patching to fix CVEs based on real-world risk.
- Leverage automated prioritization of threats so that you are can patch strategically and optimize resource allocation.
- Go beyond patching to automate responses so a threat is countered without the contingency of human intervention.

Features to watch for in your desktop/laptop device hygiene solution:

- For desktop/laptop devices, it's essential to update software regularly to eradicate – or at least limit – vulnerabilities. Since patching can become overwhelming, it's helpful to find a solution that can automatically assess risk and deliver actionable intelligence, with prioritization given to the most pressing vulnerabilities.
- Risk-based prioritization brings visibility to the riskiest weaknesses in an environment. This enables organizations to target the most critical patch needs. Active threat context, which means mapping vulnerabilities to real-world threat-based information, is critical as it helps IT/security teams prioritize patching to combat threats that are likely to do the most damage.



Step 4

Secure your users

The only people who seem to like passwords are the threat actors who weaponize them. In addition to being burdensome for users, password-based authentication lacks device, app, network and threat context. There is no way of knowing if the person entering the password is an employee or an attacker who has obtained an employee's password. Even the most complex passwords can be compromised with relative ease via brute force, phishing and other types of attacks.

Credentials, like passwords, remain among the most sought-after data types in breaches – involved in 61% of breaches⁹. Credentials are compromised faster than any other kind of data, and this is particularly true in phishing, which typically goes after credentials for use in gaining further access to their chosen victim organization.

SSO solutions create a single point of failure that can be exploited by hackers to gain access to most or all enterprise apps. According to research¹⁰, forty-two percent reuse passwords across accounts, and 17 percent recycle two to five passwords for everything. That means that if someone has an account compromised outside of a work context but they're using the same passwords at work, your organization is at risk.

With the rise of remote work, it might be assumed that organizations tightened up password protocols, but in research by Verizon¹¹, more than one-third of respondents said their company relaxed authentication requirements to cope with COVID-19 restrictions.

It's time for passwordless authentication via zero sign-on.

Zero sign-on is an authentication method that uses zero passwords (like how single sign-on uses a single password).

Benefits of securing your users via passwordless authentication include:

- No passwords = no credentials to be stolen or phished.
- No passwords = happier users who do not have to remember passwords or get locked out of accounts.
- Raises the maturity of your zero trust security.
- Conserve funds previously spent on managing password resets and handling breaches.

“There is no way of knowing if the person entering the password is an employee or an attacker who has obtained an employee's password”.

Features to watch for in your authentication solution:

- The ideal solution will deliver passwordless access to devices, business apps and cloud services.
- Effective passwordless access relies on multifactor authentication including possession (what you have, like a mobile device), inherence (biometrics like fingerprint, Face ID, etc.), and context (location, time of day, etc.) instead of knowledge factors (like passwords or security questions) to establish authentication.
- For a zero trust security approach with contextual access, leverage a solution that can integrate with a unified endpoint management solution that can verify user, device, application, network and threats before granting access.
- Look for passwordless authentication solutions that integrate seamlessly with existing identity solutions like IdP/IAMs, MTD/XDR/EDR, SOAR, SIEMs, and more.

Step 5

Provide secure access

The network perimeters that worked when your team was in-office no longer suffice in the Everywhere Workplace. With employees working from various (and often unpredictable) locations, a contemporary network perimeter must reflect this dynamic, removing limitations and complexities while ensuring security.

Today's networks should be built on the principles of the software-defined perimeter (SDP). An SPD provides an integrated security architecture that is otherwise difficult to achieve via existing security products such as anti-malware. It's designed to leverage proven, standards-based components such as data encryption, remote attestation, mutual transport layer security and Security Assertion Markup Language. Incorporating these and other standards-based technologies helps ensure that SDP can be integrated with your existing security systems.

While SPD is a network structure, it still requires a layer of security to maximize benefits. That is where zero trust – and specifically zero trust network access (ZTNA) – comes into play. Gartner defines ZTNA as a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications. SDP can be used to implement zero trust networks.

Benefits of establishing secure access everywhere include:

- Verifying that only trusted, authenticated users have access to resources.
- Allowing the network to blur the outside perimeter, permitting more flexible deployments and easier workflows for the end user.
- Avoiding the limitations and complexities of hard perimeters, including their propensity for opening up extra, unnecessary access into subsections of the network.
- Preserve security and visibility while facilitating access.

Features to watch for in your zero trust network:

- Data sovereignty: Application data does not transverse through vendor network nor is exposed to the internet. This direct path maximizes performance and user experience.
- Holistic visibility: Activity per-user, per-device and per-application, including SaaS deployed resources.
- Continuous and adaptive evaluation of client security posture, with automated policy enforcement based on various changing contextual elements such as behavior and location.



Step 6

Manage your compliance and risk

To stay in compliance and to mitigate threats, it's imperative to get a handle on governance, risk and compliance (GRC) management.

Too often, organizations manage compliance manually...in spreadsheets, believe it or not. They also commonly spend a huge volume of money on piecemeal security products without truly understanding how to integrate and leverage them. That translates to the proverbial "throw spaghetti at the wall to see if it sticks" approach.

It's essential to generate a big picture with regard to risk exposure. Most assessments of security posture are made after an attack and are specific to the attack vector. This reactive approach, combined with too many empty seats in IT roles, is a substantial issue.

“Too often, organizations manage compliance manually...in spreadsheets, believe it or not.”

Benefits of understanding compliance and risk include:

- Replace manual tasks with automated compliance processes.
- Set the stage for smoother audits.
- Proactively mitigate risk.
- Align budget with real risk, removing guesswork.
- Create a more strategic and reliable compliance framework.
- Meet ever-evolving requirement changes without developers.
- Free up human resources to focus on more strategic work.

Features to watch for in your compliance solution:

- A strong solution will ease the compliance burden with quick and easy regulatory documentation imports to M.A.P citations with security and compliance controls.
- Capacity for proactive risk management means dedicating attention to the right place at the right time.
- Seek to replace manual tasks with automated repetitive-governance activities, making your compliance run like a well-oiled machine.
- Process maturity management means you can assess the maturity of your critical security processes and controls, and optimize based on priority and risks.
- To ensure efficient and accurate results, look for a solution with automated guidance through the risk-assessment effort.

M.A.P your cybersecurity journey


Each of these steps are essential elements of managing, automating and prioritizing your cybersecurity journey. Overwhelmed? Not sure where to start? It's critical to take partners and leverage solutions to support your journey. The right solutions will be comprehensive and integrated to ease the burden on your IT staff. Optimal solutions will also preserve a productive, intuitive user experience that maintains integrity no matter where, when or how your employees work.

[Work Anywhere. Secure Everywhere.](#)



About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit [ivanti.com](https://www.ivanti.com)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

[ivanti.com](https://www.ivanti.com)

1 800 982 2130

sales@ivanti.com

1. Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time
2. Ivanti: Patch Management Challenges. <https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges>
3. Statista: Global average cost of a data breach 2021.
4. Statista: Average <https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/> length of downtime after a ransomware attack 2021.
5. The biggest data breach fines, penalties, and settlements so far | CSO Online
6. 2021 Data Breach Investigations Report | Verizon
7. <https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges>
8. https://www.ivanti.com/resources/v/doc/white-papers/spotlight_ransomware2021_risksensesecsw?_ga=2.114312003.538830105.1638796042-898995573.1638285247
9. 2021 Data Breach Investigations Report | Verizon
10. Best Password Managers 2021 | The Strategist (nymag.com)
11. People and behaviors | Verizon