ivanti

The Ultimate Guide to Unified Endpoint Management

How Modern Endpoint Management Solutions Impact Security and Employee Experience

Inside:

01 The new standard for post-pandemic endpoint management

02 What is unified endpoint management?

03 4 business benefits of a modern UEM solution

04 4 endpoint security use cases with UEM solutions

05 How to choose your UEM solution

06 References

ivanti

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein. For the most current product information, please visit ivanti.com

01

The new standard for post-pandemic endpoint management

Five years ago, endpoint management and security were comparatively straightforward.

For most organizations, endpoint devices that were used for corporate work lived in the office – an environment that could be controlled and a location where, hopefully, most of the devices could be easily found and managed by the on-site IT and Security staff.

Then, the Covid-19 pandemic upended traditional on-premises office life.

Exceptions to the pre-pandemic “walled garden” standard approach certainly existed – corporate laptops and mobile devices operated off managed Wi-Fi networks before 2020 kicked them all into a permanently remote posture!

However, the immediate stay-at-home orders issued to flatten the curve of the Covid-19 virus sent previously on-premises IT and Security teams around the world scrambling to cobble together the best working arrangements they could out of the technology and devices they had.

Exceptions to the rule were now the rule for everyone.

Now, with the decline of Covid-19 as a global menace, many employers are encouraging employees to return to the office and the previous technology status-quo. Ivanti research found that while only 13% of knowledge workers prefer to work solely in-the office, 56% of C-suite leaders believe that employees must be in the office to be productive. (Ivanti)

This gap between how employees want to work and where their managers feel their employees would be effective has put IT and Security in an extremely uncomfortable – and frankly unsustainable – position.

This tension is further enflamed when a complete return to the on-site management and walled garden networks of 2019 looks both unlikely and unwise:

> Two-thirds of all employees would rather quit than return to the office for a full work week, according to a 2022 survey by global job posting site Monster.com – and 40% of all respondents claimed they'd quit if forced to return regularly for just one out of five work days in a work week. (Shumway)

> In a November 2022 ultimatum, Twitter CEO Elon Musk demanded that employees either return to their local office for 40 hours a week or resign. (Yang) Hundreds of workers called his bluff and resigned. (Bond) By early January 2023, Twitter's full-time employee count had shrunk by over 80% from its initial headcount at about 7,500 employees to about 1,300 – with fewer than 550 full-time engineers. (Kolodny)

> When Amazon CEO Andy Jassy ordered his tech employees to return to the office full-time in February 2023, they pushed back. Eventually, he relented, stating that they must be in the office only three days a week. (Palmer)

For those believing that return to office work will improve productivity, research says otherwise:

- During the pandemic, Gallup recorded their highest-ever employee engagement levels at 40%; it has since dropped to less than one-third. (Smith)
- The first half of 2022 shows a record "slump" in productivity across the first half of 2022 – correlating with the increased pressure from organizations to require all employees to return to the office full-time. (Tsipursky)

These trends tell us that even if organizations see their employees comply with return to office mandates, they may simply be quietly quitting: doing the bare minimum while seeking out new opportunities that allow them the flexible working arrangements they found most appealing during the pandemic emergency. (Tsipursky)

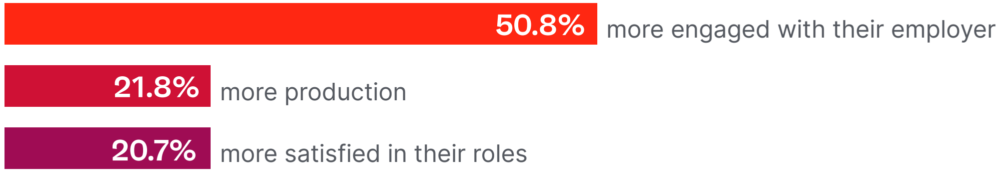
The obvious solution? Encouraging employees to continue working remotely, on-premises or a combination that best suits each individual user whenever possible.

In fact, employees who work in a hybrid or remote environment report being 21.8% more productive, 20.7% more satisfied, and 50.8% more engaged, as reported in a 2022 Integrated Benefits Institute survey. (Bonner)

Of course, this new requirement presents new difficulties for both IT and Security teams – which is where unified endpoint management solutions can assist.

After all, even if your organization thinks it's a solely on-premises working environment with absolutely zero remote working considerations – or wants to work towards that goal – your team knows that a 100% in-office working and security set-up will not be sufficient; they must account for those "exceptions" to the in-office rule, as we'll discuss in this guide.

Employees who work in a hybrid or remote work environment are:



Hybrid and remote "exceptions" to your in-office rule

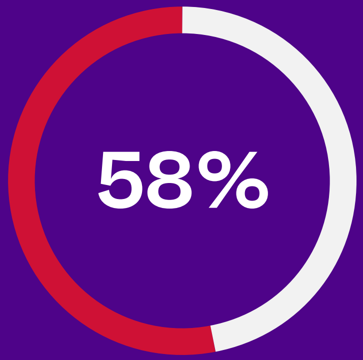
Your organization may consider itself fully "in-office" – and thus, only requiring the traditional endpoint management and security solutions that were popular pre-pandemic – but does work truly occur 100% on-premises?

Of course not!

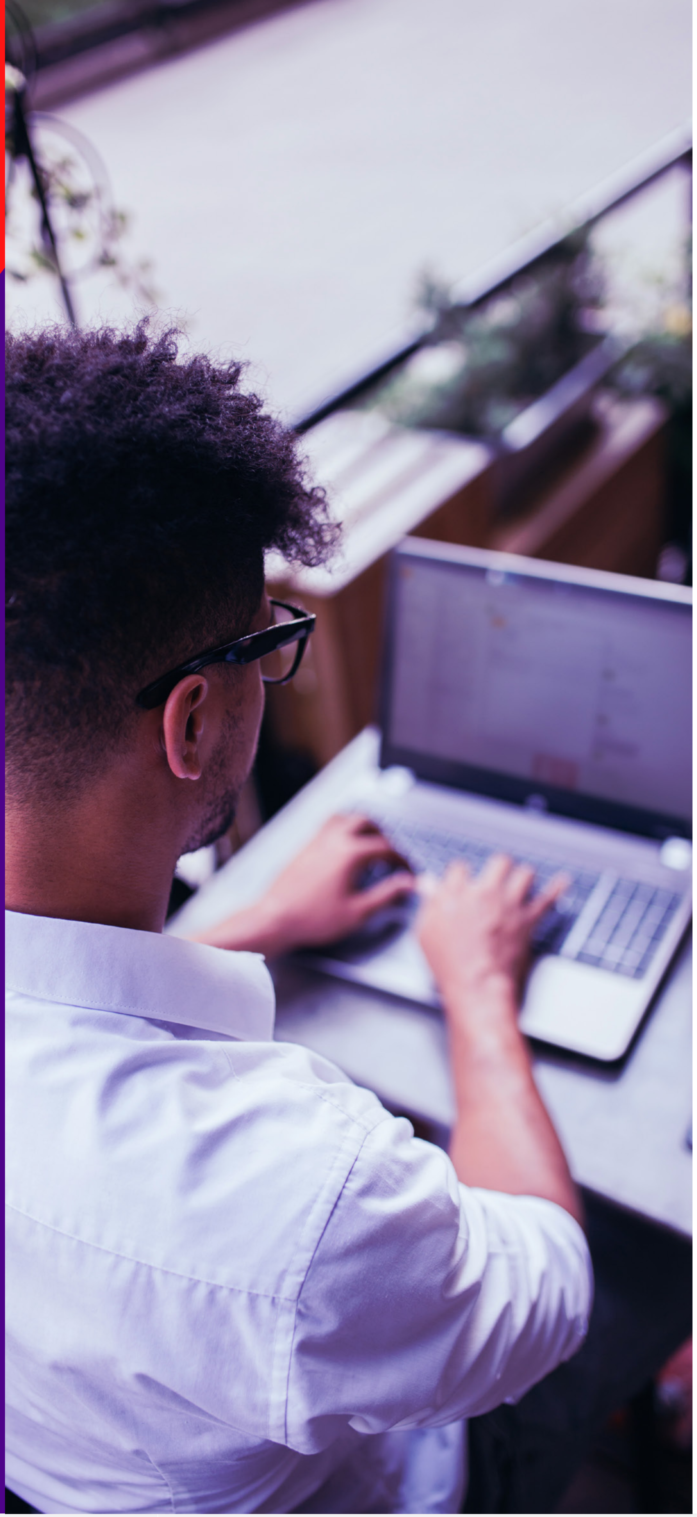
IT and Security teams must account for all edge-cases to the standard procedures, which makes a hybrid technology management and security strategy more robust than following management's assumptions that the only required working environments to secure and manage are in-office.

For example, hybrid IT management and security strategies would cover these "exceptions" to office-only working situations:

- **Healthcare providers** on call for the weekend who need to access patient files to respond to a call.
- **Teachers** grading papers at home or responding to parent emails after hours.
- **Financial advisers**, who should only be able to access their emails on a secure server... but may have installed an app that lets them access it on their personal devices.
- **Parents** trying to work from home while caring for a sick child.
- **Government employees** attending conferences or traveling for incident remediation, but still requiring home-office access to agency networks.
- **Executive leaders** seeking exemptions for convenience due to seniority.
- **Salespeople.**



of CISOs say that their companies have experienced more cyberattacks since allowing their employees to work remotely.



Even if a workplace has allegedly “returned to the office,” these end users and others like them will expect remote access to work data and applications from mobile devices via any network their Bluetooth can reach.

Thus, IT and Security teams must adapt strategies that allow employees to succeed in and out of the office, which means effectively wrangling devices and networks. It means securing all endpoints and their users, in any location, on any network – for all organizational data.

But this new requirement to manage and secure endpoints in a de facto hybrid workplace – regardless of official return-to-work status – doesn’t mean organizations are forced to rely on the same panicked pandemic strategies for device management they employed several years ago.

Those emergency-driven solutions worked for a time, but they are insufficient for long-term endpoint management and protection against modern risks and vulnerabilities – increasing organizations’ need for a truly unified endpoint management solution.

In fact, 58% of CISOs say that their companies have experienced more cyberattacks since moving to remote working. (Proofpoint)

What is unified endpoint management?

Unified endpoint management (UEM) is a technology that empowers IT and Security teams to find, manage and secure multiple endpoints – that is, devices, hardware and other technologies – from a single platform or dashboard, covering a wide range of operating systems (OS) and device types from many different manufacturers and developers.

At its core, UEM is the latest evolution of endpoint management solutions, which in turn were developed from the first mobile device management (MDM) technologies.

- **Mobile device management (MDM) –** today often renamed as "modern" device management – was the tech industry's first stab at tackling the management, enforcement and security dilemmas swirling around ever-growing fleets of devices. These solutions would allow IT to control, secure and enforce policies, configurations, and software on smartphones, tablets, and other endpoints that support MDM APIs, but were frequently limited to devices running specific operating systems.

- **Enterprise mobile management (EMM)** took MDM technology and merged it with software application management solutions such as mobile app management (MAM), mobile content management (MCM) and mobile information management (MIM) to manage the lifecycle of software on the device, data on specific apps and access to corporate data.

However, the blended endpoint management approach was still not robust enough to account for the traditional personal computers, servers and other mainstay corporate endpoints, as well as many of the growing edge-use cases within modern organization environments – including IoT devices and more “ruggedized” or specialized equipment found in specific-yet-common working situations.

IT teams at larger organizations found themselves sitting in a patchwork system to manage multiple OSs: macOS, Windows, iOS and Android, but also ChromeOS, Linux and other specialized or IoT-enabled devices.

While each OS vendor supports commands and configurations through their native MDM, there are several critical tasks that are not included in MDM APIs:

- Device status (jailbreak, root detection)
- Location
- Notifications
- Mobile threat defense

And so, unified endpoint management technology was born from organizations’ need to provide additional capabilities and application controls while expanding them across multiple OS and device types for both mobile *and* traditional endpoint management.

03

4 business benefits of a modern UEM solution

In this section, learn how UEM:

1. Consolidates tech stacks.

2. Automatically discovers unknown assets.

3. Increases user compliance.

4. Improves digital employee experience (DEX).

The UEM difference

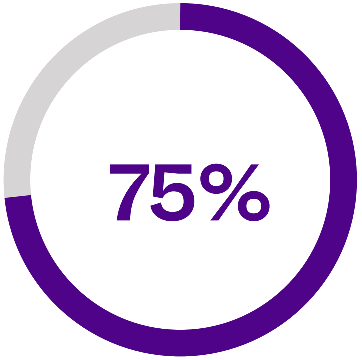
Now, most organizations already have at least one solution in place to manage the bulk of their owned and managed devices.

One 2022 survey of IT professionals found that 80% of respondents had already consolidated to a single endpoint management team or planned to do so within the next two years. And 75% of respondents have invested in some sort of BYOD (bring your own device) enablement technology. (Cipolla, Wilson and Silva)

Rather than existing in device-level silos, UEM solutions make better use of modern AI and machine learning (ML) capabilities, as these tools leverage the same base set of organization-wide information to draw conclusions, rather than relying on siloed information streams from separate tools.

Modern UEM solution advantages include:

1. **Single pane of glass" dashboards or portals,** which offer already stretched-thin IT and Security teams one consolidated solution instead of multiple niche products.
2. **Automatic identification and remediation of unknown devices** and so-called "shadow IT" through dynamic, automatic asset discovery – both on-premises and via the cloud.
3. **Increased end user compliance** with all IT and Security policies through unified device enrollment and enforcement.
4. **Improved digital employee experience (DEX)** with automatic and proactive remediation of device issues, to help IT teams shift left.



of IT professionals say their organization has invested in BYOD enablement.

1 A “single pane of glass” approach consolidates burdensome tech stacks.

With growing economic uncertainty, there’s a global call from investors and C-suites alike for their organizations to optimize strategic outputs with fewer resource investments – maximizing efficiencies and squeezing every ounce of value out of every tool, employee and timeline.

As part of this mandate, more and more organizations are pivoting to purchase more generalized and integrated technology solutions, rather than seeking out point solutions that require more manpower and specialized knowledge than their IT and Security teams can reliably support.

This strategic shift towards tech stack consolidation makes sense, especially when organizations consider global burnout and technology workforce trends:

- 64.4% of information services employee respondents reported burnout in a 2019 global survey – one of the highest rates of any industry. General “technology” sector employees also reported elevated burnout levels at a 60% response rate. (Paychex)
- 68% of surveyed incident responders say they’re typically assigned two or more incidents at once, with each incident requiring an average two to four weeks to resolve; 64% of those same responders have also requested medical help to treat burnout and anxiety. (Morning Consult and IBM)
- The top barrier to cybersecurity excellence for organizations around the world is “tech stack complexity” – followed by a “security skills gap” of the current security workforce – according to a 2022 global survey of security professionals. (Ivanti)

As one CISO told the *Wall Street Journal*:

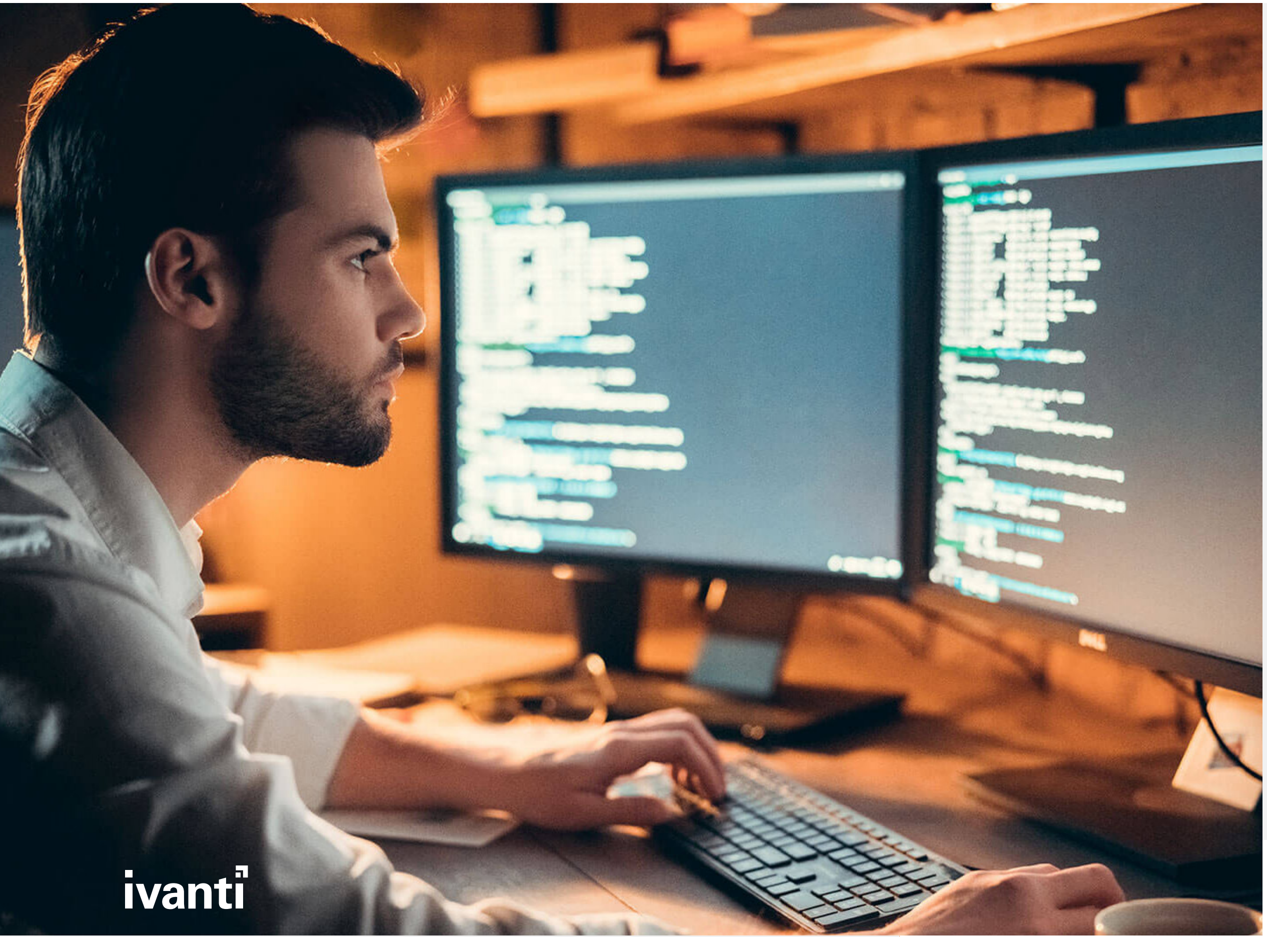
> “If I have to get one solution that does just five or six things pretty darn good but not excellent, then wonderful, I’m taking that solution all day. It’s easier to manage, it’s cheaper for a budget, and I’m getting more bang for my buck.”

Adam Glick
CISO at SimpliSafe, Inc. (Rundle)

Simply put? There are just too few people on-staff or in the job market with the skills required to manage each device, application and incident as they appear on disconnected solutions.

Properly configured and implemented, modern UEM platforms offer both IT and Security teams the closest possible "single pane of glass" view into their entire organization's endpoint environment, dynamically reporting on:

- Department- and user-level device use and management.
- Individual user access and activity, to evaluate overall productivity and potential security concerns.
- An endpoint's security status, including currently installed patches and use cases.
- A device's overall cost to the operation, accounting for historic maintenance and licensing costs.



Each of these points may be accounted for by point solutions for a given device type or OS, with even greater levels of granularity and detail for the most optimized of operations.

However, only a modern UEM solution can truly unify these related-yet-distinct needs into a single, easy-to-manage dashboard for overworked IT and Security teams to leverage within their personal workflows.

2 Automated asset discovery finds hidden costs with minimal manpower.

Just as using multiple technology solutions to manage endpoints increases overall expenses, insufficient asset discovery can result in increased overhead and costs for organizations – costs that the IT team will ultimately bear, regardless of where the leaks occur.

IT teams are increasingly aware of the danger of previous undiscovered (and thus unmanaged) hardware and software, more commonly known as shadow IT:

- 36% of IT professionals cite shadow IT concerns as a substantial challenge for modernizing their IT infrastructure. (Insight Enterprises & CIO)
- Shadow IT is one of the top concerns cited by surveyed CIOs for government continuity, following ransomware attacks and supply-chain attacks. (NASCIO)
- 41% of surveyed IT decision makers say that “decentralized” and shadow IT is one of the biggest trends that will impact global organizations in the near future. (Vanson Bourne for Nutanix)

Why have shadow IT considerations risen to the forefront of IT department minds? More hybrid workplaces and BYOD (bring your own device) policies bring with them more devices and applications that are used by end users, but not necessarily directly owned or managed by the IT team itself.

According to one survey of IT decision makers (Bitwarden), their end users say they use shadow IT because:

1. Their daily jobs are faster or easier with the shadow IT options of their choice, rather than organization-provided resources (63%).
2. They don’t have the correct internal authorizations to use devices or apps they think they need for their roles (48%).
3. IT is too slow in answering their requests for app or device access, or otherwise too complicated to bother with (38%).

Real-World Repercussions

Tech & License Consolidation Savings with UEM

According to a commissioned Total Economic Impact™ study conducted by Forrester Consulting on behalf of Ivanti, a composite enterprise-sized organization managing 10,000 endpoints that grows 5% annually achieved an ROI of 261% over three years by implementing Ivanti Neurons for UEM.

36% of the TEI study’s estimated benefits for the composite organization came from retiring individual endpoint management solutions and trimming software license expenditures from unused apps. (Forrester Consulting TEI study)

For more information, please read the Total Economic Impact™ of Ivanti Unified Endpoint Management (UEM) Solutions.

FORRESTER

The Total Economic Impact™ Of Ivanti Unified Endpoint Management (UEM) Solutions

Cost Savings And Business Benefits Enabled By UEM Solutions

JULY 2022

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY IVANTI

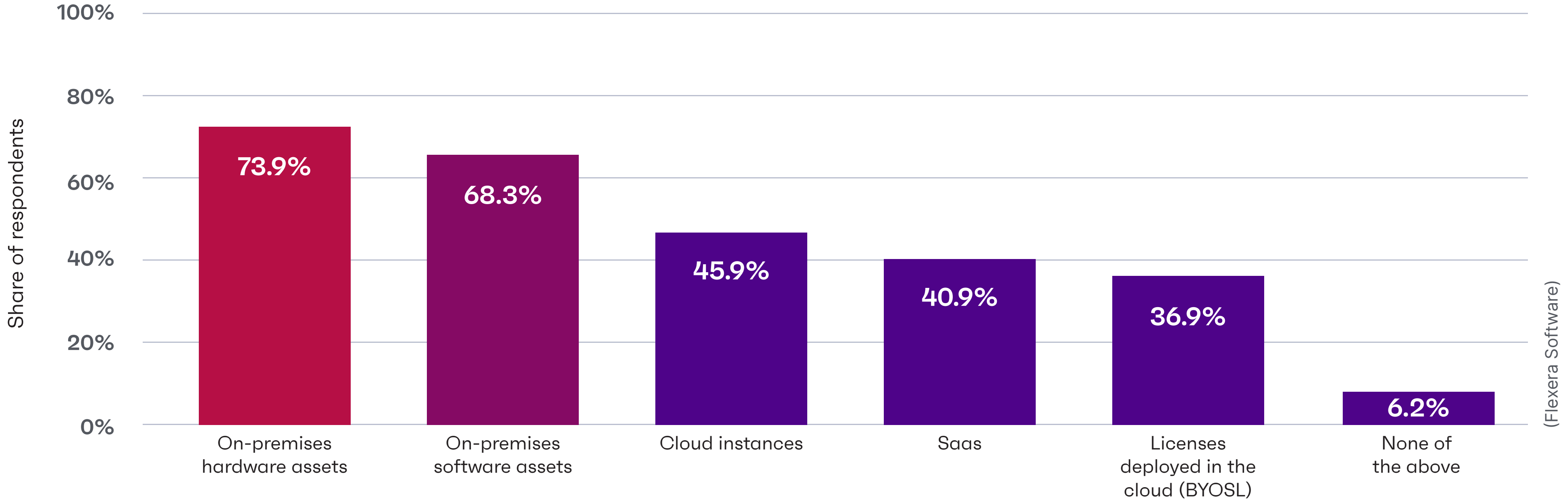
To add more fuel to this fire of a shadow IT problem, IT teams have a better handle on asset visibility for traditional on-premises deployments than they do for any remote or cloud-based assets. (Flexera Software)

These global surveys and studies correlate with Ivanti's own anecdotal experience with clients and customers alike, who tend to find 25-30% previously unknown devices accessing organization networks after deployment of a UEM solution with active asset discovery capabilities.

Automated asset discovery run through a centralized UEM platform allows IT teams to:

- Detect all devices when they connect to organization infrastructure and networks.
- Reduce the risk of transient devices being online without remediation or segmentation.
- Remotely scan devices without an agent.
- Segment and quarantine potential harmful unknown devices, while still allowing the flexibility of a BYOD policy.

Q: Do you feel you have accurate visibility into the following environments?



(Flexera Software)

3 Automatic device enrollment speeds onboarding and end user compliance.

Part of a de facto hybrid work strategy involves accounting for initial onboarding of new employees – complete with provisioning new devices with the appropriate software and access permissions to end users who may never set foot in the office!

UEM solutions offer preconfigured user and device profiles to make deployments as simple as the hiring manager going into a self-service portal for requisitions and permissions without unneeded IT team involvement.

With automated endpoint enrollment, new devices and user profiles can be enrolled with minimal interruption to IT staff's regular duties or employees' ordinary workflows.

Automatically enforced policies and device configurations from the primary UEM solution also ensures universal policy compliance.

Finally, by deploying a UEM solution, organizations are no longer forced to rely on end users opting into needed updates or security applications. The UEM-managed devices automatically enroll themselves into the specific update schedule or application installation – no user interactions or permissions required!

Real-World Repercussions

From Upwards of 2-3 Days to 5-10 Minutes for Installing and Configuring Software

During interviews for a commissioned TEI study conducted by Forrester Consulting on behalf of Ivanti, an integration engineer at a footwear retailer estimated that his team used to spend two to three days per device installing and configuring software. (Forrester Consulting TEI study)

After implementing Ivanti Neurons for UEM, however, the interviewee stated: "Now, once it's imaged, they just install Ivanti and drag that device into all of the software tasks. It's done in five to ten minutes, and they just check it at the end of the day to ensure all the applications are there. That's definitely saved time from the user onboarding process." (Forrester Consulting TEI study)

FORRESTER®

4 End users report better digital experiences and increased productivity.

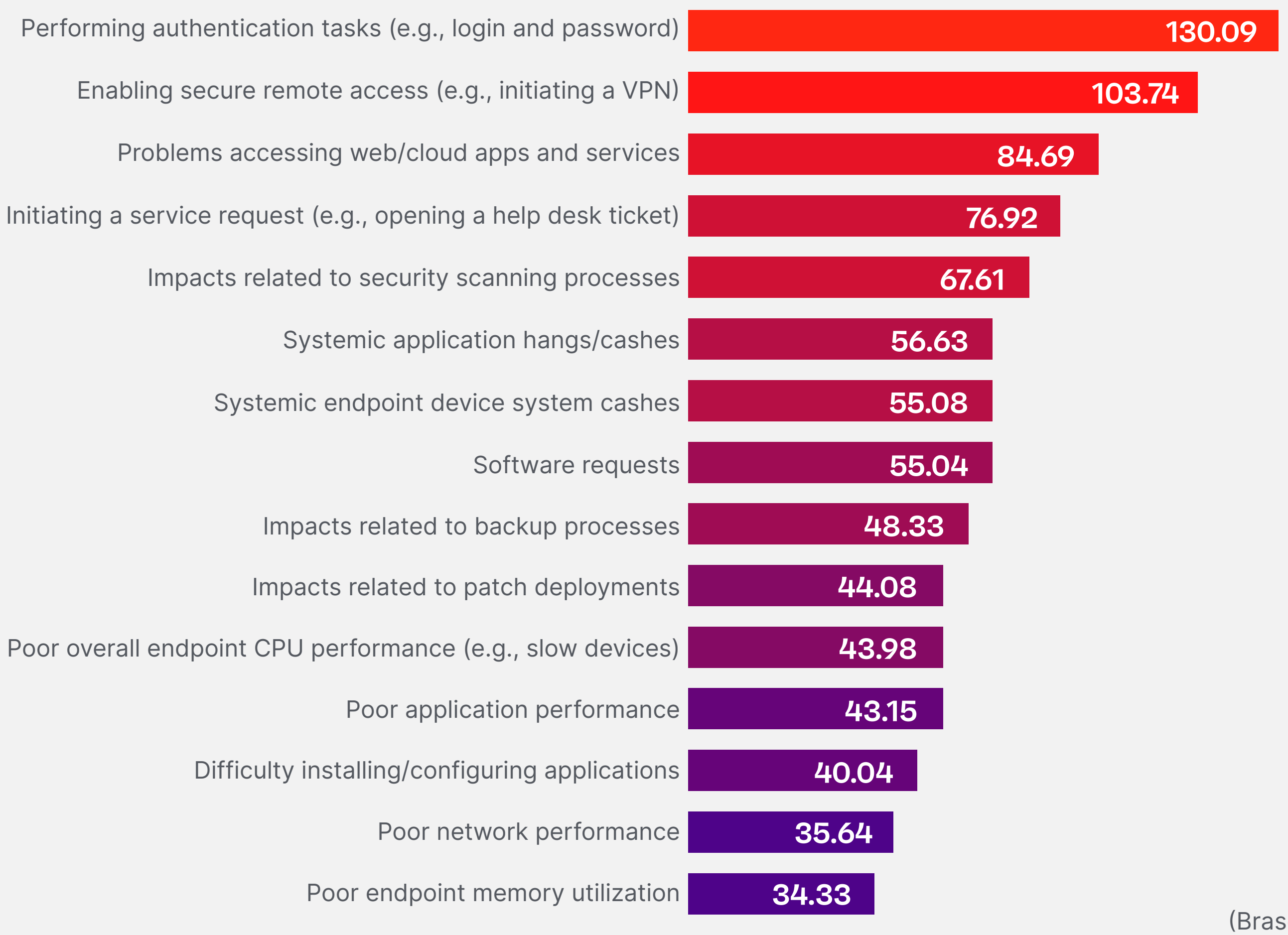
Every IT and Security team will agree with this single, simple fact: digital employee experience (DEX) matters.

Recent DEX research backs up this almost instinctive truth:

- 26% of surveyed employees – and 31% of IT and Security professionals – have considered leaving their job at least in part due to difficulties with technology. (Ivanti)
- The average employee is impacted by 919 endpoint management challenges every year, which works out to almost four issues each business day. (Brasen)
- It takes a user as long as 20 minutes to resolve each interruption caused by bad endpoint management and technology issues. (Brasen)

In fact, DEX is so important, that Gartner analysts predict that by 2025, 50% of IT organizations will establish a DEX strategy, team and accompanying management – up from just 15% in 2022. (Wilson, Cipolla and Paulman)

Average number of times per year each user suffers digital experience issues, according to surveyed businesses



(Brasen)

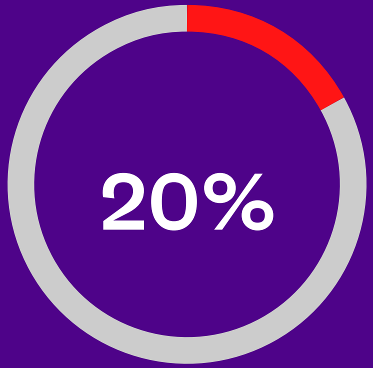
Of course, implementing a proper DEX strategy is a challenge in almost any situation. However, it becomes exceptionally difficult when only 20% of surveyed C-suite leaders actively plan to assign budgets for improving their employees' experience in the coming year. (Ivanti)

However, UEM solutions can give IT teams a quick overview of the device and user activities, allowing busy technicians to assess issues at a glance or dive deeper into robust analytics to determine the root cause of user frustrations for faster fixes.

Modern UEM solutions – with customized device and user-activity alerts, as well as pre-programmed service-level agreements and playbooks – can even automatically detect and proactively fix many of these poor endpoint management technology issues.

In this way, properly configured and robust UEM solutions represent one of the most fundamental and crucial components of a robust DEX strategy, helping IT teams "shift left" in their service management by remediating device issues before their users submit a ticket for assistance.

IT and Security teams everywhere can save the organization valuable time and money through proactive technology platforms like UEM solutions – even if their C-suites still need to come around to the importance of DEX investments.



Only 20% of leaders plan to assign specific budgets for improving employee experience.

ivanti

04

4 endpoint security use cases with UEM solutions

In this section, learn how your UEM solution helps your Security team:

1. Incentivize good security behaviors.

2. Secure a growing hybrid work environment.

3. Automatically enforce policies.

4. Easily integrate with patching or mobile threat defense solutions.

Why UEM users must consider endpoint security, too

You may have noticed that we frequently reference both the IT and Security teams throughout this guide – and that's no accident.

Third-party analysts believe that – considering post-pandemic Everywhere Work embracing more remote and hybrid approaches, rather than solely on-premises offices – UEM solutions will shift to incorporate more endpoint security use cases for "proactive and resilient defenses" against modern threat actors. (Cipolla, Wilson and Silva)

It's no surprise, then, that endpoint security remains a top cybersecurity investment priority for organizations worldwide – topped only by cloud security tools and internal user training. (PwC)

(And, if the proposed UEM solution could help secure cloud apps, then that would be a bonus for everyone involved!)

UEM solutions offer a unique starting point for both IT and Security teams to work from the same set of baseline information – their organization's devices, user profiles and network activities – to properly manage, secure and service all endpoints.

1 **Investing in a DEX-focused technology stack** to incentivize good security behaviors from end users.

2 **Securing an organization's rapidly expanding attack surface** means Security teams must address a wider variety of threat vectors from ever before, from IoT devices to unknown Internet connections.

3 **Enforced security policies and monitored user, device and app behavior** can prevent lateral movements in the organization's network from a compromised endpoint, and signal initial intrusions or potential insider threats before damage is done.

4 **Security tools such as patch management or mobile threat defense solutions** easily integrate with modern UEM solutions, providing a simple and speedy method for Security teams to remediate prioritized risks without interfering with regular user – or IT admin – operations.

However, while UEM's device onboarding automations and policy controls offer some basic cyber hygiene protections – and their device and user activity logs offer robust monitoring that can be enthusiastically used by the Security teams – most platforms will require additional controls and tools to reach their complete potential as an organization's single point of truth for all endpoint security. (Verizon)

1 Security's stake in UEM starts with DEX.

More than almost any other department outside of IT itself, Security teams will support investments for a more proactive DEX technology – including UEM solutions, especially as the risks of shadow IT and ever-expanding endpoint attack surfaces keep increasing in a post-pandemic, hybrid workplace.

- CIOs cite shadow IT solutions or products as a top concern for continuity of governments around the world. (NASCIO)
- 12.8% of 2022 cloud-based cyberattacks involved shadow IT. (Shackleford)
- Only 52% of surveyed security professionals report a "high" degree of asset visibility at their organization – and 10% said they don't use any sort of asset discovery tool at all. (Ivanti)

And hackers are already taking advantage of this gap between what the Security team knows they can protect – and what users have done to make their working days easier.

12.8% of all cloud-based cyberattacks in 2022 involved shadow IT.

When Bad DEX Almost Let Hackers Blow Up a Petrochemical Plant

In 2017, threat actors hacked into Saudi Arabian petrochemical plant Triconex. The security team only realized their systems had been breached when six controllers malfunctioned, triggering an alarm.

Incident responders quickly discovered that someone had remotely accessed the systems to insert malware – but that seemed impossible!

After all, the plant's security systems had been designed to foil remote attacks by requiring an employee to insert a physical key at the plant's console to make any configuration changes.

However, the plant's physical layout separated the controller from the control room, requiring operators to walk back and forth from one space to another to implement changes. An employee had kept their physical key in the controller's console to allow for them – and the hackers – to remotely access the code for updates.

Had other redundant security systems not alerted plant employees to the critical failures triggered by the hacker's activities, Triconex's compromised controllers could have turned off all safety systems and killed plant employees, either through chemical leaks or outright explosions.

This cyberattack could have been one of the first hacks resulting in a known human fatality – all because of one tired employee and the security designer's failure to consider human behavior while creating "foolproof" security systems. (Rhysider)

2

Secure more diverse working environments and IoT endpoints via UEM clients.

Remote work conjures images of employees working in a coffee shop, headphones plugged in, blissfully unaware of the fellow “customer” waiting for them to visit the restroom so proprietary files can be downloaded and their unlocked laptop exploited.

While human error will always remain in some capacity, endpoint security solutions and policies – enforced by the IT team’s UEM platform – will help to remediate some of the risks invited by a more geographically diverse workplace.

Let’s discuss two of the more common risks for endpoint security: the proliferation of the Internet of Things (IoT) and man-in-the-middle attacks in public network settings.

(Spoiler alert: both scenarios can be remediated through proper asset discovery, network segmentation and device monitoring – all of which can be executed through UEM solutions with the proper security-focused configurations and supporting features.)

Real-World Repercussions

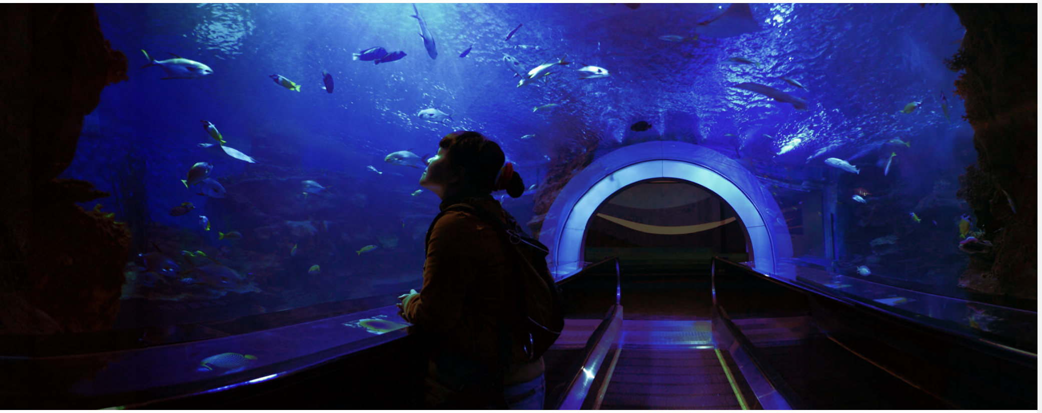
Unexpected Internet of Things (IoT) Attacks

IoT attacks made up more than 12% of all global malware attacks in 2021 – up from less than 1% of all malware attacks in 2019. (IBM Security)

Yet, 47% of surveyed IT professionals reported that their organization had no IoT compliance policy. (SAM)

IoT-enabled devices in both corporate and remote workplaces can be remediated through relatively simply network segmentation and active scanning capabilities.

However, many of these devices are ones that organizations and end users alike wouldn't necessarily consider in their risk analysis until it's too late – as these organizations discovered.



Fish tank thermometers

One North American casino discovered what havoc unmanaged IoT could wreak on their operations, as hackers exploited a vulnerability in their casino lobby's fish tank thermometer. Since this IOT-enabled tank was improperly segmented on the casino's network, the hackers could move laterally into the casino's cloud infrastructure and continue their attack. (Wei)

Medical devices

The WannaCry ransomware attack in 2017 prompted manufacturers and government agencies to reconsider vulnerabilities of internet-connected medical devices – including insulin pumps and pacemakers. (Chase, Coley and Connolly)

Vehicles

2015: Hackers hijacked a Jeep Cherokee, shutting down its engine mid-drive on the highway. (Greenburg)

2023: A Tesla driver discovered that the official Tesla mobile app allowed them to enter – and drive – a vehicle they did not own. (Day)

Post-2023: Government officials warn that "there is currently no comprehensive [...] cybersecurity approach" for either electric vehicles or their chargers (SANDIA) – vehicles which organizations' employees will drive to offices or offsite meetings, and to which they'll Bluetooth-connect their corporate devices.

Real-World Repercussions

Equifax's (Almost) Man-in-the-Middle Hack

One of the most common attacks on mobile devices and endpoints is the man-in-the-middle (MitM) attack. When employees connect to sensitive information on an insecure network or internet connection, hackers can put themselves in the middle of the data flow and "catch" any proprietary information.

The prospect of a MitM attack was why Equifax, an American consumer credit reporting company, took down their apps from both Apple and Google in 2017.

After the company infamously exposed some 143 million customers' personal information to hackers lurking in their network for months because they failed to patch a known exploited vulnerability (Khandelwal), security researcher Jerry Decime became curious: after this breach, had Equifax strengthened their security across the organization?

Decime looked at the mobile app versions of the Equifax software, and – to his surprise – discovered that the apps did not continue to use HTTPS protocols after initial authentication in a variety of critical areas. (Decime)

Any information transmitted after authentication between the user's device and the Equifax servers – including more personal information and financial transactions! – could have been intercepted and exfiltrated by a clever hacker who realized their security was simply surface level.

To Equifax's credit, they responded to Decime's communication within the hour and took down the insecure apps from both the Apple and Google app marketplaces. (Weissman)

However, this classic example of a MitM (almost) attack underscores the vital importance of secure communication between a user and a company's server – or your employees and your organization's sensitive information and networks.

UEM solutions and partner security tools can proactively limit exposure to these types of attacks through:

- Robust user access profiles.
- Automatic credential deprovisioning.
- Secure data access and communication channels, such as VPNs or Zero Trust controls – also deployed and monitored via UEM solutions.

3 Enforced security policies and device records prevent hackers from gaining a foothold in organization networks.

Proactive cybersecurity strategies not only try to stop hackers from breaking into organization networks, but also account for what happens if bad actors manage to enter.

Take the humble USB drive. A mainstay of salespeople everywhere, it can hold large files such as presentations, videos and music to use in new computers without having to wait for a network connection to upload or download material.

Of course, if USB drives can carry large files for legitimate purposes, then they can also carry malware, too.

UEM solutions can automatically deploy and enforce removable media policies by default. Through such policies, your organization's end users must request special permission to use memory-carrying devices with their company-owned machines, rather than leaving every device and endpoint automatically exposed to these attacks.

Real-World Repercussions

Stuxnet: The World’s Most Famous USB Drive Malware

Stuxnet is the name given to a computer virus allegedly crafted by certain intelligence agencies to bring down Iran’s nuclear enrichment program.

The facility operated under the tightest security – which meant that it was air-gapped from any Internet or outside network access. The only way malware could make it inside the facility was if an already trusted insider personally plugged it into a computer on the facility’s network.

So, the attackers made a computer virus that only attacked the industrial control systems the Iranian facility used for the centrifuges and loaded up the entire malware package on USB drives.

The tainted drives were distributed throughout the region for the nuclear scientists to find – perhaps at conferences, perhaps just handed out by trusted colleagues in the region.

Eventually, a scientist made the fatal mistake and plugged in a USB drive laced with the Stuxnet malware... and the program lost an estimated 1,000 centrifuges and wasted material, helping to pressure Iranian leadership into signing the 2015 Iranian Nuclear Deal.

To learn more about Stuxnet, check out these resources:

- “Ep 29: Stuxnet” by Jack Rhysider
- “Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon” by Kim Zetter

The device and user logs that a UEM platform records can be used for security purposes, too.

If the organization has reason to believe an employee may present an insider threat, then the Security teams can check a device's records for signs that sysadmin-level tools such as PowerShell were illegally installed and used on a user's device.

Or, perhaps an organization's system alerts to an ordinary "user's" activity, which shows the user suddenly performing advanced networking techniques on their organization's managed device.

Such activities may be a sign that it's not actually the authorized user at all, but rather a hacker hiding behind that user's authentic (but compromised) credentials, attempting to escalate privileges within the corporate network.

With the right configurations, alerts and security tools, these activities could be detected on an endpoint or mobile device long before the hacker ever moved laterally in the organization's network or gained admin-level permissions.

And – as rising cyberinsurance rates place new pressure on already strained organization finances – both IT and Security teams may find it quite economical to enforce stricter removeable media policies and user activity alerts for both proactive risk remediation and lower insurance premiums. (Breg)

4

Easy integrations offer simple, one-and-done security implementations.

While a well-integrated UEM platform offers basic cyber hygiene opportunities, it cannot be the end-all of your endpoint security solutions.

However, UEM solutions offer a supremely well-positioned launch pad for other tools – such as patch management or mobile threat defense solutions. After all, the UEM itself has a client directly installed onto every owned and managed organization device.

It's basically a few clicks away for other security tools to be hooked into that same device via the UEM client, immediately augmenting your endpoint security defenses while not detracting from your organization's DEX or end user productivity.

UEM + Risk-Based Patch Management

For example, UEMs can be combined with risk-based patch and vulnerability management solutions for a seamlessly proactive risk response to remediate actively exploited vulnerabilities in your current environment.

1 **The Security team analyzes current threat intelligence data,** running currently exploited vulnerabilities against your organization's currently used devices and applications.

- The UEM's active scanning capabilities ensure no device or application is missed during this initial assessment!

2 **The Security team deprioritizes or expedites current unpatched vulnerabilities,** depending on your organization's risk environment and priorities. They may consider:

- Priority level of potentially impacted devices, users, OS and organization-critical functions.
- Whether a vulnerability has been actively exploited by known threat actors in the wild.
- What sort of access or permissions an exploit could grant a threat actor.
- How often potentially impacted devices or applications are used by the organization, either passively or actively.
- How difficult a patch will be to apply, or if other remediation will need to occur (quarantine, segmentation, etc.).

3 **The IT team receives a list of prioritized patches,** along with:

- Information on why these patches should be implemented, based on the organization's unique risk factors – which reassures the IT team that Security isn't asking them to just patch all possible vulnerabilities!
- Specific devices or users for patch rollout, per predetermined cadences.
- Known possible interferences with current software suites or workflows.

4 **The IT team automatically rolls out patches to identified devices and endpoints via the UEM platform,** scheduling updates for least possible impact to end user productivity and keeping an eye out for any odd activities indicating a patch has interfered with regular workflows.

For more on risk-based patching and remediation strategies, please consult *The Ultimate Guide to Risk-Based Patch Management.*

ivanti

The Ultimate Guide to
Risk-based Patch Management

A working reference for IT Ops and security
for modern patch program implementations

ivanti.com

UEM + Mobile Threat Defense

Everyone is vulnerable to phishing – even the pros!

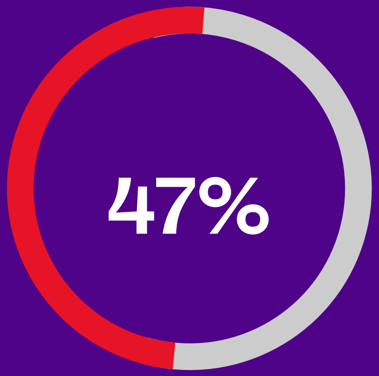
Phishing campaigns are a known entry point for ransomware gangs in particular, making up 54% of all ransomware delivery methods as of 2020. (Datto)

Specialized "whaling" phishing attacks – hacker-crafted email campaigns specifically targeting executive leaders in major corporations – resulted in American companies losing an estimated $2.4 billion USD in 2021. (Verizon)

New research has shown:

- 47% of IT professionals admit to falling for a phishing attack. (Ivanti)
- Only 43% of security professionals say their organizations have experienced a phishing attack in the last 24 months (Ivanti) – even as other industry reports find that 83% of organizations experienced a successful phishing attack in 2021 (Verizon).
- Over a third of senior leaders admit to clicking on a phishing link – which is four times the rate of other office employees. (Ivanti)

There's a 40-point gap between how many phishing attacks Security teams believe their organizations experience – and how many phishing attacks occur.



of IT professionals have fallen victim to phishing attacks.

So, if:

- IT specialists fall for phishing emails
- Security specialists don't realize their organizations are receiving phishing attacks
- Senior executives are getting targeted at higher rates – and falling for those attacks at higher rates

... then security training and spam filters on organization inboxes aren't enough to stop users from compromising organizations' security through phishing campaigns.

While a UEM's configurations and settings may help limit the initial damage caused by a phishing link click – particularly if it's been paired with a patching solution, severely hampering hackers' ability to escalate their privileges or move in the network – it will not be nearly as effective if not paired with a specialized mobile threat defense (MTD) solution.

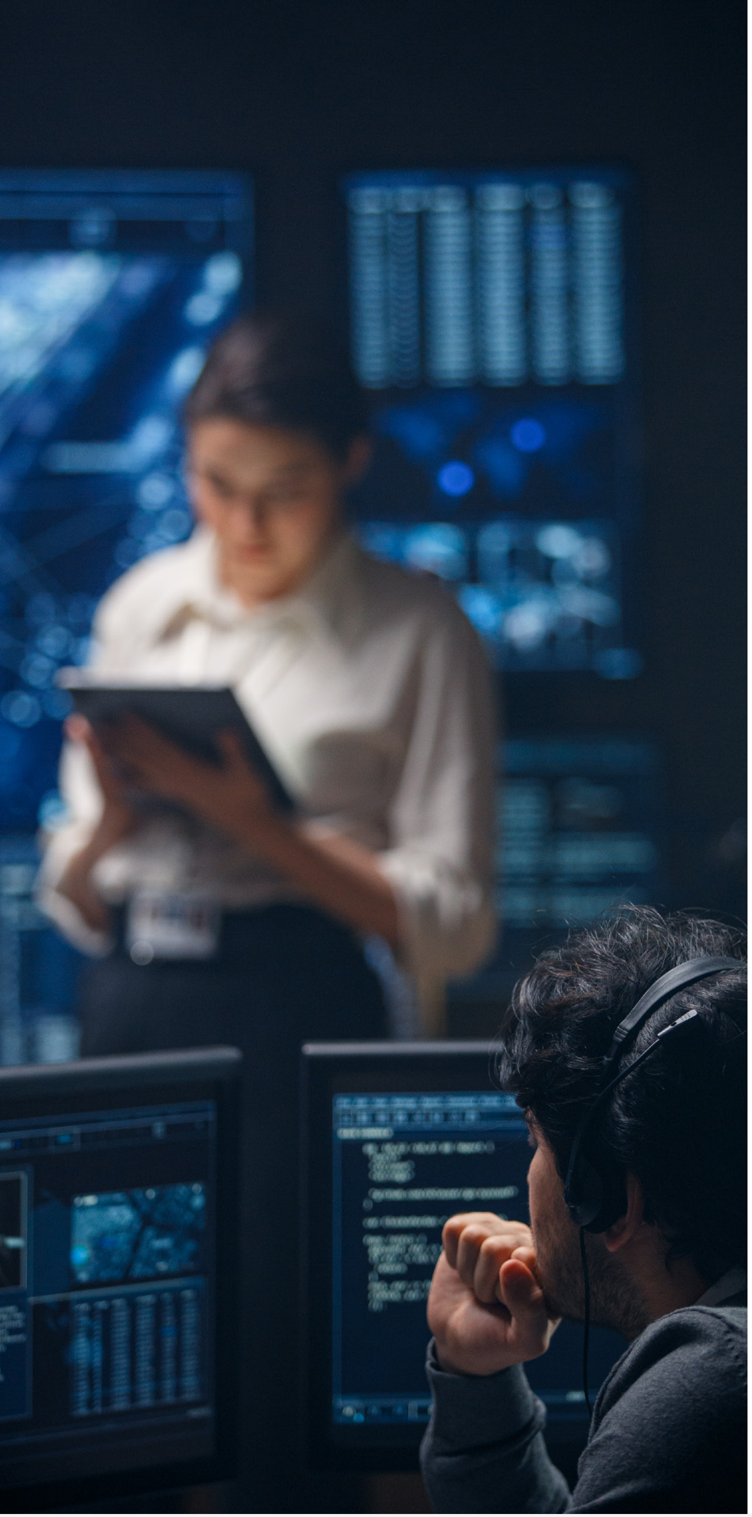
The best MTD solutions can run through an enrolled device's UEM client – either owned by the company or as part of a BYOD program – not interfering with any regular user activities or eating up any additional memory.

If the MTD solution detects:

- **An incoming phishing link:** the system immediately blocks the movement and ensure the action isn't completed by the user.
- **Potentially malicious activity:** the MTD and UEM solutions then automatically proceed with various levels of remediation, depending on the specific activity and potential threat level – up to and including removing user access to any organization applications, even on a personally owned device! – until the user has removed the app or otherwise fixed the issue.
- **An uninstalled OS update:** the system politely offers a push notification to the user, encouraging them to install the update. Increasingly levels of remediation are implemented if the user continues to not update their device — up to and including quarantine of any organization apps or access from the out-of-date device.

04

How to choose your UEM solution



There are many strong UEM solutions out there. While most offer the basic set of capabilities outlined in this guide, each vendor offers unique capabilities.

How, then, do you pick the UEM provider that's right for your organization? One that can meet you where you are right now – but can also scale and offer new possibilities for ever-better controls and security as your organization's needs mature?

Your unified endpoint management solution should:

- ☐ **Support the full range of devices and OS** your organization currently uses – or might use in the future – including macOS, iOS, iPadOS, Windows, ChromeOS, Android and Linux.
- ☐ **Offer a "single pane of glass" dashboard** that offers information on devices and user activity for both IT and Security teams alike to work from the same set of data.
- ☐ **Support both on-premises and cloud deployments**, including cloud-native applications – even if an organization believes that they're "just" in the office!
- ☐ **Dynamically search for assets**, ensuring no devices are left unmanaged – and no hackers are sneaking Wi-Fi pineapples onto your network. (Lutkevich)
- ☐ **Aggregate and clearly report on user and device information** to inform broader IT asset and Security endpoint strategies such as software licensing agreements or risk-based patching strategies.
- ☐ **Facilitate simple, automatic device enrollment and deployments.**
- ☐ **Run as quietly and "invisibly" as possible**, ensuring a positive technology experience for end users while proactively fixing issues and allowing IT teams to shift left into more strategic initiatives than clearing basic help-desk tickets.
- ☐ **Natively integrate with related endpoint security tools** such as risk-based patch and vulnerability management solutions and mobile threat defense products, as a UEM platform cannot do everything on its own – and run from any vendor that tries to tell you otherwise!
- ☐ **Implement standard automations, service-level agreements and alerts** such as deprovisioning protocols, onboarding procedures, activity spikes or lags, jailbreaking behavior from malicious apps, approved patch rollouts, etc.

Real-World Repercussions

The Total Economic Impact™ study for Ivanti Neurons for UEM

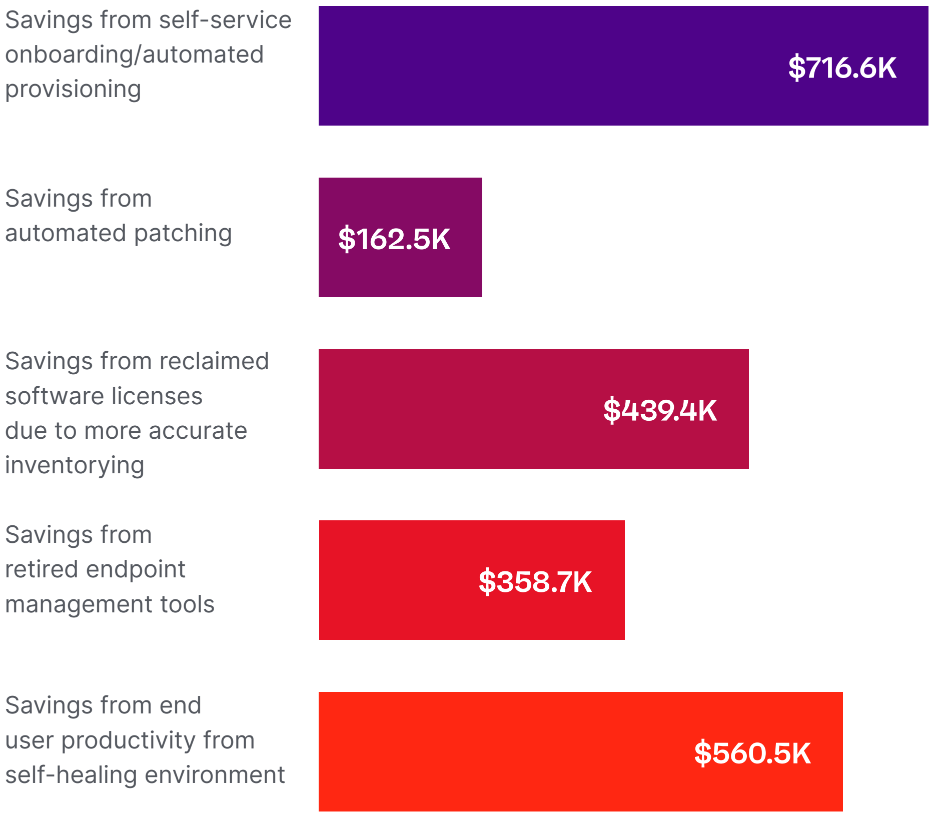
A July 2022 Total Economic Impact™ study by Forrester Consulting commissioned by Ivanti found that – by implementing Ivanti Neurons for UEM – a composite enterprise-sized organization managing 10,000 endpoints growing at 5% annually experienced benefits of $2.24 million USD over three years versus costs of $619,000. (Forrester Consulting TEI study)

These benefits added up to a net present value (NPV) of $1.62 million USD and a three-year ROI of 261%, with a payback period of the composite organization's initial investment within six months of installation. (Forrester Consulting TEI study)

According to the same commissioned TEI study, these savings were generated from:

- Tech stack consolidation
- Reclaimed software licenses
- Automated patching
- Improved user productivity
- Self-service onboarding and provisioning

Benefits (Three-Year) for Composite Organization



According to interviewees of commissioned TEI study

Self-Service Onboarding and Automated Provisioning
$716,632 USD 3-year savings for composite organization

“What we’ve developed now with Ivanti is an onboarding form that a supervisor can submit using the self-service portal. It automatically cuts a ticket and forwards it to the right teams. We don’t have to do a checklist like we would before.”

(The interviewee further estimated a reduction of IT time spend on the onboarding process by 50%.)

– IT specialist for a government agency

Tech Stack Consolidation and Retired Legacy Tools
$358,734 USD 3-year savings for composite organization

“My remote-control solution was $75,000 a year. My [IT asset management] (ITAM) was another $100,000. Knowledge management was another $20,000 a year... If I merge to one vendor and get all of those costs together, I get to save.”

– Director of IT and telecom support for a deathcare company

Automated Patching Capabilities and Integrations
$162,515 USD 3-year savings for composite organization

“It took us a month to design and discuss how we wanted to automate patches. Once we had the policy built, it takes less than an hour to set up a rollout project and then the patching just happens. I don’t have to do it and I have confidence that what I’m looking at is accurate.”

– Integration manager for a footwear retailer

Reclaimed Software Licenses
$439,449 USD 3-year savings for composite organization

“Before, if we were going to try and reclaim software, it was a very long process to try and reach out to users, asking them, ‘Hey, you haven’t use this in quite some time, can we pull it?’ As we brought our software licenses into the EPM solution [part of Ivanti Neurons for UEM], we’re able to run software reclamation automatically [...] That’s probably been our biggest savings that we’ve seen there.”

– Manager of infrastructure and endpoint delivery services for a food production company

Improved End-User Productivity
$560,521 USD 3-year savings for composite organization

“By doing some of the self-healing — updating old profiles, rebooting computers if they haven’t rebooted in seven days, patching in the evening — that work has helped our end users become more productive because the computers are getting back some of the resources that were being hogged up before [...] There is a financial benefit to the end-user side because of every minute they are able to save.”

– Director of IT and telecom support for a deathcare company

For more information, please read the Total Economic Impact™ of Ivanti Unified Endpoint Management (UEM) Solutions.

FORRESTER

The Total Economic Impact™ Of Ivanti Unified Endpoint Management (UEM) Solutions

Cost Savings And Business Benefits Enabled By UEM Solutions

JULY 2022

References

1. Bitwarden. 2022 Password Decisions Survey. November 2021. https://bitwarden.com/images/resources/2022-password-decisions-survey.pdf.
2. Bond, Shannon. Twitter employees quit in droves after Elon Musk's ultimatum passes. 17 November 2022. https://www.npr.org/2022/11/17/1137413251/twitter-employees-quit-elon-musk.
3. Bonner, Carole. Health and Wellbeing for the Remote & Hybrid Workforce. 20 October 2022. https://8926463.fs1.hubspotusercontent-na1.net/hubfs/8926463/Remote%20Hybrid%20Workforce_Formatted.pdf.
4. Brasen, Steve. Evolving Requirements for Digital Employee Experience (DEX). 4 August 2022. https://www.ivanti.com/resources/v/doc/ebooks/ema-iva009a-ivanti-requirements-ebook.
5. Breg, David. Quarterly Cyber Insurance Update. 10 February 2023. https://www.wsj.com/articles/quarterly-cyber-insurance-update-february-2023-62141c19.
6. Chase, Melissa, et al. Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook. 14 November 2022. https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response.
7. Cipolla, Tom, et al. Magic Quadrant for Unified Endpoint Management Tools. 1 August 2022. https://www.gartner.com/doc/reprints?id=1-2AQEK9FU&ct=220802&st=sb.
8. Datto. Datto's Global State of the Channel Ransomware Report. November 2020. https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf.
9. Day, Lewin. Tesla App Unlocks Someone Else's Car, Lets Them Drive Away in It. 14 March 2023. https://www.thedrive.com/news/tesla-app-unlocks-someone-elses-car-lets-them-drive-away-in-it.
10. Decime, Jerry. Settling the score: taking down the Equifax mobile application. n.d. https://www.linkedin.com/pulse/settling-score-taking-down-equifax-mobile-application-jerry-decime/.
11. Flexera Software. 2021 State of IT Visibility Report. June 2021. https://info.flexera.com/ITV-REPORT-State-of-IT-Visibility.
12. Forrester Consulting study commissioned by Ivanti. The Total Economic Impact™ Of Ivanti Unified Endpoint Management (UEM) Solutions. July 2022. https://rs.ivanti.com/reports/forrester-tei-of-ivanti-uem-solutions-2022.pdf.
13. Greenburg, Andy. Hackers Remotely Kill a Jeep on the Highway—With Me in It. 21 July 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
14. IBM Security. X-Force Threat Intelligence Index 2022. February 2022. https://www.ibm.com/downloads/cas/ADLMYLAZ.
15. Insight Enterprises & CIO. Insight intelligent technology report 2022: IT ambions for business transformation. November 2021. https://ca.insight.com/en_CA/content-and-resources/gated-content/insight-intelligent-technology-report-ac1252.html.
16. Ivanti. 2022 Digital Employee Experience Report. 28 June 2022. https://rs.ivanti.com/ivi/2700/4e528f833de3.pdf.
17. —. 9 Must-Know Phishing Attack Trends. 20 July 2021. https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465.
18. —. Getting Started With DEX: Core Areas of Focus to Deliver a Great Digital Employee Experience. 23 Novemer 2022. https://rs.ivanti.com/ivi/2734/f6efbc801083.pdf.
19. —. Government Cybersecurity Status Report. 9 March 2023. https://www.ivanti.com/resources/v/doc/ivi/2747/a856c631661d.
20. —. Press Reset: A 2023 Cybersecurity Status Report. December 2022. https://www.ivanti.com/lp/security/assets/s1/2023-cybersecurity-status-report.
21. Khandelwal, Swati. Equifax Suffered Data Breach After It Failed to Patch Old Apache Struts Flaw. 14 September 2017. https://thehackernews.com/2017/09/equifax-apache-struts.html.
22. Kolodny, Lora. Twitter is down to fewer than 550 full-time engineers. 20 January 2023. https://www.cnbc.com/2023/01/20/twitter-is-down-to-fewer-than-550-full-time-engineers.html.
23. Lutkevich, Ben. Wi-Fi Pineapple. October 2022. https://www.techtarget.com/searchsecurity/definition/Wi-Fi-Pineapple.

References

24. Morning Consult and IBM. IBM Security Incident Responder Study. 3 October 2022. https://www.ibm.com/downloads/cas/XKOY5OLO.

25. NASCIO. The 2021 State CIO Survey. October 2021. https://www.nascio.org/wp-content/uploads/2021/10/2021-State-CIO-Survey.pdf.

26. Palmer, Annie. Amazon employees push CEO Andy Jassy to drop return-to-office mandate. 21 February 2023. https://www.cnbc.com/2023/02/21/amazon-employees-push-ceo-andy-jassy-to-drop-return-to-office-mandate.html.

27. Paychex. Feeling the Burn(out): Exploring How Employees Overcome Burnout. 25 February 2019. https://www.paychex.com/articles/human-resources/impact-of-employee-burnout.

28. Proofpoint. 2022 Voice of the CISO: Global Insights Into CISO Challenges, Expectations and Priorities. May 2022. https://www.proofpoint.com/sites/default/files/white-papers/pfpt-us-wp-voice-of-the-CISO-report.pdf.

29. PwC. 2022 Global Digital Trust Insights. December 2021. https://www.pwc.se/sv/pdf-reports/cybersecurity/cyber-global-digital-trust-insights-2022.pdf.

30. Rhysider, Jack. Darknet Diaries, Episode 68: Triton. June 2020. https://darknetdiaries.com/transcript/68/.

31. Rundle, James. “Economic Uncertainty Weighs on Cyber Chiefs.” Wall Street Journal 13 January 2023. https://www.wsj.com/articles/economic-uncertainty-weighs-on-cyber-chiefs-11673562985.

32. SAM. IoT Security Landscape Report. July 2022. https://securingsam.com/wp-content/uploads/2022/04/SAM_IOT-Security-Report.pdf.

33. SANDIA. Cybersecurity for Electric Vehicles Charging Infrastructure. July 2022. https://www.osti.gov/servlets/purl/1877784/.

34. Shackleford, Dave. SANS 2022 Cloud Security Survey. March 2022. https://8645105.fs1.hubspotusercontent-na1.net/hubfs/8645105/white-paper/sans-2022-cloud-security-survey.pdf.

35. Shumway, Emilie. Monster: Two-thirds of workers would quit if forced to return to the office five days a week. 26 September 2022. https://www.hrdive.com/news/monster-two-thirds-workers-would-quit-forced-back-to-office/632690/.

36. Smith, Ray A. Quiet Quitters Make Up Half the U.S. Workforce, Gallup Says. 29 September 2022. https://www.wsj.com/articles/quiet-quitters-make-up-half-the-u-s-workforce-gallup-says-11662517806.

37. Tsipursky, Gleb. The return to the office could be the real reason for the slump in productivity. Here’s the data to prove it. 16 February 2023. https://fortune.com/2023/02/16/return-office-real-reason-slump-productivity-data-careers-gleb-tsipursky/.

38. Vanson Bourne for Nutanix. Nutanix Enterprise Cloud Index: Application Requirements to Drive Hybrid Cloud Growth (2019 edition). November 2019. https://www.nutanix.com/content/dam/nutanix/resources/gated/analyst-reports/enterprise-cloud-index-2019.pdf.

39. Verizon. Mobile Security Index 2022. 2022 August 2. https://www.verizon.com/business/resources/reports/2022-msi-report.pdf.

40. Wei, Wang. Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer. 16 April 2018. https://thehackernews.com/2018/04/iot-hacking-thermometer.html.

41. Weissman, Cale Guthrie. Here’s Why Equifax Yanked Its Apps From Apple And Google Last Week. 15 September 2017. https://www.fastcompany.com/40468811/heres-why-equifax-yanked-its-apps-from-apple-and-google-last-week.

42. Wilson, Dan, et al. Market Guide for DEX Tools. 31 August 2022. https://www.gartner.com/doc/reprints?id=1-2B07Z49S&ct=220902&st=sb.

43. Yang, Mary. Elon Musk gives Twitter employees an ultimatum: Stay or go by tomorrow. 16 November 2022. https://www.npr.org/2022/11/16/1137105935/twitter-elon-musk-ultimatum.

The Ultimate Guide to Unified Endpoint Management

How Modern Endpoint Management Solutions Impact Security and Employee Experience

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com