ivanti

4 Benefits of Modern Unified Endpoint Management

How integrating a modern, flexible UEM solution enhances both security and employee experience

Inside you'll learn how UEM:

01 Consolidates tech stacks

02 Automatically discovers unknown assets

03 Increases user compliance

04 Improves digital employee experience (DEX)

This eBook is part of [The Ultimate Guide to Unified Endpoint Management](#).

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

Introduction

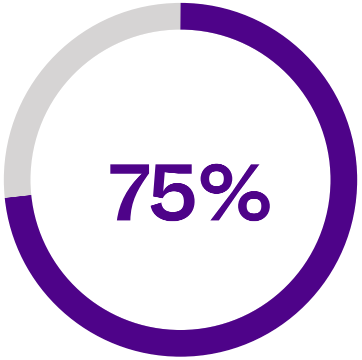
Now, most organizations already have at least one solution in place to manage the bulk of their owned and managed devices.

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.

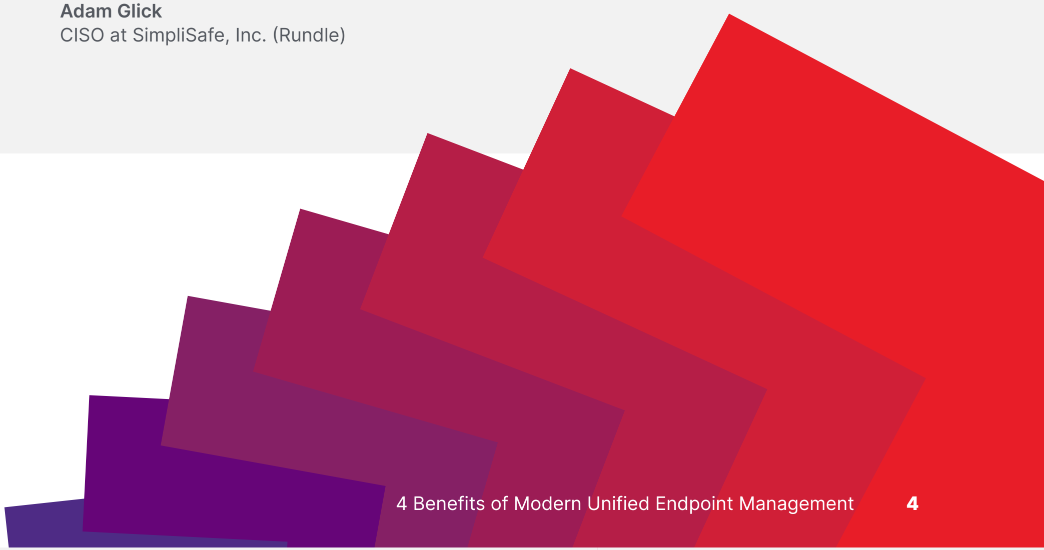
This strategic shift towards tech stack consolidation makes sense, especially when organizations consider global burnout and technology workforce trends:

- 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.”

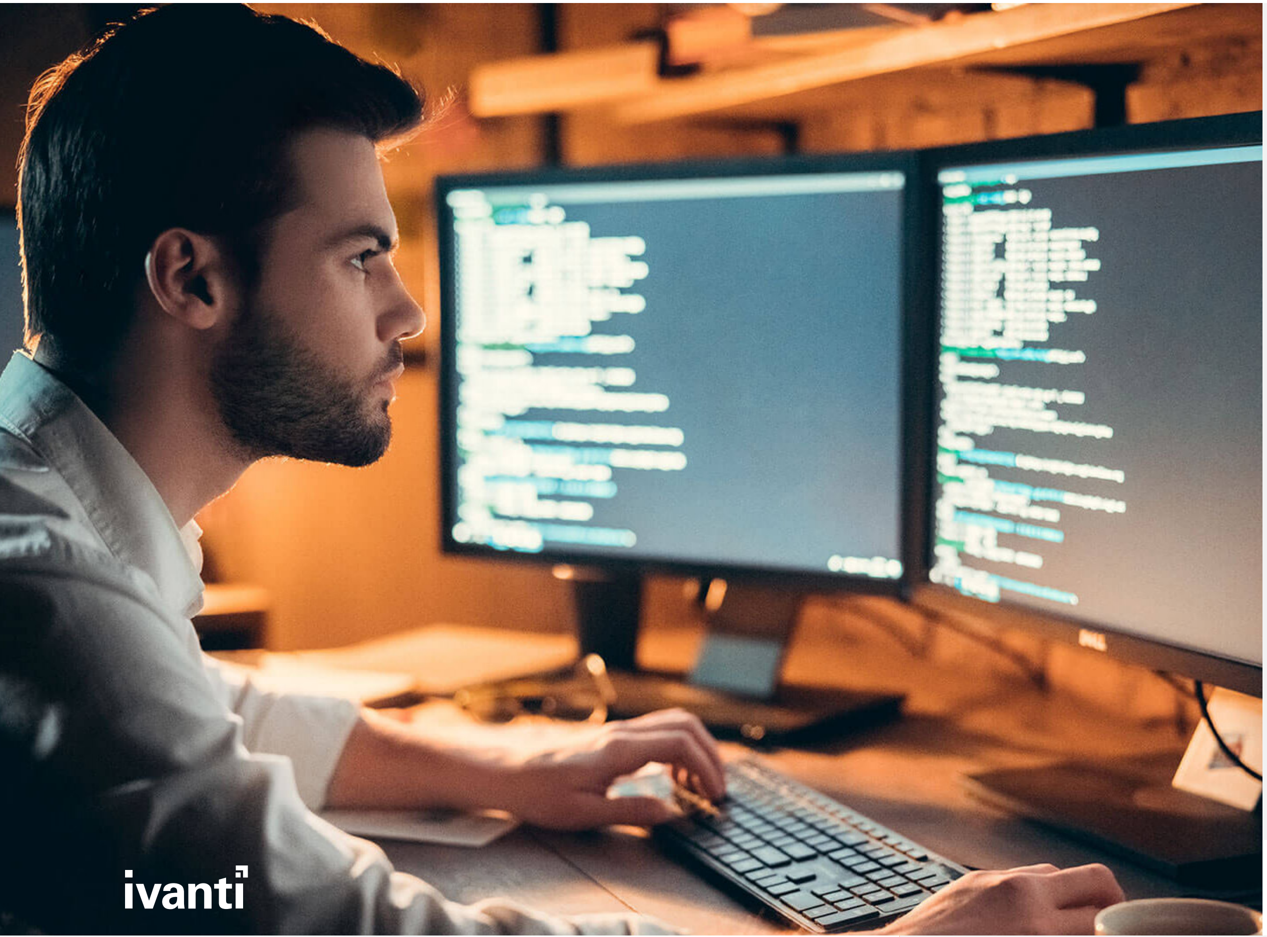
Adam Glick
CISO at SimpliSafe, Inc. (Rundle)



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

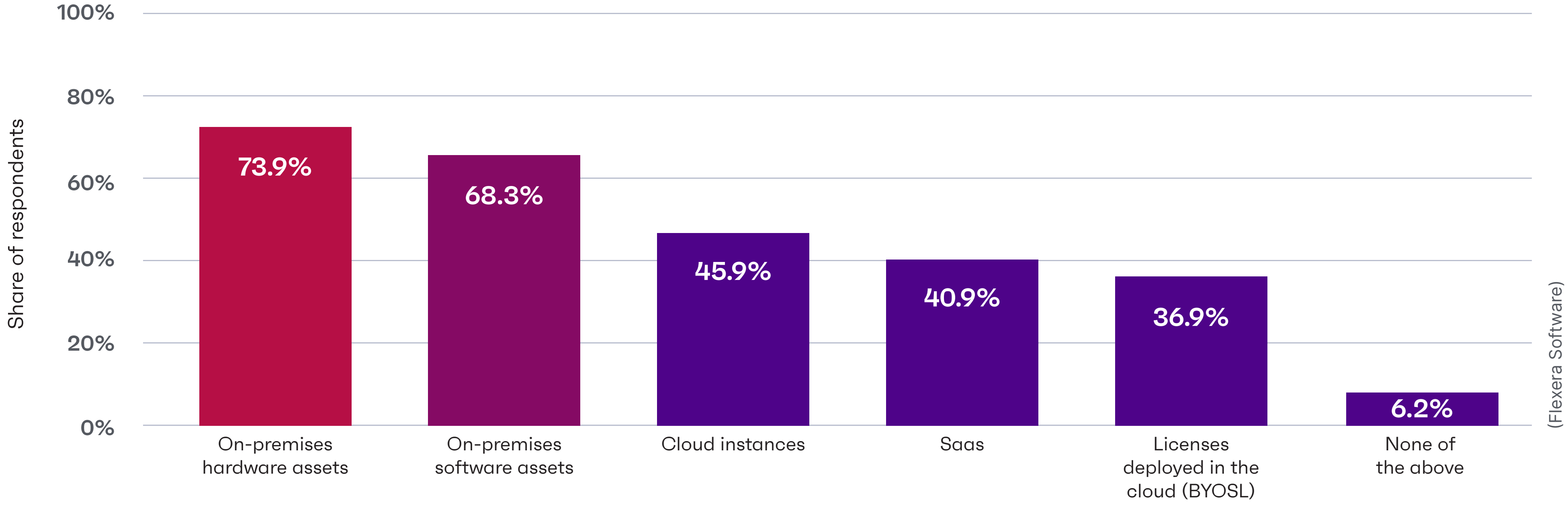
To add more fuel to this fire of a shadow IT problem, IT teams have a better handle on asset visibility for traditional on-premises deployments than they do for any remote or cloud-based assets. (Flexera Software)

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.

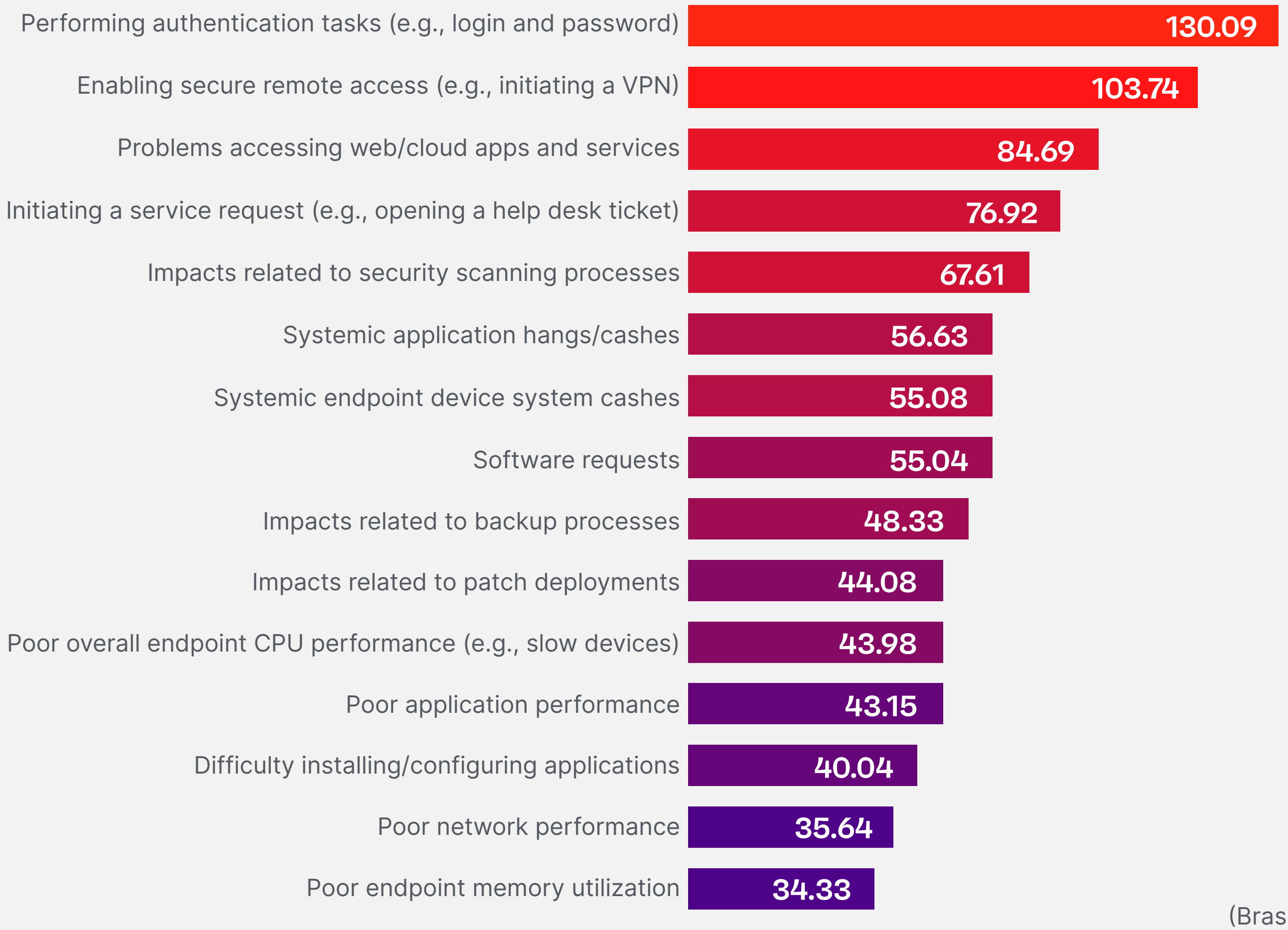
Every IT and Security team will agree with this single, simple fact: digital employee experience (DEX) matters.

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.

References

1. Bitwarden. 2022 Password Decisions Survey. November 2021. https://bitwarden.com/images/resources/2022-password-decisions-survey.pdf.
2. 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.
3. 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.
4. Flexera Software. 2021 State of IT Visibility Report. June 2021. https://info.flexera.com/ITV-REPORT-State-of-IT-Visibility.
5. 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.
6. IBM Security. X-Force Threat Intelligence Index 2022. February 2022. https://www.ibm.com/downloads/cas/ADLMYLAZ.
7. 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.
8. Ivanti. 2022 Digital Employee Experience Report. 28 June 2022. https://rs.ivanti.com/ivi/2700/4e528f833de3.pdf.
9. —. Press Reset: A 2023 Cybersecurity Status Report. December 2022. https://www.ivanti.com/lp/security/assets/s1/2023-cybersecurity-status-report.
10. Morning Consult and IBM. IBM Security Incident Responder Study. 3 October 2022. https://www.ibm.com/downloads/cas/XKOY5OLO.
11. NASCIO. The 2021 State CIO Survey. October 2021. https://www.nascio.org/wp-content/uploads/2021/10/2021-State-CIO-Survey.pdf.
12. Paychex. Feeling the Burn(out): Exploring How Employees Overcome Burnout. 25 February 2019. https://www.paychex.com/articles/human-resources/impact-of-employee-burnout.
13. 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.
14. 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.
15. 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.

Explore more in the full Ultimate Guide to Unified Endpoint Management.

Access your Guide

ivanti

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