ivanti

Shifting Security Left

How to power responsive security environments with current IT tools

Inside:

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

Security’s Crossroads:

Balancing proactive cybersecurity needs against tech consolidation pressure

In this section:

1. Create a responsive cybersecurity ecosystem…
2. …or consolidate your tech stacks?
3. How security can do both at once!

ivanti

Standing at the crossroads of conflicting security mandates

Your cybersecurity team must be proactive to counter future cyberattack risks while continuously remediating current security emergencies – a difficult task at even well-resourced and supportive organizations! – while simultaneously reducing their tech stack footprint, "making do with less" to align with increased budget pressures across every department.

How in the world could you accomplish both?

Of course, that's why you're reading this guide – so let's look at both mandates within context of the broader organization.

After all, at this crossroads, you can't just pick one mandate and ignore the another.

Your security team must find a way to walk both roads at once for proactive remediations with fewer resources.

This guide will show you how.

Security Mandate #1:

Create "responsive cyber ecosystems" for proactive remediation

In a recent Gartner report, for example, analysts described the need for modern security teams to develop what they're calling a "responsive cyber ecosystem."

These responsive ecosystems:

- Continuously scan the environment
- Identify current and potential risks
- Attempt to respond before problems emerge

These goals are achieved through continuous threat exposure management, user and access validation and the creation of a "digital immune system" that detects and minimizes security gaps.

These are ambitious initiatives for any security team, but especially difficult in today's environment encouraging the reduction of security tools – as we'll discuss next.

> These trends move forward risk resolution efforts by applying a **continuous approach to threat management and cybersecurity validation.** They help improve detection and response capabilities, and build more digitally immune identity ecosystems.
>
> - Gartner
> "Top Strategic Cybersecurity Trends for 2023"

Gartner

ivanti

Security Mandate #2:

Consolidate tech stacks in the security cost-centers

Meanwhile, the second trending demand to consolidate and restructure security tools illustrates how not even security and IT departments can entirely avoid the financial pressures of an unpredictable economy.

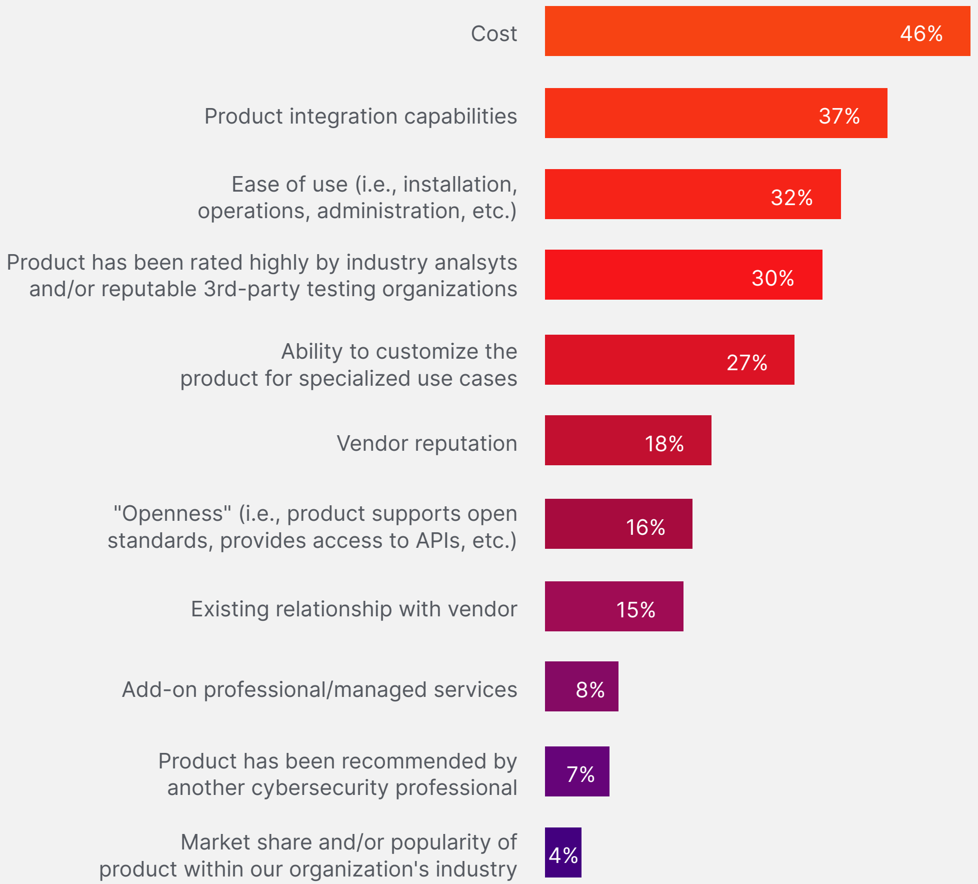
After all, while important for business security and functioning, both teams do not directly generate revenue.

This perception of security as a cost center has led to increased pressures on CSOs and CISOs to lower department overhead – in part through technology consolidation and increased integrations of their current tools – per industry interviews from the Wall Street Journal.

And, according to recent research from ESG and ISSA, surveyed cybersecurity professionals are more likely to consider cost, product integration capabilities and ease of use before third-party testing or industry analyst recommendations.

These pressures have further driven organizations to consolidate their tech stacks, seeking multifunctional platforms rather than niche or "best of breed" technologies.

Which of the following product considerations are most important to your organization when purchasing cybersecurity technologies?



(Percent of respondents, N=280, three responses accepted) Source: ESG, a division of TechTarget, Inc.

The third path: Leveraging cross-department tools for proactive security use cases

With two seemingly opposed mandates – not only to put out current fires but also stamp out future ones, and on an increasingly limited budget for no room for single-use tools – security teams face an impossible decision at an unclear crossroads.

Which road should they take?
Which priority comes first?

However, what if there was a way to forge a new route: an as-yet unnamed third path that could allow security teams to meet both obligations?

This third option must lead to both outcomes – proactive remediation and fewer expensive point tools – without getting lost in its implementation, burning out teams or wasting time and resources.

This path is only possible if security can better reuse and repurpose other teams' tools and solutions for their own use cases.

The first opportunity? The IT team's current tools and architectures.

In this way, security teams can create a responsive cybersecurity environment while reducing costs through repurposing already-budgeted and in-use IT platforms.

And, the benefits of the security team using already implemented IT tools extend beyond immediate cost savings. Analysts agree that tool simplification often improves operations and makes employees more efficient.

Shared tool platforms also:

- Enhance interdepartmental collaboration,
- Reduce the administrative burden on any individual team and
- Improve overall cybersecurity postures.

So, it is possible for security teams to achieve tactically proactive remediations without the niche tools catering to a single use case – but only if both security and IT teams expand their approaches into a shared understanding of the importance of "shifting left" beyond IT help desk ticket reductions or security's DevSecOps applications.

02

Defining “Shift Left” Beyond DevSecOps:

Finding common ground between security and IT approaches

In this section:

1. Conflicting “shifting left” definitions in security and IT
2. A shared approach for shifting left

Conflicting "shift left" definitions for security and IT

While both security and IT industries use the phrase "shifting left," each team defines the term differently. These differences lead to increased friction between the teams, despite several similarities and shared goals.

	Security's "Shifting Left" for DevSecOps	IT's "Shifting Left" for Help Desk Tickets
Definition	Security specialists and tools identify security risks during development, rather than as a last-minute before final deployment.	Technology automatically identifies potential IT problems before end users notice and file help-desk tickets.
Focus	Focuses on product and / or process development as part of a DevSecOps release model.	Focuses on service management of IT help desk obligations to internal end users.
Immediate Outcomes	Reduces product and process deployment delays through proactive, continuous remediation.	Reduces overall help desk ticket submissions and lowers escalation rates to higher-level IT specialists.
Other Benefits	Encourages a "security first" organizational culture, as security is no longer a last-minute consideration. Eliminates silos as security moves from external regulator to integral team member.	Empowers less specialized IT experts to correct problems. Lowers overall labor costs with fewer help ticket demands.
Timeline Impact	When security is proactively considered instead of a last-minute impediment to delivery, development timelines for products and processes become increasingly predictable (if possibly extended) with reduced known security risks.	IT personnel have newly found time and resources for both professional development and increased bandwidth more strategic, proactive tasks.

Ultimately, as different as the tactical expressions of shifting left are for the security and IT teams, each department's use case shares several fundamental traits.

In fact, both models demonstrate security and IT's shared need for proactive, less time-intensive remediation of problems early in the process, to counter costly last-minute emergencies.

A shared approach to shifting left for security and IT

At Ivanti, we use the term "shifting left" to refer to any strategic process which de-escalates and fixes issues before they become true problems or emergencies – often before any external stakeholder becomes aware there was an issue in the first place!

This way, shifting left becomes a cultural approach of automatic, proactive remediation that spans departments, uniting previously siloed processes under a single, unifying foundational approach.

While this definition closely reflects IT's core use case – that is, fixing problems before they start and before anyone else would know there's an issue – this shifting left approach aligns closely with security's mandate of creating a proactive and responsive ecosystem beyond DevSecOps-specific implementations or considerations.

By its very nature of fixing problems before humans know they exist, automation plays a heavy role in helping any department shift left – but especially for shared security and IT use cases, as each team will discover in the next chapter.

What does shifting left mean?

In this guide, "shifting left" is how we refer to the strategic processes and tactical automations which **identify, de-escalate and fix smaller problems before they become bigger emergencies** – often before any external stakeholder realizes any issues may have existed.

03

IT Tools + Security:

Practical use cases for security teams to co-opt common IT tools

In this section:

1. ITAM and ITSM + Security
2. UEM + Security

Common IT tools to use for security: ITAM, ITSM and UEM

Out of all the possible IT tools that security could use, we'll focus on two common solution platforms: service management, and device and endpoint management.

These solutions can be broken down further into three distinct solutions:

1. IT asset management (ITAM).
2. IT service management (ITSM).
3. Unified endpoint management (UEM), which also includes modern device management (MDM) clients and capabilities.

While IT has traditionally had oversight and budgetary allocations for these common technologies, security can still collaborate with their IT partners.

That partnership turns a once-point solution and niche product stack into a robust, cross-department, multi-purpose platform that can survive consolidation purges.

Common IT solutions and tools

Service Management

ITAM (IT Asset Management)

- Automatically updated list / database of an organization's assets
- Can track standard and default variables about assets, users and activity

ITSM (IT Service Management)

- IT's central user job board and quasi-project manager
- Can contain wikis, FAQs and internal form functionality
- Can host IT-related backend automations

Device and Endpoint Management

UEM (Unified Endpoint Management)

- Foundational endpoint device management and policy controls
- Can contain MDM clients that exist on each organization device and endpoint

ITAM and ITSM + Security

In this section:

- Defining ITAM and ITSM
- Security-specific use cases of ITAM and ITSM
- Shifting security left with ITAM and ITSM

ivanti

Quick definitions: ITAM and ITSM

IT Asset Management (ITAM) tools	IT Service Management (ITSM) tools
ITAMs provide management of Configuration Items (CI), such as hardware and software assets.	ITSM improve IT's ability to respond to track, respond and service technology requests from the end user and any other internal clients.
With this tool, enterprises can configure, optimize and track CIs throughout their lifecycles – from purchase to disposal.	ITSMs may also contain supplemental functionality for users to fix simple and common technical problems in a "self help" move to level-zero help desk support.

ITAMs rarely exist without partner ITSM platforms, though ITSM products can be implemented without supplementary ITAM partner functionality.

Together, a great ITAM and ITSM solution platform tracks:

- Original purchase date and information.
- Device owners and users.
- Currently applied user access application policies.
- Software OS, as well as current application and software installations and use.
- Device location.
- Device type.
- Performance, usage and compliance status.

Security-specific use cases for ITAM & ITSM

With the right set-up, policies and collaboration with the IT team, your organization's current ITAM and ITSM platforms could provide important insights for security teams, including:

1. **Dynamic asset discovery**
2. **Configuration Management Database (CMDB) opportunities**
3. **Increased Governance, Risk and Compliance (GRC)**
4. **Unique IT automations that can be reconfigured to assist highly manual security tasks**

1 Security and asset discovery

Asset discovery and management are foundational to any security program. In fact, every major cybersecurity framework (CSF) or data protection regulation considers asset discovery fundamental to building a secure system.

Why? Well, the first step to launching a successful cyberattack is usually reconnaissance. A bad actor seeks visibility into an organization's CI assets and systems, so they know what and how to launch an attack.

Asset discovery requirements in select CSFs

CSF	Relevant section	Relevant citation for asset discovery
NIST Cybersecurity Framework	First Core Function: Identify	"Identify: Develop an organizational understanding to manage cybersecurity risk to systems, people, **assets**, data, and capabilities."
Center for Internet Security (CIS) Critical Security Controls, V8	1st Control: Inventory	**"Actively manage (inventory, track, and correct) all enterprise assets** (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately **know the totality of assets** that need to be monitored and protected within the enterprise. "This will also support **identifying unauthorized and unmanaged assets** to remove or remediate."
Australia Cyber Security Centre: Essential Eight	Maturity Levels Overview	"This system includes **asset discovery** as an important step to prevent attacks at every maturity level."
European Law Directive 2022/2555 (NIS2)	Paragraph 44	"The CSIRTs [computer security incident response teams] should have the ability, upon an essential or important entity's request, to **monitor the entity's internet-facing assets**, both on and off premises, in order to identify, understand and manage the entity's overall organisational risks as regards newly identified supply chain compromises or critical vulnerabilities."

So, every framework states that – to defend against cyberattacks – your security team must understand exactly what you're protecting.

Of course in practice, most organizations tend to have a 20-30% gap in their network asset visibility.

In fact, only 47% of IT professionals would say that their organizations have full visibility into every device that attempts to access their networks.

However, the same automatic asset discovery capabilities included in various IT technologies platforms – including ITSM and ITAM products – could allow security teams to proactively analyze the risks associated with technological assets and users.

> **"If we don't know what's in our environment, we cannot secure it.**
>
> "The number one thing you are concerned about with vulnerability management **is understanding your attack surface and what's visible."**
>
> **- Chris Goettl**
> VP of Endpoint Security Product Management, Ivanti

For IT, automated asset discovery helps them reconcile budgeted device and software purchases against on-network devices and usage statistics.

When synced with an ITSM, these statistics can be paired with user help desk requests – to contextualize IT tickets and possible outages.

For security teams, the same asset discovery features in IT's solutions can be reused to meet the asset discovery requirements of any security framework.

And, automated asset discovery's security use case can be pushed even further than its default settings might suggest, helping security teams:

Detect

a vendor's device and control their access to conform with third-party access policies,

Scan

devices remotely for compliance with organizational security policies and patch updates, and

Segment or remediate

transient devices.

2 Security and CMDB

Knowing your assets is the first and most foundational step towards proactive security implementations. However, for your team to fully understand your organization's overall risk environment, you need to know how each device, app and user interacts with one another.

IT's Configuration Management Database (CMDB) provides essential insight into these relationships.

While an ITAM tracks an asset's lifecycle, CMDBs – often housed within ITSM platforms – manage the relationships between configuration items (CIs) and their environment.

Like an ITAM, a CMDB will include basic asset and user information, such as who uses a certain workstation and its location. But, it will also include contextual information, such as which devices and software interact with that workstation.

To an experienced security eye, these relationships reveal a CI's exposure to risk – and clues on how to mitigate that exposure.

Security and GRC

Mapping these on-network relationships and activities also allows for contextualized, real-time Governance, Risk and Compliance (GRC) understanding and enforcement.

How ITAMs & ITSMs help security's GRC

Governance

Greater context via shared data
No one wants to issue an order that no one will follow – or has no relevance to their team or organization.

Security and IT teams can help executive stakeholders understand their organization's current risk, user and asset environment, drafting relevant and meaningful policies with accurate data collected by ITAM and ITSM capabilities.

Default policies via backends
By using the same backend systems that IT already administrates, security teams can ensure their security-focused policies, controls and documentation are organized and easily accessed.

It also ensures policies are included by default within the broader organizational documentation that informs technology processes across departments.

Risk

Attack surface mapping via discovery
Using ITSM and ITAM products, security teams can map their organization's potential attack surface and analyze network, devices and user composition.

Better understanding of the true attack surface exposed to hackers informs security strategies and tactics that will work best with the organization's unique threat environment and network activities

Automation triggers via CMDB
Security teams can make use of current CIs and create custom, security-specific variables tracked in the ITAM's CMDB as both triggers for and components of automated formulas.

Compliance

Vendor enforcement via data collection
Using data collected via ITAM lists and constantly-updating ITSM platforms, security teams can help write vendor contracts that support and enforce practical compliance with their organization's policies, decreasing supply-chain security risks.

Endpoint enforcement via discovery
Asset discovery features allow both IT and security to identify unauthorized devices on sensitive organizational networks.

These features could also support automatic compliance alerts on devices; network segmentation; or even outright endpoint quarantine as needed – deployed via and enforced by other IT tools, such as UEM and MDM clients.

Security enforcement via IT policies
The same IT features that enforce general computer policies across the organization can also report on and enforce security protocols when required – from putting guardrails on IT admins assisting users with help desk issues, to sending alerts on possible policy breaches or insider threat indicators.

Real-World Repercussions

A hospital tablet thought experiment

Pretend for a moment that you work for a hospital.

Your IT and security teams track all endpoints that have internet capabilities, including tablets that should only ever be accessed by medical personnel.

However, a security specialist notices some odd activities for a tablet that should only ever look at internal hospital databases and intranets.

In fact, its entries have logged access to an external internet browser – and have attempted to download "leaky" gaming apps.

Since that suspicious behavior was flagged through ITSM / ITAM automations – in part using CMDB logs and CI variables – your security team investigates and asks the most recent logged users about the activity.

Eventually, the floor's supervisor admits they informally authorized staff to let patients use the tablet for casual internet browsing while they received treatment.

(In fact, this floor only sees pediatric patients!)

Admittedly, the supervisor went against internal protocols and policies designed to keep everyone – including the children! – secure from hackers.

However, the security team may choose to not punish this errant end user, assuming good intentions rather than laziness or bad attitudes.

Instead, they may work with IT and redeploy older, soon-to-be-retired tablets for patient use.

These tablets could let patients be able to play (security approved) games during treatment, while cordoned off from sensitive hospital intranets – automatically tracking any malicious activity.

While it might take a little sweat-equity from everyone involved at the start, this solution would be a triple win:

Patients feel catered to and well-treated, as they had before.

Security and IT together avoid becoming the "Department of No," enforcing a policy that users are actively trying to circumvent.

End user staff have an option besides sharing their "real" tablets with patients. They feel safe with security, making them more likely to willingly comply with future security and IT requests.

4 Shifting security’s workload left with ITAM and ITSM automations

As you consider co-opting IT’s tools for security use cases – particularly ITAMs and ITSMs – consider how you can use the current IT-focused automations and implementations to encourage your team’s shifting left.

You’ll find you can commit to more security actions with less labor, going beyond basic alerts and dials on dashboards for truly proactive risk remediation.

1 Improve the self-service options for end users

with security requests and questions, freeing up your senior analysts from phishing identification.

2 Unify security incident resolution

with IT’s ticketing software and prioritization queues (as fed from request forms) for better prioritization, tracking and contextualizing.

3 Repurpose background IT automations

for security purposes, since the same automations that can repair devices before users need to file tickets can also better secure endpoint environments and sense malicious activity.

Automation #1:

Improve security self-service for "Level Zero" support.

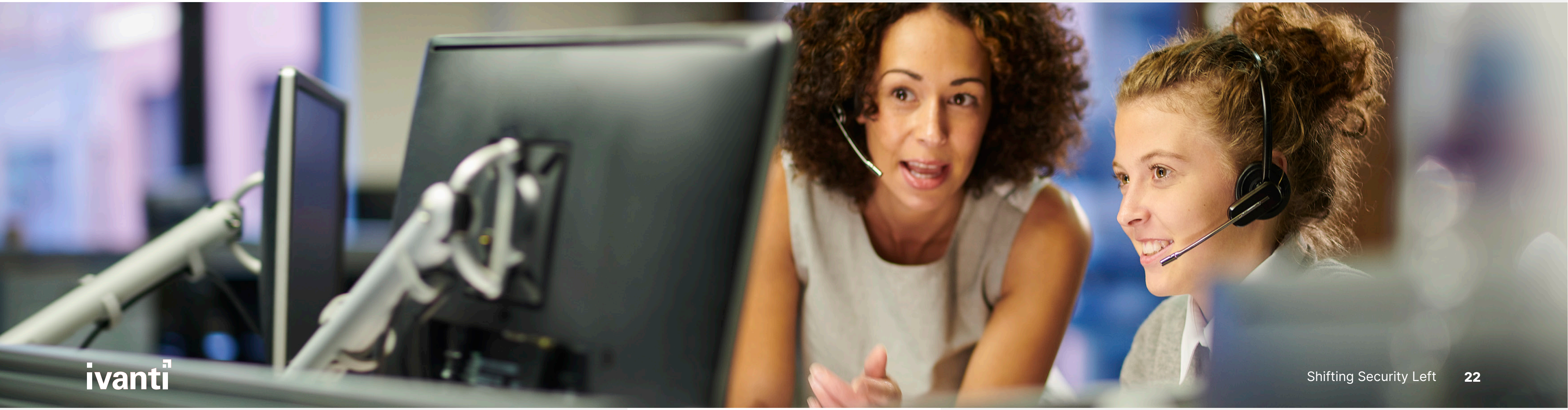
The same system that lifts the burden on IT help desks can also be used for security questions!

By centralizing common security-related questions and requests – such as how to enable two-factor authentication, report a suspected phishing attack or request a password reset – end users can help themselves, rather than asking directly for help from the security team.

By consolidating security's most frequently needed answers, information and requests into one place with the same infrastructure as IT, end users will know exactly where to go – after all, it's the same place they go for IT information! – and won't try to find a way around the system.

In your security wiki, consider including:

- **All current policies** – each prefaced by a scannable list of which users and devices are covered by a policy, what limitations or permissions are granted by the policy, exception request process and locations, and (most importantly) how this policy protects the organization.
- **How to request new passwords or usernames.**
- **How to submit a new vendor or software for security approva**l – as well as why security must approve a one-off app and how that keeps the organization safe.
- **How to implement 2FA** on each of the organization's supported devices and applications.
- **Security policy roadmaps** for planned future implementations, as approved for internal stakeholder communications.



Automation #2:

Unify security ticket queues with contextualized device and user data

The same ITSM platform with help desk tickets can form specific queues for security questions and remediation prioritizations.

You could even implement request forms for file access or policy exemptions within the security wiki, for level-zero “self service” user support.

These forms could then feed user requests into a centralized public queue, rather than scattered throughout email inboxes for specialists to ignore for “higher priorities.”

Then, these requests can easily be reassigned and resolved by lower-level security employees, reserving your strategic manpower for higher priority items.

Plus, with the creation of your security wiki, your security team can link back to policies written in the wiki to support their decision to either grant or deny requested permissions – even for executive stakeholders!

Automation #3:

Repurpose IT automations for extended, proactive security use cases.

The same repairing and proactive IT automations that trigger based on specific settings within ITAM and ITSM can be cloned and tweaked for a wide variety of security purposes.

IT automations for security use cases

Deprovisioning

Make sure departing employee or vendor credentials are decommissioned, triggered on contract terminations or user status inputs.

Baseline assessments

Automations can collect and aggregate your organization’s activity “baseline,” helping you spot future security impacts to productivity and possible intrusions.

Malicious activity flagging

Alert to potential internal threats or compromised accounts, triggered by out-of-norm CIs – prompting a manual device or user review by a human security analyst.

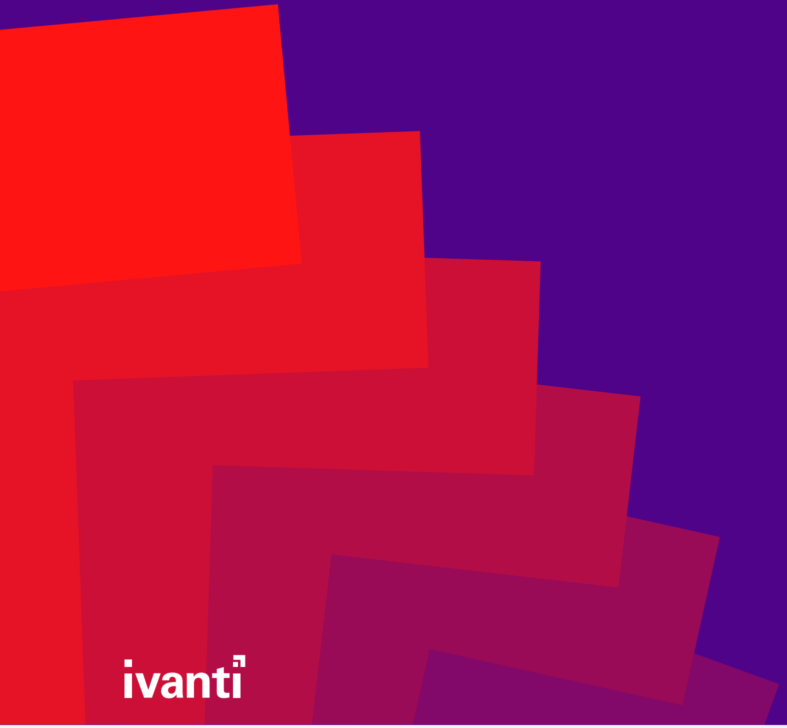
Rollout monitoring

During patch or policy rollouts, automations could be set to watch for disruptions, based on predetermined waterfall cadences and prioritized per user or device profiles as governed by current workflows.

UEM + Security

In this section:

- Defining UEM and MDM
- Security-specific use cases of UEM
- Shifting security left with UEM automations



Quick definitions: UEM and MDM

Unified endpoint management (UEM)

UEMs are an IT technology platform that system administrators use to manage multiple endpoints – that is, devices, hardware and other technologies – from a single platform or dashboard.

UEMs cover a wide range of operating systems (OS) and device types from many different manufacturers and developers.

Mobile device management (MDM)

Today often renamed as "modern" device management, MDMs were once a standalone niche technology that helped IT teams control and enforce policies, configurations and software on smartphones, tablets and other endpoints that support MDMs APIs.

However, MDMs were frequently limited to devices running specific operating systems, requiring IT teams to run several MDMs at once to manage all devices.

Today, while OS and niche device manufacturers still release point-MDM products to manage their endpoints, comprehensive UEM solutions will contain MDM functionality within their platforms.

UEM platforms allow IT teams – and now security teams! – to manage their hardware and software assets from a single platform and dashboard, regardless of:

- OS,
- Device type,
- Device or access location, or
- Unique user permissions.

Security-specific use cases for UEM

Your IT team's UEM and MDM clients can be reconfigured for security team's needs, including:

Proactive device deployments for new employees with security-first access controls in mind for specific devices and user profiles

Robust Internet of Things (IoT) controls and network segmentations to lock down difficult-to-update, hard-to-track devices that offer hackers a foothold into core networks

A comprehensive, cross-OS and cross-device foundation for future expansions and use cases – both IT and security alike! – when budgets increase and needs push

Security and device onboarding

A simple place for security to slip into current IT processes is during the initial onboarding of new employees – especially if your organization currently runs hybrid or fully remote deployments.

After all, IT is responsible for provisioning new devices with the appropriate software and access permissions to end users who may never set foot in the office.

This process offers unique opportunities for security to make sure even remote users and devices are securely configured from the onset, before they ever connect to an organizational network.

UEM solutions also allow IT admins to set preconfigured user and device profiles on new laptops or PCs based on previously established virtual machines (VMs).

Combined with an ITSM, hiring managers can use a self-service portal for requisitions and permissions without actively involving anyone in IT before the actual requisition and device / profile configurations.

Chances are, your IT department already has a process in place for new user onboarding. Ask them about:

- What process steps they already have in place,
- How they use their UEM for deployment, and
- Where your security personnel and policies might slip into their standard operating procedures.

Real-World Repercussions

Embedding Security Policies From Day One

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.

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.”

Rather than being an afterthought “when you have time,” your team’s configuration requirements could be included within this initial onboarding.

All that’s needed is thoughtful negotiations with your IT partners for the least-obtrusive default permissions, applications and accesses each user profile, team or device type requires at your organization.

FORRESTER®

Security and IoT

IoT endpoint security policies – delivered and enforced through UEM and MDM clients – offer a fantastic value-added opportunity as your security team seeks to repurpose current IT's tech stack.

After all, 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.

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

Perhaps it's not that these organizations lacked IoT policies, but rather that they just didn't know about them – either that they should have them, or how they should implement them.

However, with added security input from your teams and specialists, you'll be able to remediate vulnerable Internet-enabled devices in both corporate and remote workplaces through the UEM's relatively simply network segmentation and active scanning capabilities.

Real-World Repercussions

Thermometer Threats

One North American casino discovered what havoc unmanaged IoT could wreak on their operations when hackers exploited a vulnerability in their casino lobby's fish tank thermometer.

Since this Internet-enabled tank was improperly segmented on the casino's network, the hackers moved laterally into the casino's cloud infrastructure, continuing their attack.

Security and cross-OS integrations

While this eBook is all about repurposing current IT tools and platforms, we know that eventually, your organization's security risks and requirements will outgrow the policies and enforcement options your current tools offer.

However, UEM solutions offer a supremely well-positioned launch pad for integrating future security tool deployments in every device and user access profile – no matter where they are or what OS they run on.

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 end user productivity – a huge win for your IT allies.

Future security integration options to deploy via UEMs and MDMs

Patch Management (PM) and Risk-Based Vulnerability Management (RBVM)

A step beyond the automations and monitoring facilitated by ITSM, ITAM and UEM platforms, the UEM itself can be combined with risk-based patch and vulnerability management solutions for a seamlessly proactive risk response to remediate actively exploited vulnerabilities.

By pairing PM and RBVM solutions with a security-configured IT platform, security and IT teams alike can contextualize the most urgent patches for actively exploited vulnerabilities, cross-referenced by your current asset environment and critical workflow information from the ITAM / ITSM platform and distributed by the UEM per any IT-security SLAs.

Mobile Threat Defense (MTD)

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 be less effective than if policy is paired with a cross-OS mobile threat defense (MTD) solution.

The best MTD solutions can run through an enrolled device's UEM client – either owned by the organization or used in a BYOD program – while it dynamically senses, segments, quarantines and alerts on potentially malicious activity and phishing attacks.

Shifting security's workload left with UEM

Just as ITAM and ITSM offered IT-focused automation opportunities for security to shift left and become more proactive with previously manual tasks, UEMs also feature their fair share of automations that will prove useful for security goals.

UEMs have unique automations and implementations for security teams to:

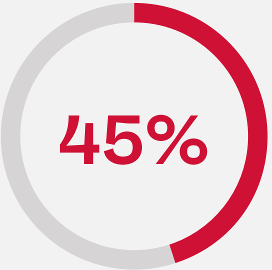
- Guarantee 100% decommissioning policy compliance of departing employees and third-party vendors' "zombie credentials."
- Enforce security policies on actively managed or BYOD devices allowed to access organization networks – whether they're in the office or working remotely.
- Sift through compiled, security-focused device records during incident response or for alert contextualization.

1 Guaranteed decommissioning compliance for “zombie credentials.”

In a global Ivanti survey of over 900 security professionals, only 68% of respondents said that their organization followed the credential deprovisioning guidance for terminated or resigning employees, third-party contractors and other vendors.

In fact, 45% of those same security professionals reported that they suspected former employees and contractors still have active access to company systems and files using old login information that was never decommissioned: “zombie credentials.”

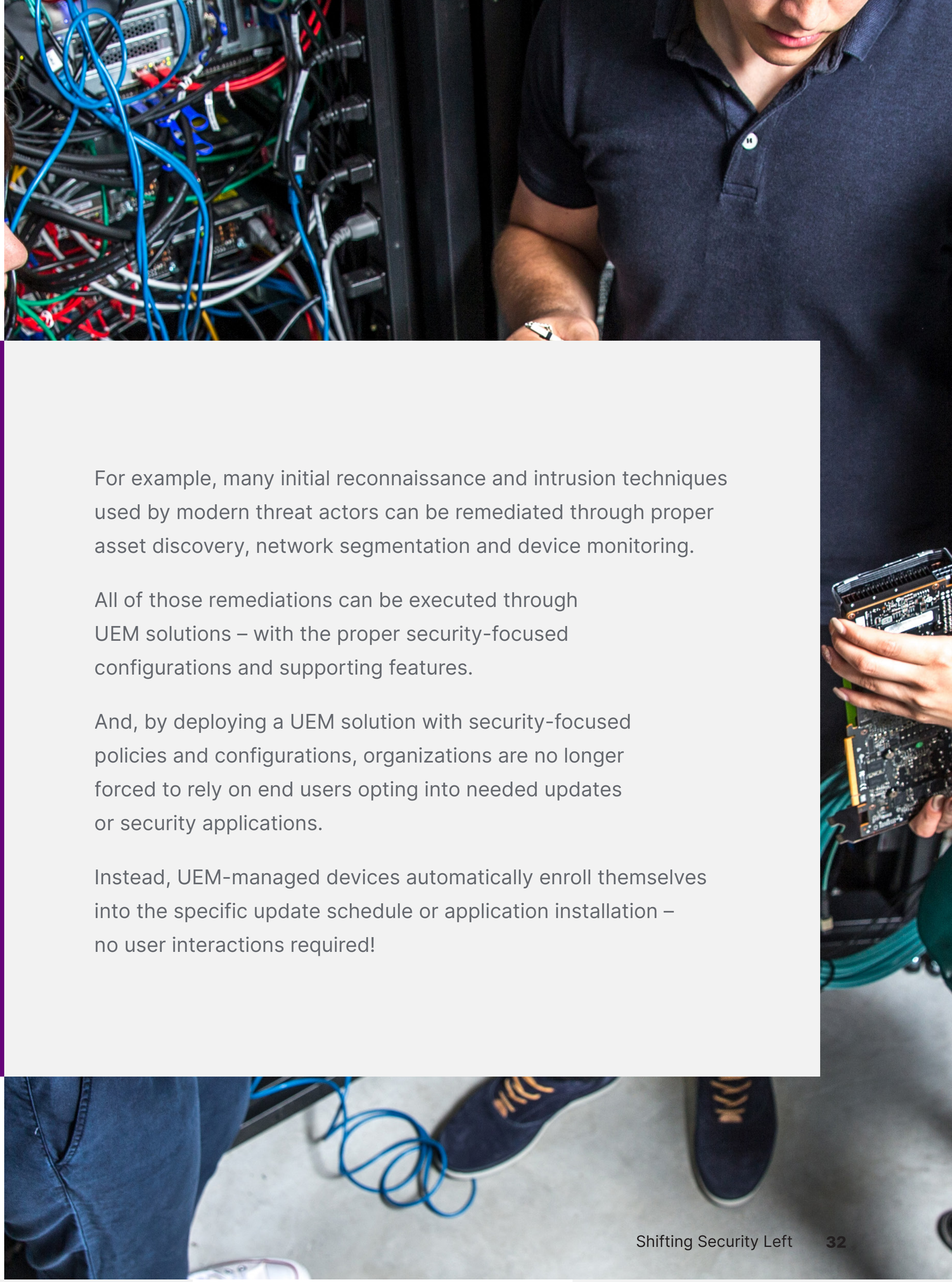
Automations within UEM platforms and the device-hosted MDM clients allow for immediate decommissioning of zombie credentials when a user’s internal profile is marked as no longer actively employed – eliminating future external threats from previous insider assets.



of security professionals say they either suspect or know that former employees and contractors still have active access to systems or files in the form of still-active usernames, passwords and login information.

2 Enforce security policies on all managed endpoint devices – in-office or remote.

While human error will always remain the weakest point of any security strategy, security solutions and policies – enforced by the IT team's UEM platform – will help remediate some of the risks invited by your less-invested end users, especially if they're in remote or hybrid workplaces.



For example, many initial reconnaissance and intrusion techniques used by modern threat actors can be remediated through proper asset discovery, network segmentation and device monitoring.

All of those remediations can be executed through UEM solutions – with the proper security-focused configurations and supporting features.

And, by deploying a UEM solution with security-focused policies and configurations, organizations are no longer forced to rely on end users opting into needed updates or security applications.

Instead, UEM-managed devices automatically enroll themselves into the specific update schedule or application installation – no user interactions required!

3 Review UEM-hosted device records during incident response.

The device and user logs that a UEM platform records – usually managed and reviewed by IT staff to better repair end user devices – can be used for security purposes, too.

If the organization has reason to believe an employee may present an insider threat, for example, then the security team 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 elevated admin-level permissions.

And – as rising cyberinsurance rates place new pressure on already strained organization finances – both IT and security teams will find it fiscally responsible to enforce stricter policies and user activity alerts for both proactive risk remediation and lower insurance premiums.

04

All Roads Lead to DEX: Security

In this section:

1. Why both security and IT teams (should) care about DEX

2. How backend DEX from shared tech stacks helps technical administrators

DEX: security's secret advantage when shifting left with IT

Throughout this guide, we've shown that security teams can grow from reactive emergency tactics into more proactive and responsive cyber ecosystems while simultaneously shrinking their technology footprint – just by making use of the ITSM, ITAM and UEM functionalities already supported by their IT team.

However, there's an additional advantage that organizations can see by combining and consolidating their IT and security tools: improved digital employee experience, or DEX.

These DEX benefits can cover the entire organization, above and beyond just end users, including use cases focused on:

- **Security needs**
- **IT needs**
- **General technology admin needs**

71%

of best-in-class security organizations say that end user DEX is a high priority or outright mission-critical to their organization's security strategies.

(That's a 20-point increase over less mature organizations!)

End user DEX benefits both security and IT

While security and IT departments both care about digital employee experience for different reasons, improving end user DEX is a win for everyone involved!

DEX benefits for security

DEX Benefit	Why security teams care
Better user experience disincentivizes shadow IT.	Employees turn to non-approved devices or apps – shadow IT – when they see the organization's version as cumbersome or frustrating. This shadow IT can introduce vulnerabilities into a network and expose organizations to cybercrime: 12.8% of cloud-based cyberattacks involved shadow IT in 2022. By prioritizing end user DEX, organizations make working with security-authorized applications and devices easier for end users while decreasing shadow IT. Why would they go to the trouble of installing a third-party app, if what they have works?
Backend, "hidden" implementations of security policies encouraging tacit user compliance.	Organizations can (and do!) issue paper policies requiring their end users to stay secure by taking or avoiding certain actions. Or… security teams could simply implement backend automations which silently enforce policies on every managed device and network user profile. Users only learn about these policies if they take an unauthorized action – otherwise, they'll never realize these restrictions exist. These DEX-friendly security implementations mean that organizations no longer rely on the goodwill and memory of the average end user, but rather on solid backend implementations that don't ask the user to do anything at all!
Hybrid-compatible security controls offer location-agnostic user convenience.	With remote and hybrid workforces on the rise, security teams can no longer rely on the basic "walled garden" approach to network or endpoint security… or for users to be able and willing to bring in potentially compromised machines into the office. Therefore, leveraging backend IT platforms like UEMs and ITAMs that can track, manage and secure any device type running on any OS – both on-premises and remote! – ensures security teams can keep organizations safe without requiring users to come into the office.

Did You Know?

Your organization’s IT department may have had ongoing DEX initiatives for improved end user productivity.

By partnering with the security team, your IT leaders will have additional leverage to justify the now-shared tech stack – allowing their DEX program to continue, when it may have otherwise been considered too abstract for C-suite stakeholders to justify further investment.

DEX benefits for IT

DEX Benefit	Why IT teams care
Fewer user experience issues mean fewer service desk tickets and faster service delivery.	If devices work the way their users require – with no interruptions for restarts or slow processing due to poor RAM – then they have no reason to file help desk tickets. When a religious organization implemented a DEX-focused ITSM, their IT team saw their ticket counts shrink and a 90% better service experience for their help desk support staff.
User self-remediation decreases IT labor costs.	When troubleshooting and request forms are located where end users can find and use it, then users – not your highly paid IT staff – can fix their own issues. After implementing an ITSM-based self-service portal with supplemental backend technology, one university found its new IT technology fully embraced by its students and staff alike – with widespread adoption of its new self-help functionality on network-linked devices.
DEX-focused technologies resolve root issues – not stop at surface-level fixes.	DEX-focused tech stacks allow IT teams to quickly assess and view devices and their user activities, no matter where in the world the faulty device may be. These insights – coupled with sophisticated automations that can "heal" more mundane and commonplace issues – let the IT professional diagnose and repair problems faster. The device is fixed the first time, on the first ticket – not forcing an end user to come back again and again for the same problem.

Administrator DEX benefits from shared tech stacks

Excellent digital employee experience doesn't stop at end users. The administrators who use such technology should also enjoy great DEX, too!

Additional DEX benefits for security and IT admins

DEX Benefit	Why admins care
Working tools and devices help users perform the jobs they were paid to complete!	31% of surveyed security and IT professionals have considered resigning from their current positions – in part due to technology difficulties. Why grind down your most expensive human assets, if improving their experience with your technology could help retain them in a competitive job market?
Shared platforms and dashboards with a DEX-first focus mean greater competency and collaborative understanding across departments.	Intuitive tool sets shared across departments allow for a shared understanding of information and a seamless presentation of problems. This shared knowledge and context increases empathy, reduces misunderstandings and improves cooperation across every department. And, skills transfer quickly from one department to another, since each shares a fundamental understanding of the underlying platforms.
Shared tech stacks could help recoup up to 9% lost admin productivity every year.	Tech employees frequently pivoting between different programs are losing substantial production time, per a recent Harvard Business Review article on "toggling." Computer-based knowledge workers switch ("toggle") between platforms, interfaces, screens and other microtasks an average 1,200 times a day – wasting an estimated four hours per working week and 9% of their paid annual labor. A consolidated, shared platform – or at least a tech stack featuring similar user interfaces and dashboards! – will reduce toggling strain on both security and IT administrators, improving focus on assigned challenges without distraction.

References

- Australian Cyber Security Centre. (30 June 2017). “Essential 8 Maturity Model”: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- Bowermaster, P. (February 2023). “Shift Left to Risk-Based Proactive Security Management.” CIO’s The Future of Work Summit.
- Center for Internet Security. (2021). “Critical Security Controls Version 8”: https://www.cisecurity.org/controls/v8
- Forrester. (2022). “The Total Economic Impact of Ivanti Unified Endpoint Management (UEM) Solutions”: https://rs.ivanti.com/reports/forrester-tei-of-ivanti-uem-solutions-2022.pdf
- Forrester. (2022). “The Total Economic Impact of the Ivanti Enterprise Service Management. A Forrester Total Economic Impact Study Commissioned by Ivanti”: https://rs.ivanti.com/reports/forrester-tei-ivanti-enterprise-service-management-platform-2021.pdf
- GDPR.EU. (n.d.) “GDPR Checklist for Data Controllers”: https://gdpr.eu/checklist
- Goettl, C. (25 March 2021). “Automated Patch Management and Team Swarming are Key Security Practices.” Ivanti: https://www.ivanti.com/blog/automated-patch-management-and-team-swarming-are-key-security-practices
- Goettl, C., & Masserini, J. (1 September 2022). “Vulnerability Management in Real Life: 5 Best Practices from Real-World RBVM Programs.” Ivanti: https://www.ivanti.com/webinars/2022/vulnerability-management-irl-5-best-practices-from-real-world-rbvm-programs
- Goettle, C. & Stryker, A. (11 May 2023). “Vulnerability Patch Prioritization Problems: Cybersecurity Research Results Part 2.” Security Insights: https://ivantiinsights.buzzsprout.com/1554237/12876518-vulnerability-patch-prioritization-problems-cybersecurity-research-results-part-two
- Harvard Business Review. (29 August 2022). “How Much Time and Energy Do We Waste Toggling Between Applications?”: https://hbr.org/2022/08/how-much-time-and-energy-do-we-waste-toggling-between-applications
- Ivanti. (18 August 2018). “7 Experts on What Shift Left Means for IT Departments”: https://www.ivanti.com/blog/7-experts-on-what-shift-left-means-for-it-departments
- Ivanti. (2022). “The NIST Cybersecurity Framework (CSF): Mapping Ivanti’s Solutions to CSF Controls”: https://www.ivanti.com/resources/v/doc/ivi/2694/fa2e133f20a8
- Ivanti. (2022). “The Ultimate Guide to Risk-Based Patch Management”: https://www.ivanti.com/resources/v/doc/ivi/2705/11190ce11e80
- Ivanti. (2023). “Press Reset: A 2023 Cybersecurity Status Report”: https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465
- Ivanti. (2023). “ITSM+ Toolkit”: https://www.ivanti.com/resources/v/doc/ivi/2760/e094c24df239

- Ivanti. (2023). “The Ultimate Guide to Unified Endpoint Management (UEM)”: https://www.ivanti.com/resources/v/doc/ivi/2508/b7d55619d0ee
- Ivanti. (28 June 2022). “2022 Digital Employee Experience Report”: https://www.ivanti.com/resources/v/doc/ivi/2700/4e528f833de3
- Ivanti. (n.d.) “IT Jargon Explained: CMDB:” https://www.ivanti.com/glossary/cmdb
- Ivanti. (n.d.) “IESO Shifts Left for Streamlined IT Operations”: https://www.ivanti.com/customers/ieso
- Ivanti. (n.d.) “Southstar Bank “Shifts Left” with Ivanti Neurons”: https://www.ivanti.com/customers/southstar-bank
- Miller, T., & Spicer, D., Stryker, A. (19 January 2023). “IT vs Security: When Hackers Patch for Profit.” Security Insights: https://ivantiinsights.buzzsprout.com/1554237/12071546-it-vs-security-when-hackers-patch-for-profit
- Morning Consult and IBM. (3 October 2022). “IBM Security Incident Responder Study”: https://www.ibm.com/downloads/cas/XKOY5OLO
- National Institute of Standards and Technology. (2018). “Framework for Improving Critical Infrastructure Cybersecurity” (p14): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Official Journal of the European Union. (14 December 2022). “Directive (EU) 2022/2555 of the European Parliament and of the Council”: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- Oltsik, J. (2022). “ESG Research Report: Technology Perspectives from Cybersecurity Professionals.” Enterprise Strategy Group - Information Systems Security Association International: https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Security-Process-and-Technology-Trends-Jul-2022.pdf
- Perri, L. (2023, April 19). “Top Strategic Cybersecurity Trends for 2023.” Gartner: https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023
- Pickering, D. (2022, May 5). “What is DevSecOps? How Great Developers Shift Left for Security.” Ivanti: https://www.ivanti.com/blog/what-is-devsecops-how-great-developers-shift-left-for-security
- Rundle, J. and Nash, K. (2023, May 22). “Security Chiefs Trim the Fat.” The Wall Street Journal: https://www.wsj.com/articles/security-chiefs-trim-the-fat-as-budgets-bite-83c82f99
- SAM. (July 2022). “IoT Security Landscape Report”: https://securingsam.com/wp-content/uploads/2022/04/SAM_IOT-Security-Report.pdf
- Shackleford, Dave. (March 2022). “SANS 2022 Cloud Security Survey”: https://www.sans.org/white-papers/sans-2022-cloud-security-survey
- Verma, A., Goettl, C., & Hindman, M. (2022). “How to Win Budget and Influence Non-InfoSec Stakeholders for Your 2023 Cybersecurity Program.” Ivanti: https://www.ivanti.com/webinars/2022/win-budget-and-influence-non-infosec-stakeholders-for-your-2023-cybersecurity-program

Shifting Security Left

How to power responsive security
environments with general IT tools

ivanti

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