BeyondTrust

>>> How ITSM and Integrated Security Accelerate the Business and Reduce Risk

Supercharging ITSM & Reducing Cyber Risk

TABLE OF CONTENTS

Introduction

There are more demands than ever on the service desk. Optimizing IT Service Management (ITSM) is crucial to the success of businesses. With fast and flexible workflows that efficiently satisfy the resource needs of a diverse set of users, modern ITSM can act as the engine for business acceleration. This includes giving users access to the emerging technology investments that enable digital transformation.

ITSM is also fundamental to protecting your organization from the proliferation of cyber threats targeting vulnerable points of entry to critical resources. Modern ITSM is uniquely positioned to reduce risks by securely managing access to IT resources for a growing number of users, both internal and external. At the same time, savvy attackers are targeting the service desk itself, such as via social engineering attacks, use of stolen or reused credentials, exploiting excess privileged access, and launching MFA fatigue attacks.

Clearly, integrating security across ITSM has never been more critical. With that said, cumbersome security controls that disrupt ITSM workflows can quickly alienate users and sabotage your business benefits. ITSM security needs to advance to match the evolution of your IT landscape and support more dynamic modes of consumption—empowering employees to work securely, without introducing friction or disrupting workflows.

Read on to learn the important ways ITSM is evolving to address modern changes and create new efficiencies. Also gain insight into the essential security considerations that must be integrated across ITSM to protect your service desk and safeguard the data and assets of your enterprise and your customers—whether they be internal or external.

The Evolution of Modern ITSM

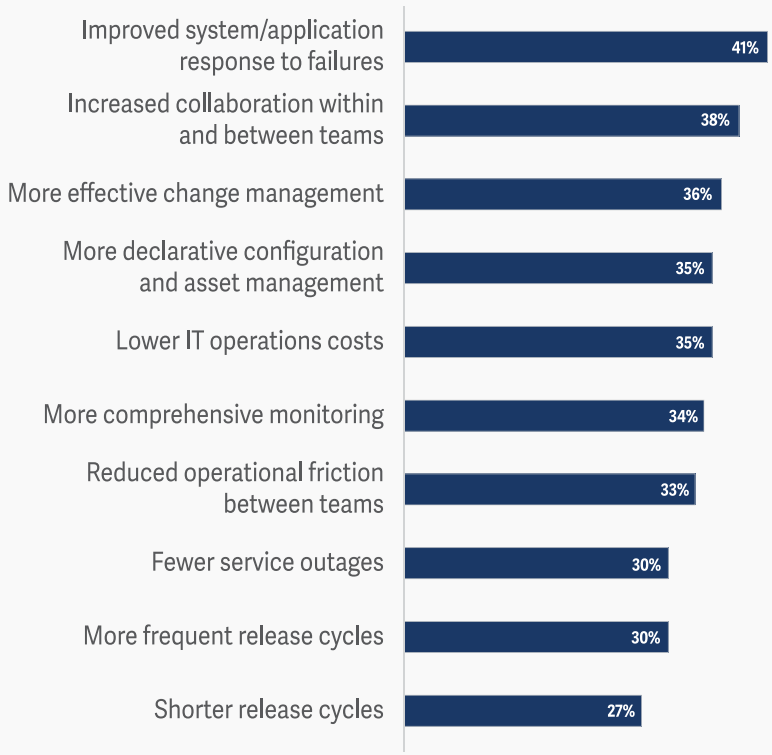
Today's enterprise consumers expect fast service 'where they live', on any device, from any location. They want the flexibility of multi-channel support (help via portal, phone, chat, etc.), and self-service options. They expect frictionless, smart services that not only automate common processes, but adapt quickly to new technologies and needs. This demands that modern ITSM be more responsive to a broader base of enterprise consumers (remote workers, developers, contractors, vendors, third parties, and even customers). Moving your services closer to your consumer—and becoming more responsive—requires smoother workflows, flexible service options, and intelligent adaptability. Smart, adaptable ITSM not only improves the user's experience, but frees the IT team from low-value routine work.

Out of necessity, modern ITSM has evolved to meet heightened user expectations. Greater flexibility of service choices, automated workflows, and self-service options all reflect the growing call to become more responsive to the changing needs of the consumers of IT, and the business itself.

The business benefits of modern, well-integrated ITSM depend closely on the extent and maturity of your implementation, and perhaps most pointedly, the inclusion of DevOps. These benefits include:

- Faster response times to service requests, evidenced by improved mean time to repair (MTTR) and other metrics, leading to more efficient use of resources (both IT and employee)
- Improved first call/contact resolution rate (FCRR)
- Lower IT operating costs
- Better monitoring/tracking of assets and actual usage.

TechTarget's Enterprise Strategy Group (ESG) recently surveyed organizations that modernized their ITSM. Modernization initiatives included better "integration into workflows and the use of automation to enhance efficiency, streamline operations, and ultimately deliver better user experiences." These organizations reported additional business benefits, some of which may be surprising and are displayed in the following chart:



Source: *Modern IT Service Management: Widespread Adoption Yields Major Benefits Despite Complexity. ESG. Jon Brown, Senior Analyst. June 2023.*

While traditional, inward-looking, operational metrics, such as MTTR, are still valuable, ITSM needs to include broader user experience measures and consider Experience Service Agreements (ELAs). End-user satisfaction—sometimes referred to as the customer satisfaction score (CSAT)—is another measure for support desk efficiency. Such newer measures of ITSM success reflect contributions to larger, even strategic, business initiatives, such as greater collaboration, innovation, and productivity.

The 'Engine' of Business Acceleration

Hidden Value in the ITSM Knowledge Base

ITSM represents a valuable knowledge base for modern organizations. The data captured across ITSM processes reflects the fundamental nuts-and-bolts operations of the organization, from tracking and managing access, to resource usage, to configuration and change management. This knowledge is invaluable for making many data-driven business decisions. This knowledge base can even serve to power ML/AI initiatives: the automatic categorization of incidents, building a solutions repository, the intelligent assignment of incoming requests, guiding faster event resolutions, and more.

ITSM acts as the coordinator of all the disparate processes that go into supporting users with the IT services they require to do their jobs. When this support is fast, smart, and flexible, ITSM can drive productivity gains across the enterprise; and it can accelerate the digital business.

A few ways these productivity gains can be achieved, include the following:

Workflow "Visualization" and Automation: IT usage and supporting processes are automatically monitored and, over time, their performance is instantiated by actual usage data. You can visualize bottlenecks more easily and, most importantly, this knowledge base serves as the feedback loop for more effective, revised, and new automated workflows.

Process clarification: Strictly-defined service management not only empowers users to accomplish tasks faster, and with less friction, but also cuts across departments and organizational silos. Unequivocal, data-based discovery of incidents or the root cause of inefficiencies can reduce time loss and costly disputes. The upside is you encourage collaboration between departments and business units.

Auditing and Compliance: ITSM is the natural focal point for collecting data and the managing of access to IT resources. This includes access to regulated data (e.g., financials and personally identifiable information (PII)), as well as sensitive corporate information like intellectual property, trade secrets, or plans for a merger.

ITSM is especially important in the monitoring and protection of identity security information, like login credentials and permissions. This database documents everything fundamental to business audits and compliance reports: approval processes, sign offs, whether changes followed procedure, etc. Centralization of this information makes compliance and forensic efforts much more straightforward.

In summary, modern ITSM is strongly positioned to drive enhanced collaboration, innovation, and productivity across the enterprise.

Securing Your ITSM Gains

The evolution of ITSM to address modern service challenges, boost productivity, improve customer service, and serve as a business acceleration catalyst is gaining momentum. However, these advances can easily be undone by lax security practices and poor security integration.

The demand for faster service and more collaboration, combined with digital transformation trends—such as increased utilization of cloud resources and more distributed (and remote) workforces—are all amplifying risks to the business and to the service desk itself.

The increase in technologies, identities, access, and privileges / entitlements has vastly increased the attack surface in recent years.

98% of security professionals say the number of identities are increasing, primarily driven by cloud adoption, the rise of remote working, increased mobile device usage, and third-party relationships.

Source: 2023 Trends in Securing Digital Identities. IDSA. June 2023.

Nearly half (47%) of critical misconfigurations in the cloud are related to poor identity and entitlement practices.

Source: 2023 Cloud Risk Report. CrowdStrike. June 2023.

The #1 ranked threat to cloud computing is insufficient controls around identities, credentials (passwords, keys, etc.), access and privileged accounts.

Source: Top Threats to Cloud Computing. Cloud Security Alliance (CSA). June 2022.

IT services organizations must not only protect against external threats, but also insider threats, including innocent mistakes (e.g., public cloud misconfigurations, development publishing errors, or leveraging unapproved applications or tools with shadow IT). Increased complexity also tends to contribute to increased instances of human error.

As long as service desks and help desks fail to monitor their technicians (track call logs, keep record of authentication changes, etc.), use poor password hygiene practices, lack strong MFA controls (FIDO 2 and more "phishing-resistant" technologies), or use unsecure remote access, it's a good bet threat actors will continue to be opportunistic, and successful, with their attacks.

74% of all breaches include the human element, with people being involved either via error, privilege misuse, use of stolen credentials or social engineering.

Source: 2023 Data Breach Investigations Report. Verizon. June 2023.

Here are four key areas of focus to improve ITSM security and resilience against threats:

1. **Social Engineering Threats**

   Many service desk technicians are susceptible to social engineering attacks. These users are simply doing what they've been trained to do—help resolve user issues. Help desk agents are also frequent targets for email phishing campaigns, and increasingly, phone calls (vishing) involving "users" pretending to need help with a password reset or other issue.

   In the past couple years, MFA fatigue attacks have even targeted service desks to bypass weak implementations of MFA. It's imperative to pair user training with the right technologies (identity security, privileged access management, etc.) to defend against social engineering threats.

2. Insecure Remote Access

As remote work and remote access have exploded, many existing remote access technologies—VPNs and RDP, etc.—have commonly been extended for inappropriate use cases. For instance, VPNs tend to have limited access controls and ability to segregate activities, while also lacking auditing capabilities over individual usage. As such, they should not be used on BYOD or used by a vendor to remote in.

Many processes and activities across ITSM involve privileged access; this access needs to be secured as such, meaning least privilege is enforced in both amount and duration of access, and all session activity is closely monitored and recorded.

3. Poor Credential Hygiene

Service desk technicians are often required to use admin credentials with elevated privileges to resolve support issues. Although privileged account credentials are a common target for attackers, credential management best practices are commonly sacrificed trying to quickly resolve issues. In fact, many service desk teams share and store credentials in plain text.

According to the 2023 Verizon Data Breach Investigations Report, 86% of breaches involve stolen credentials. Another recent Bitwarden's 2022 Global Password Survey found that 84% of people reuse passwords across multiple sites. If a reused password is cracked, it can potentially be used to hijack all the accounts using the password. Such practices were implicated in several high-profile service desk breaches in 2023.

It's imperative to instantly provide technicians with the credentials and authentication they need for expedited access to IT systems, while always enforcing credential management best practices, such as unique, complex passwords.

Embracing Zero Trust Security

Integrating security within ITSM, making it easy and intrinsic to service workflows, helps extend the application of least privilege across the enterprise. Least privilege can be enforced consistently, precisely when it is most required, with requests for new services and escalated privileges.

4. Excess Privileges / Entitlements Sprawl

Almost every cyberattack today exploits privileged access, either as part of the initial exploit (malware executing privileges), or to move laterally once a foothold has been gained. Most users have far more privileges than they need. The proliferation of cloud technologies has also resulted in the explosion of applications and machine identities with default privileges that are broad and that may be unmonitored by humans.

Enforcing the principle of least privilege access is one of the most effective ways for not only securing ITSM and the enterprise, but also in reducing errors and making compliance easier. Applying least privilege entails removing access wherever it is unneeded, and provisioning access with granularity to ensure the right levels of access are granted to those who need it, and only for those finite moments it is required. For instance, you should be able to enforce granular permissions over which features a service desk representative has access to. You may even want to require end-user prompting, so that the user receiving support must approve representative actions.

In 99% of pentesting engagements, IBM's X-Force Red was able to compromise client cloud environments through users' excess privileges and permissions.

Source: 2022 IBM Security X-Force Cloud Threat Landscape Report. September 2022.

How Well-Integrated ITSM Security Enables & Protects the Business

Siloed security tools create more friction that slows down workers—and the service delivery. And frustrated users will look to circumvent procedures, introducing more risks to the enterprise.

Dealing with many different tools also keeps IT/IT support teams bogged down with more administrative tasks, diminishing the quality of service they could be delivering.

The higher the interoperability and the stronger the integrations of your total ITSM solution, the better the experience for both your service desk technicians and their customers.

A comprehensive security stack that seamlessly integrates across modern ITSM to create one cohesive solution, protects the benefits you gain through accelerating your business, while also significantly reducing cyber risks.

ITSM needs to integrate the right security capabilities to apply the right policies, and it needs to be integrated in a way that is as invisible and frictionless as possible to all the different users and customers.

What should you look for in a cohesive solution?

For starters, the total solution must have broad platform support (Windows, macOS, Linux, iOS, Android, ChromeOS, non-traditional endpoints, etc.) and enable simple, smooth, and secure access to endpoints and systems quickly—from within a single application. There should be no "chair-swiveling" at the service desk, nor the need to cut and paste data from screen to screen.

Integrated ITSM security should centralize, manage, and track access privileges such that end users, the consumers of IT services, don't have to scramble or use additional applications to get the resources and services needed to do their jobs. The needed credentials should be available securely to the service desk from within the ITSM solution. And these credentials should always be secure, managed, unique, and abide by other best practices.

A modern, cohesive solution must also accommodate remote users, employees, and third parties. You should be able to connect to any remote device and securely initiate a remote session from within the ticket. The integration would enable the check-out of credentials using authorized ITSM approval flows—Incident, Change Request, Problem, and Request.

The integrations should include verifying and launching a privileged session from within the ITSM ticket. Privileged actions such as configurations or change management (e.g., software updates and patching)—which may include approval processes—can then be done directly from a change request. This not only secures the session, but also enforces any change management to adhere to the current authorized processes.

The overarching aim is to streamline service requests, make workflows as fast and as smooth as possible, while ensuring only the right users gain access to the right asset(s).

Well-integrated security also makes compliance activities much easier. Tightly interweaving security through ITSM workflows provides end-to-end tracking and documentation of access history: change requests, who approved them, and to which privileged account and asset. Otherwise, you would be dealing with multiple (or many) disparate applications. The integrated ITSM security solution becomes an indispensable system of record for providing complete, reliable, and readily-available audit trails and compliance reports.

Integrated Security Capabilities to Prioritize for a Total ITSM Solution

Modern ITSM is uniquely positioned to reduce the risks introduced by the changing IT consumer landscape. Capabilities to prioritize in an integrated ITSM security solution include:

- ☑ Robust security architecture that makes the integrated software technologies (remote access, etc.) resistant to misuse by insiders or compromise by attackers.
- ☑ Prebuilt integrations for common technologies and custom integration capabilities and robust APIs.
- ☑ Seamless integration with external user directories, such as LDAP, for simple and secure user management.
- ☑ Strong MFA, particularly for any privileged access.
- ☑ Secures remote access for privileged activities, using outbound-only session traffic, such as through TCP Port 443.
- ☑ Quickly extends highly secure access to desktops, servers, and systems, whether attended or unattended.

- ☑ Streamlines secure remote support sessions to any device – including third party access – by initiating directly from within an incident or change record.
- ☑ Applies least privilege across all access.
- ☑ Centralizes endpoint privilege management: opens tickets for new app requests, integrated approval workflow, and validates tickets before access is granted.
- ☑ Enables verification of tickets and privileged access requirements in real time, enabling seamless and comprehensive enforcement of least privilege.
- ☑ Enhances security by opening tickets based on events, connect to assets from within Incident, Change, Problem, and Request tickets, and sync assets and track data.
- ☑ Vaults and manages credentials so they are available within the solution for discovery, orchestration, and automating service ticket workflows.
- ☑ Injects managed credentials directly to initiate remote sessions, ensuring they are never revealed to end users and establishing an additional layer of obfuscation and security.

As IT infrastructure is dynamic, there are other capabilities needed to support organizational monitoring (notably change management), as well as financial and regulatory requirements. Some things to look for in an integrated solution:

- Provides comprehensive monitoring and recording. All actions take place, and can be documented, within the ticket/incident, such as request, approve, and open session.
- Enables the ability to search for and retrieve session details and associated tickets and change requests—including access or permissions—on demand.
- Provides detailed change tracking and recording, including accessing configuration items directly from a change request.

- Audits the who, what, and when of approval requests and to which privileged account and asset.
- Provides unimpeachable audit trails for fast, easy compliance reporting and forensics.

While zero trust implementations may not be possible for all facets of ITSM, as much as practical, organizations should consider aligning security controls to zero trust principles and tenets to minimize cyber risk and improve protection against threats. Doing so will also help with alignment to an increasing number of compliance initiatives.

Looking Ahead

The role of ITSM has increased substantially within the enterprise. Involving the security team early and often in your ITSM decision-making process helps overcome siloed thinking and encourages a more integrated, efficient solution, and a more collaborative approach to meeting the enterprise's objectives.

The user experience is central to the success of ITSM. Done right, the more integrated ITSM security solution can reduce risks and act as the engine for delivering strategic business advantages: increased productivity, collaboration, and innovation.

Want to better protect and enable ITSM and your service desk? **Learn how BeyondTrust does it.**