A Forrester Total Economic Impact™ Study
Commissioned By Microsoft
July 2018

FORRESTER®

The Partner Business Opportunity For Microsoft 365 Security And Compliance Solutions

Introduction

Forrester Consulting conducted a Total Economic Impact™ (TEI) study to examine and demonstrate the revenue and profitability opportunities available to Microsoft partners that build security and compliance practices around Microsoft 365 Enterprise. The robust security and compliance workloads and solutions within Office 365, Enterprise Mobility + Security (EMS), and Windows 10 enable partners to build new practice areas to assist customers in four areas: Identity management and access control (IDAM); information protection; threat protection; and, security management. Partners that build new security and compliance solution areas that help customers in these areas are increasing revenues, improving margins, creating customer stickiness, and helping differentiate their offerings from other partners.

> "With GDPR, we have a good opportunity to speed up adoption and sell and implement [Microsoft 365] E3 and E5. We could see a 20% uplift in projects and revenue because of GDPR."
>
> *— EMEA partner*

Forrester interviewed 17 Microsoft partner organizations across North America, Europe, the Middle East, and Asia Pacific that had established security and compliance practices built around Microsoft 365 Enterprise. While the maturity of these security and compliance practices varied across interviewees, our interviews revealed several benefits from building Microsoft 365 security practices, including new revenue streams, higher renewal rates, increased win rates on new customer opportunities, and improved upselling that grows customer lifetime value.

Interviewed partners shared that they were getting traction with new and existing customers in the security space due to recent high-profile security threats and breaches and new regulations like the General Data Protection Regulation (GDPR). Given this increasing focus on security and compliance themes across industries and regions, partners were actively building diverse security offerings to help customers with varying security program maturity levels. For instance, partner security and risk assessment and strategy solutions created substantial project consulting business opportunities early in the program life cycle, while setting the stage for future professional services work. Successful project work opened the door to a wide range of lucrative managed services opportunities. Partners also benefited from license revenue sharing from upselling to the Microsoft 365 E5 stock keeping unit (SKU) given the additional security solutions included in the E5 license.

The revenue and profit opportunity analysis below is built on a composite 5,000-user deal that represents the deal characteristics identified in Forrester's interviews. The analysis is intended to be used as a framework for partners to understand the total three-year business potential associated with building a Microsoft 365 security and compliance practice.

$694

Anticipated three-year increased revenue for leading Microsoft 365 security and compliance partner, per user.

$314

Anticipated three-year gross profit for leading Microsoft 365 security and compliance partner, per user.

Over 50%

Percentage of three-year revenues coming from managed services.

Partner Benefits Are Growing As Partners Establish And Scale Their Security And Compliance Practices

Partners interviewed by Forrester benefit in the following ways from building out and scaling Microsoft 365 security and compliance practices:

- **New revenue and profit opportunities.** New professional and managed service opportunities abound for partners that build security and compliance practices. Successful early-stage consulting work, including security assessments, breach remediation, security solution road mapping, and deployment services, often lands partners longer-term, reliable revenue streams through the delivery of ongoing professional services, managed services, and resalable intellectual property (IP). These downstream products and services help ensure customers remain productive and secure and provide partners with high-margin recurring revenue. The best-case model for this study finds $694 in increased revenue and $314 in increased gross profit per Microsoft 365 Enterprise user for partners that build comprehensive security and compliance practices.

> "A lot of business is coming in because of security, particularly GDPR. We are also seeing a lot of opportunity in healthcare."
>
> *- EMEA partner*

- **Higher renewal rates and increased customer stickiness.** With the recent spate of high-profile security breaches and the growing burden of regulatory compliance requirements, the Microsoft 365 Enterprise security features have given partners a massive opportunity to bolster their value propositions to customers and create customer stickiness. By complementing the Microsoft 365 Enterprise threat protection workloads (e.g., EMS, Advanced Threat Protection, Threat Intelligence, and Windows Defender ATP), information protection workloads (e.g., Azure Information Protection, cloud app security, Office 365 data loss prevention), and compliance solutions (e.g., Customer Lockbox, Advanced eDiscovery, and Advanced Data Governance) with deep security expertise, partners can expand their value propositions to customers, helping win renewals and future business.
- **Increased win rates on new Microsoft 365 customer opportunities.** Partners feel that security is a primary reason that customers move to Microsoft 365, making it one of the best entry points in discussions with existing customers and prospects. Partners note that GDPR regulations have created a greater sense of urgency among customers, helping partners win deals around security and Microsoft 365. By demonstrating security and compliance expertise, along with mastery over the Microsoft 365 security and compliance workloads for threat and information protection, partners can increase their likelihood of winning Microsoft 365 deals. For instance, one partner with significant GDPR consulting capabilities revealed that the new regulation could lead to 20% growth in its revenue.

> "Of all the Microsoft 365 value propositions, security and EMS are most important to customers."
>
> *- EMEA partner*

- **Upselling opportunities that increase customer lifetime value.** According to one partner, only 10% of its customer-installed base is currently using a Microsoft security offering, such as Advanced Threat Protection, Cloud App Security, or Azure Information Protection. Given this low adoption rate, partners have a massive opportunity to upsell existing customers to Microsoft 365 Enterprise E3 and E5 licenses, helping grow monthly recurring revenues.

For this study, Forrester included data from 17 interviewed Microsoft partners across North America, EMEA, and APAC. They ranged in size from a couple of dozen employees to hundreds of thousands of employees. Some partners were very specialized in particular workloads and others had practices covering all Microsoft 365 workloads and beyond, e.g. Azure. This study emphasizes partners with more mature security and compliance practices.

Security And Compliance Offerings Deliver Long-Term, Repeatable Revenue Opportunities

Microsoft partners interviewed for this study are growing their revenue and profitability by building a portfolio of security and compliance services and solutions that make their customers more secure and better prepared for

anytime, anywhere working. In building long-lasting, strategic relationships with key customers — both existing and new — partners are actively investing in new consulting frameworks, managed service offerings, and value-added IP that ensure their clients get the most out of their investment in Microsoft 365 Enterprise, and that their systems and users are always secure and up-to-date.

For the solution areas and revenue and profit streams below, Forrester has included proof points from the interviewed partners. Readers should apply the solution areas that are most relevant to their organization.

Our interviews identified significant variance and maturity levels across each partner's security and compliance solution portfolio. The table below shows the breakdown of the types of security and compliance services and solutions offered by partners, from "good" practice offerings to "best-in-class" offerings provided by Microsoft's most advanced and mature partners.

Microsoft 365 Security And Compliance Practices: Good, Better, And Best

Good	Better	Best
Licensing • Microsoft 365 licenses and E5 upgrades	**Pull-through project services** • Security policy implementation services • Governance, risk, compliance, and GDPR assessments and consulting services	**Managed services** • Security monitoring, alerting, and remediation services using Microsoft Security Graph API • EMS and AD user onboarding and management • Cloud application security
Project services • Secure Score and enterprise security assessments • Cloud security policy development and technology road map • Microsoft 365 pilots and deployment project services	**Managed services** • Server security monitoring and backup services	**Repeatable IP** • Data inventorying, mapping, and governance solutions • SharePoint online user and AD synchronization

Direct Project Revenues

Microsoft partners offer a variety of security consulting offerings aimed at understanding each customer's existing security solutions and policies, and assessing and remediating any security vulnerabilities, policy and governance deficiencies, and technology gaps in each customer's environment. These professional services lay the foundation for pilot and full deployment engagements around the Microsoft 365 security and compliance workloads and solutions.

Given the volume and diversity of security and compliance solutions across Microsoft 365, some partners specialize in a particular vertical, e.g., healthcare, or Microsoft 365 solution area, e.g., compliance and eDiscovery. Others are building broader, more comprehensive practices, offering both professional and managed services to solve business leaders' critical security and compliance challenges across virtually all verticals. Notably, the implementation of Microsoft's identity and access management solutions, including Azure Active Directory (AD), Windows Hello, conditional access, and Windows credential guard, is often done at the beginning of the customer journey and is seen by partners as the foundation for future security and cloud transformation project work.

> "Security is 80% of the reason why customers are moving to Microsoft 365. They now realize that the cloud is more mature."
>
> *- EMEA partner*

A typical customer journey and engagement model around Microsoft 365 security and compliance solutions during this phase consists of:

- Secure Score assessment.
- Cloud security policy development and technology road map.
- Microsoft 365 security pilot.
- Microsoft 365 identity and access management and threat protection implementation services.
- Information protection implementation services.

Gross margins for professional services during this phase of the customer journey typically range from 40% to 45%. Some partners revealed that their margins have grown over time, as larger portions of their consulting project mix transitioned toward higher-margin business and change management consulting.

- "We find that there are three major project phases. The first phase is diagnosis and strategy development. We then move into some program of process and solution redesign. That is followed with technology implementation."
- "We look at a customer's existing security environment and then create policies for cloud security. That costs about $100,000."
- "Our typical starting point is around identity, including moving Active Directory to the cloud. We also implement EMS as part of a foundation project to move to the cloud."
- "An initial threat protection project costs around €100,000. Information protection costs €10,000 with €30,000 in pull-through revenue."

Pull-Through Project Revenues

Microsoft partners with more mature security practices often help their customers build multiyear security visions and road maps as part of the initial project work, positioning themselves as their customers' trusted security partners. Subsequent security consulting project work, or pull-through projects, builds upon the initial assessment and the strategy and deployment work. It includes data governance, GDPR, and enterprise security policy and process design and implementation services. These pull-through engagements not only provide partners with the ability to more deeply engage with customers on critical security and compliance themes; they also bring in additional consulting revenues that are, on average, approximately two times the initial consulting revenue. For some partners, pull-through revenues could be much larger.

> "Our security offerings cover the complete Microsoft 365 Modern Workplace platform. That translates to years of work."
>
> *- EMEA partner*

The pull-through project revenues included in a typical three-year project life cycle consist of:

- Ongoing security policy implementation services over the three years.
- Governance and change management consulting.
- Risk identification, remediation, and mitigation efforts.
- Data inventorying, protection, and security compliance (especially around GDPR for organizations that do business in Europe).
- Gross margins that are similar to direct project products, ranging from 40% to 45%.

Interviewed partners shared the following:

- "Customers often take more on than they can handle, and things fall by the wayside, or they just don't have the right skills. That means they regularly bring us back in on remediation engagements."
- "We hear security concerns from existing customers, and that translates into new project opportunities."

> "A lot of our customers are moving to the cloud not just for cost savings, but for security reasons. So, we are working with both the CISO and CIO to modernize our customers' infrastructure to support their security objectives."
>
> *- NA partner*

- "We have a road map of work around specific security and compliance requirements. NEN 7150 is a big one for us."
- "GDPR is helping accelerate our customers' investments in other areas, including Microsoft Azure."

Managed Services

Interviewed partners consistently identified driving adoption of managed services as a top business priority. Managed services bring partners predictable and sticky recurring revenue streams that improve the accuracy of long-term budgeting, forecasting, and planning, while increasing company value in instances in which selling to another consulting company is desirable. Understandably, partners are keenly interested in shifting their business mixes to include more monthly recurring revenue (MRR), generated through the introduction of myriad managed services and other offerings that ensure their customers remain secure and compliant in a rapidly evolving threat and regulatory landscape.

Managed service offerings vary greatly in terms of service configuration, pricing models, service-level agreements (SLAs), and contract periods. Some managed services are priced on a per-user or -server basis, while other partners offer services at a flat fee with annual contracts. Partners also offer a variety of service tiers to customers, with actual service pricing varying with technical and end user support requirements, hours of availability, and SLA response times.

Forrester examined the security- and compliance-focused managed service offerings delivered by partners of different practice maturity levels. Our analysis found that the least mature security partners (i.e., "good") did not have meaningful managed services at the time of interview. More mature, or "better," practices offer some basic managed service offerings focused on "keeping the lights on," while the most mature, best-in-class security partners manage a large proportion of infrastructure and user security work that used to be driven primarily in-house. Microsoft's most advanced partners are rolling out managed service offerings that include attack simulators as part of their regular penetration testing solutions. Notably, there is an especially large security business opportunity with customers that are rolling out Microsoft 365 to their firstline workers, given the high volume of new users and the complexity of securing and managing these users for internal IT organizations.

> "There is that skill shortage that results in more clients seeking outside help . . . as a managed service where we can actually run security for them."
>
> *- Global partner*

Although attach rates for managed services are typically around 20% today, partners are employing a number of pricing, packaging, and marketing strategies to grow these to 30% or above over the next couple of years as their offerings mature, and partners get better at communicating the business value of their service offering to end customers. From a service profitability standpoint, partners indicate that service gross margins are currently around 35%, which are partially constrained by limited current customer demand for ongoing security managed services. To bolster their managed service margins, partners are developing their own intellectual property (IP) to power and automate the delivery of their managed services and support for their Microsoft 365 customers, which is expected to lead to higher margins, along with the ability to service more customers without a commensurate increase in headcount.

> "There's going to be a lot of interest in efficient long-term managed services. Companies don't want to hire 20 privacy people when they can outsource this to a provider who can take care of data protection and vulnerability monitoring, management, and response."
>
> *- NA partner*

Here are some quotes demonstrating the diverse Microsoft 365 security and compliance managed services that partners are currently offering:

- "Advanced Threat Protection is a gateway drug to the next-level EMS solution."
- "Security managed services attach super high because customers don't know how to use these new tools."
- "We do outsourced server management for $179 to $279 per server, per month. Managing the backups is another $40 to $50 per month on top of that."
- "We sell end user monitoring, alerting, and updating for $20 per user per month."
- "Azure AD managed services are $3 per month."

› “EMS managed services sells for $240 per user on an annual contract.”

Microsoft 365 CSP Channel Margin

Due to the enhanced security solutions included in the Microsoft 365 Enterprise E5 license, partners see a very large upsell opportunity for users currently on E1 and E3 licenses. This represents a large revenue opportunity for Cloud Solution Provider (CSP) partners and others who are entitled to channel margin and rebates from Microsoft. One partner said, “We are selling a lot more E5 licenses, because ATP [Advanced Threat Protection] is an easy upsell, especially for customers with large firstline workforces.”

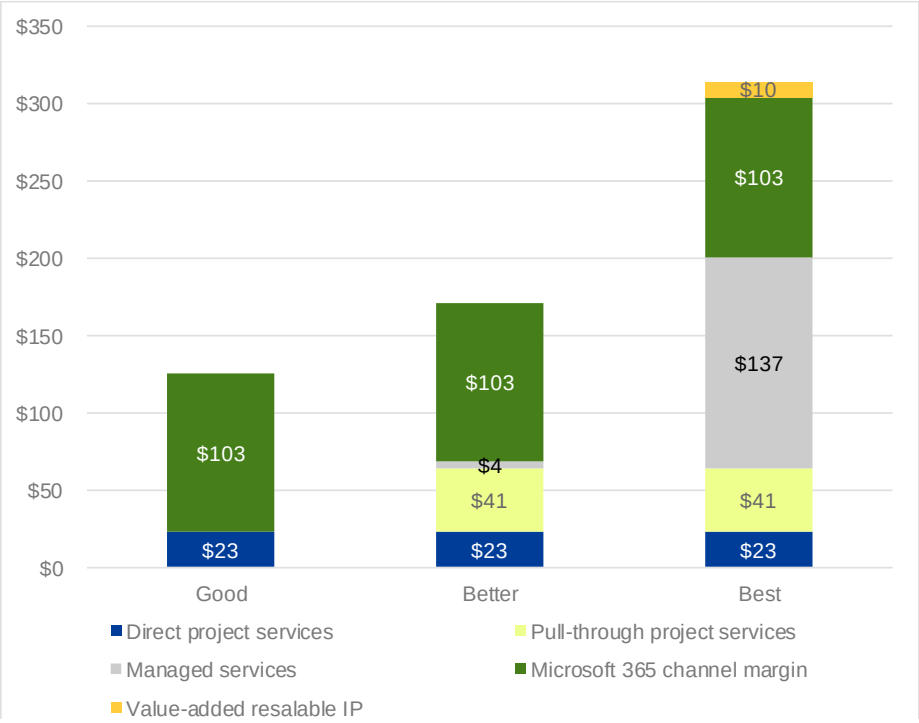
Typically, Microsoft pays 12% of license revenues to CSP partners, but this can be even higher when Microsoft offers promotions and rebates. Some of the income from license sales is intended to be reinvested in driving user adoption of the capabilities enabled through existing user licenses, with partners using some of these funds to host lunch-and-learn sessions, do assessment workshops, create training materials, etc. After these expenses, margins on the license revenue share are typically 80%.

Value-Added Resalable IP

Most partners interviewed for this study are actively building proprietary software and solutions and packaged resalable intellectual property to complement and augment existing Microsoft 365 security workloads and solutions, and to provide cross-vendor solution security. An example of an existing offering is an end user information access and monitoring tool for Microsoft solutions, such as OneDrive and SharePoint, and collaboration solutions from other vendors, to help organizations more quickly spot and address possible end user security breaches. One independent software vendor (ISV) is in the process of building a proof-of-concept for a holistic security operation solution integrated with Microsoft Intelligent Security Graph (ISG), to enable security teams to capture, enrich, and validate security alerts from Azure with the logs from its own product. This ISV expects sales growth and better customer stickiness from its ISG enabled solution, indicating that the combined offering will help customers better automate security enforcement and cyber-attack prevention.

Other partners offered security IP including a “SharePoint and Azure AD sync” solution, “data inventorying and mapping,” and “cross-vendor end user security monitoring.” As mentioned earlier, partners are developing other forms of IP to drive down managed service delivery costs and to increase managed service margins.

Three-Year Per-User Gross Profit Opportunity Based On Composite 5,000-User Deal By Partner Maturity



FORRESTER®

Security And Compliance Practice Investment Requirements

Partners interviewed for the study varied in terms of their existing security and compliance practices capabilities and talent resources. Partners with less mature security and compliance practices and capabilities often grew headcount to support their new practice areas, particularly around GDPR. For instance, one European partner with approximately 100 consultants revealed that it is adding 10 new hires to a recently developed GDPR consulting team. Several partners are investing in practice leads to drive business development for their security and compliance solutions across target segments and regions, bringing average fully burdened annual salary costs of $185,000 per hire. Other partners with well-established security practices did not need to make large incremental investments in their practices. Notably, several partners are considering collaborating with other Microsoft partners and companies in order to deliver a broader, unified security and compliance offering and value proposition to their customers, which can minimize the required investment needed to deliver these new solutions to their customers.

All partners Forrester interviewed make significant ongoing investments in training, with typical investments ranging from a few thousand to hundreds of thousands of dollars annually. Training funds are used to achieve various Microsoft certifications and to build subject matter expertise in high-demand security and compliance domains. Partners noted that hiring security consultants with the needed existing skill sets was difficult and expensive, making training of existing resources the preferred investment mode.

Partners that built out proprietary IP and managed service offerings made significant investments to build, maintain, market, and sell these offerings. Research and development, staff and sales training, and go-to-market expenses to develop these proprietary products and services ranged from a few hundred thousand dollars to build a minimum viable product, to several million to build and maintain more mature resalable IP and ISV offerings. A couple of partners set up separate companies to own these solutions and invoice for them separately.

Most partners said that security and compliance marketing spend would be reallocated from their existing marketing budgets, while others projected increased marketing spend in areas such as digital, events, thought leadership, and sales enablement. For those requiring incremental marketing expenditures, Forrester benchmarks additional marketing spend to be approximately 5% of gross security and compliance sales.

A Financial Example: Good, Better, And Best Partner Practices And Solutions

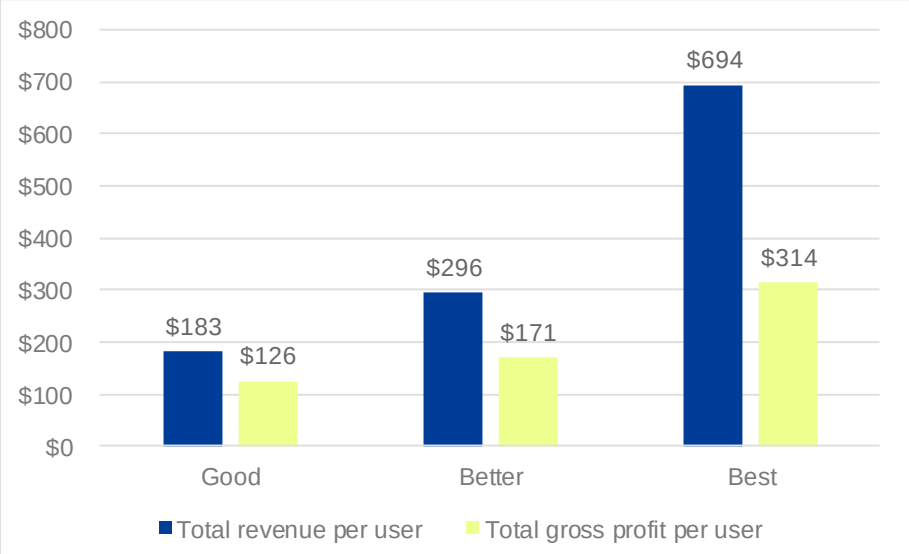
This study outlines the various revenue and profit streams that Microsoft partners may realize from building security and compliance practices around Microsoft 365. To more clearly illustrate this, Forrester built out a simple model that depicts the security- and compliance-specific revenue opportunities for a 5,000-user customer that adopts Microsoft 365. This economic model is built on the following assumptions:

- The economic model is based on a single deal with 5,000 user adopters and a two-year managed services contract. The model assumes 2% customer churn in Year 3 of the analysis, consistent with what we learned from interviewees.
- Direct project services calculated in this economic model include the following Year 1 engagements: $20,000 Secure Score assessment; $100,000 cloud security policy and technology road map; $25,000 Microsoft 365 security pilot; $100,000 in Microsoft 365 identity and threat protection implementation services; and $25,000 in information protection implementation services. Forrester notes that engagement revenue will vary significantly across industries and organizational sizes. Gross margins used in this financial example are 45%.
- Pull-through project revenues totaled $508,000 per deal over three years. This included ongoing security policy implementation services, governance model creation and coaching, risk and compliance assessments, and consulting around GDPR. Gross margins used in this financial example are 45%.

- For the “better” and “best” case partner scenarios, our model incorporates several managed services offerings. Managed services included in the “better” partner scenario include cloud server and technology security management, which assume attach rates ranging from 20% to 30% over the three-year analysis, and per-server monthly revenues of $219. The “best” case partner scenario includes a wide range of end user and internal security services, including cloud server security monitoring and backup ($219/server/month), end user security monitoring, alerting and updating ($20/user/month), EMS and Azure AD sync and support ($3/user/month), and outsourced EMS management ($20/user). Gross margins used in this financial example grow from 35% in Year 1 to 41% in Year 3 of the analysis due to ongoing partner investments in service delivery automation.
- CSP channel revenue is 12% of the license costs paid to Microsoft and heavily focused on the E5 upsell opportunity. Microsoft may offer, from time to time, promotional “kickers,” which could increase the revenue share percentage. For Microsoft 365 channel revenue, Forrester assumed an 80% gross margin, since some of these monies are intended to go back into activities that increase user adoption, as mentioned earlier in the section titled Microsoft 365 CSP Channel Margin.

The resulting combined gross margins across the revenue streams shown above is over 45% as higher-margin revenue streams from managed services and channel revenue increase. Taken all together, the security and compliance business opportunity around Microsoft 365 for partners can help organizations increase total sales, strengthen relationships with new and existing customers, and create predictable, recurring revenue streams.

Three-Year Revenue And Profit Opportunity Based On Composite 5,000-User Deal Across Practice Categories



Disclosures

The reader should be aware of the following:

- The study is commissioned by Microsoft and delivered by Forrester Consulting. It is not meant to be a competitive analysis.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in building a Microsoft 365 Security and Compliance practice.
- Microsoft reviewed and provided feedback to Forrester. Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning.
- Microsoft provided the partner names for the interviews.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. https://go.forrester.com/consulting/

ABOUT TEI

Total Economic Impact™ (TEI) is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders. The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility. https://go.forrester.com/consulting/content-marketing-consulting/