HfS Research Blueprint Report

Managed Security Services

Excerpt for Capgemini

March 2017

Christine Ferrusi Ross
Research Vice President
christine.ferrusi.ross@hfsresearch.com
@ferrusi

Table of Contents

TOPIC	PAGE
Executive Summary	3
How Customer-Centric, Digital Business Is Transforming Security	8
Research Methodology	19
Service Provider Grid	25
Service Provider Profile	29
Buyer and Provider Recommendations	33
About the Author	39

Executive Summary

Introducing the Managed Security Services Blueprint

- The ***2017 Managed Security Services HfS Blueprint*** is the second Blueprint Report to cover the Digital Trust and Security market. This report focuses on Managed Security Services (MSS) – those delivered on an ongoing basis to help clients prevent, monitor, report, and remediate threats to their businesses. To read the original report, see the October 2015 Trust-As-a-Service Blueprint.

- This Blueprint Report highlights MSS as the backbone of digital trust, enabling companies to move to the Digital OneOffice™. The Digital OneOffice describes the design and implementation of the digital customer experience and the creation of an intelligent, single office to execute and support it. (See the January 2017 POV for more details on Digital OneOffice.) Digital trust is the concept of ensuring that security is woven through all business operations so customers and other third parties trust you as a viable business partner

- The HfS Blueprint identifies relevant differentials between Managed Security Services providers across two main categories: innovation and execution. Execution excellence is non-negotiable as clients rely on the provider to monitor, detect, and remediate incidents and threats. Innovation in security is particularly relevant as new threats and threat actors appear daily and clients' security postures are constantly changing.

- In addition to looking at service offerings and capabilities, we looked at new ways to price engagements and the move to outcome-based models. We believe these pricing changes are indicators of shifts toward business-based and customer-experience-enhancing security.

Managed Security Services Value Chain

Strategy, Architecture, and Infrastructure	Risk and Threat and Prevention	Risk and Threat Monitoring	Incident Detection and Reporting	Remediation
• Security posture needs assessment and execution • Application and infrastructure security implementation and integration • Support for board-level security discussions	• Threat intelligence • Application and infrastructure testing for security issues • Process change to embed security in business operations	• Ongoing monitoring of systems and logs, including updates based on changing security posture • Analytics for trends, patterns, and behaviors	• Reporting and analysis of detected incidents and threats • Support for board-level discussions of detected incidents	• Recommendations and actions to address threats and incidents • Recommendations for ways to enhance response in the future

SERVICE-ENABLING TECHNOLOGIES

Digitization and Robotic Automation • Analytics • Mobility • Social Media • Cognitive Computing • Artificial Intelligence

SECURITY TECHNOLOGIES AND PLATFORMS

Firewalls • Endpoint Protection • Network Monitoring • Intrusion Detection • Application Security • Device Security • Data Protection • Identity and Access Management • Mobile Security • Threat Intelligence • Predictive Analytics • Antivirus • Log Management

Note: HfS' value chain of work follows a process flow of activities, but this isn't necessarily the way clients buy services. Clients often ask for specific point solutions like identity management. But within that offering, the workflow often still follows the value chain process above. See the security services grid for a specific list of specific services we included as part of managed services.

Key Highlights: The State of Managed Security Services

- **Risks, specific threats, and the number of threat actors are all increasing – both in number and impact.** Companies are looking for managed services firms to help them prevent, monitor, and remediate current threats. But companies also expect that their providers will evolve the services over time to ensure that new threats don't go undetected.

- **Analytics are non-negotiable components of security services today; predictive analytics will be non-negotiable tomorrow.** Every provider we evaluated discussed the importance of strong analytics to find and report incidents to clients. Many talked about their work in predictive analytics to help clients mitigate new risks and incidents that perhaps aren't found in traditional ways. Many challenges exist in proactive risk remediation (who wants to be the one who takes an action on a risk that hasn't happened yet?) But despite the challenges, predictive analytics are critical to keeping up with constantly changing security environments.

- **Industry expertise is moving beyond understanding of vertical-specific regulatory requirements and threats.** Security needs to be integrated into the business, not just support the business. And a key way for security services providers to help clients is to understand their business context better. Providers and clients now expect stronger industry knowledge to provide this business context. Tying security into business operations helps move into a value-creation role and to drive improved customer experiences.

- **Talent wars complicate the security landscape.** Like many complex technical spaces, the security area faces a talent shortage. We found that most providers are following standard recruiting and retention best practices. But some of the leading-edge firms show more creative approaches to ensure they have enough talent to serve clients and mitigate the cannibalism that happens in security services talent pools.

Key Highlights: Managed Security Services Providers

- The Winner's Circle reflects an ability to execute well on a broad set of capabilities while focusing on emerging issues like predictive analytics and crafting differentiated thought leadership in the market.

  The ranking reflects an analysis of Innovation and Execution in managed security, where we placed extra value on offerings and delivery that demonstrated understanding of how security fits into broader business context, proactively stayed current with changing security threats, and had a vision for security's role in the customer experience.

  - **Winner's Circle:** Providers that rose to the top: Accenture, Capgemini, Cognizant, EY, IBM, Infosys, Unisys, and Wipro
  - **High Performers:** Providers driving the core of the market: CSS Corp, Luxoft, SecureWorks, and Tech Mahindra
  - **Execution Powerhouses:** Providers bringing proven value to their clients: TCS

- All of the providers covered in this Blueprint provide a very high level of Security Services, and it's important to evaluate against your individual needs. The scoring differences among the providers was often small.

AS-A-SERVICE ECONOMY

Use of operating models, enabling technologies and talent to drive business outcomes through outsourcing. The focus is on what matters to the end consumer.

HfS uses the word "economy" to describe the next phase of outsourcing as a new way of engaging and managing resources to deliver services.

The 8 Ideals of the As-a-Service Economy:

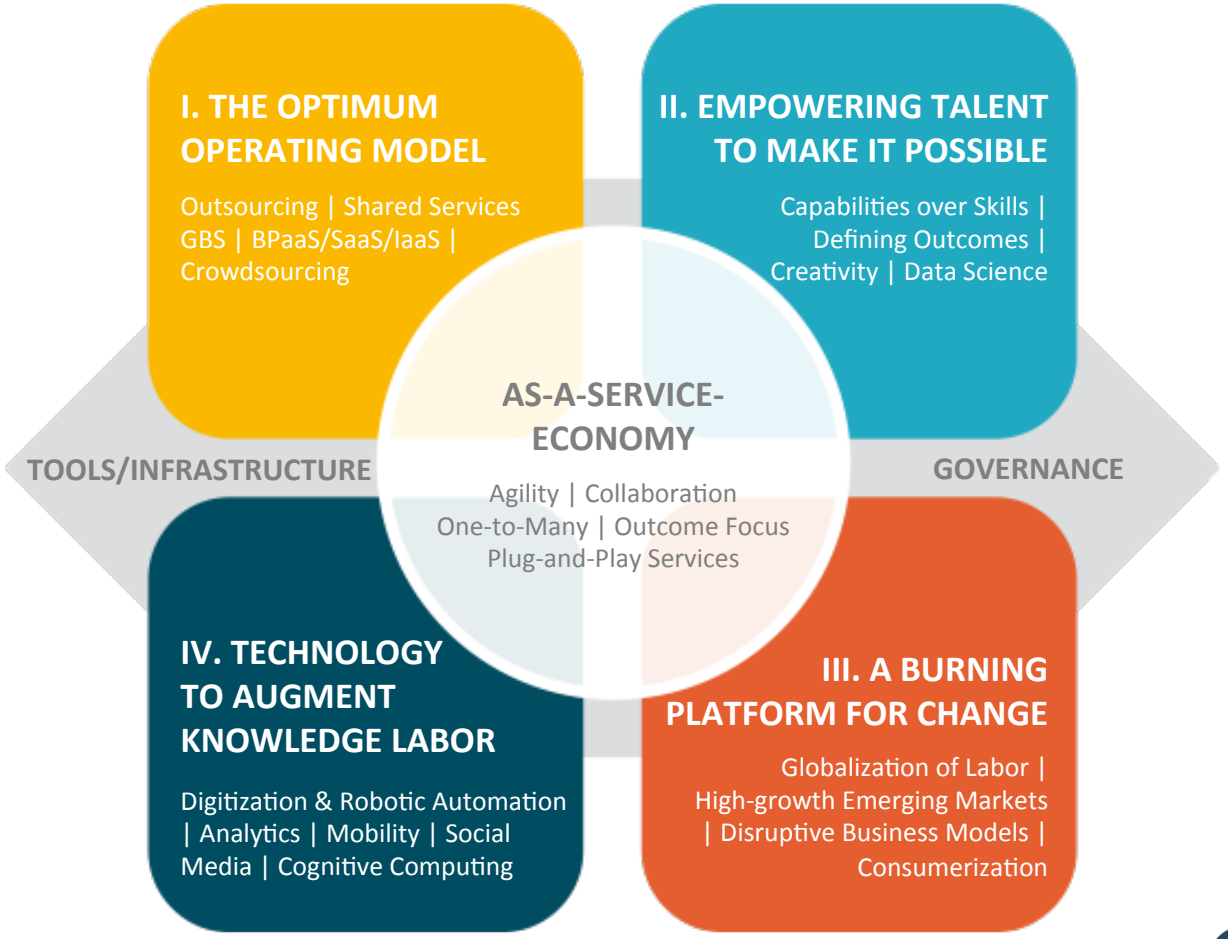
1. Write Off Legacy
2. Design Thinking
3. Collaborative Engagement
4. Brokers of Capability
5. Intelligent Automation
6. Accessible and Actionable Data
7. Holistic Security
8. Plug-and-Play Digital Services

Source: Beware of the Smoke: Your Platform Is Burning by HfS Research, 2015

How Customer-Centric, Digital Business Is Transforming Security – and Vice Versa

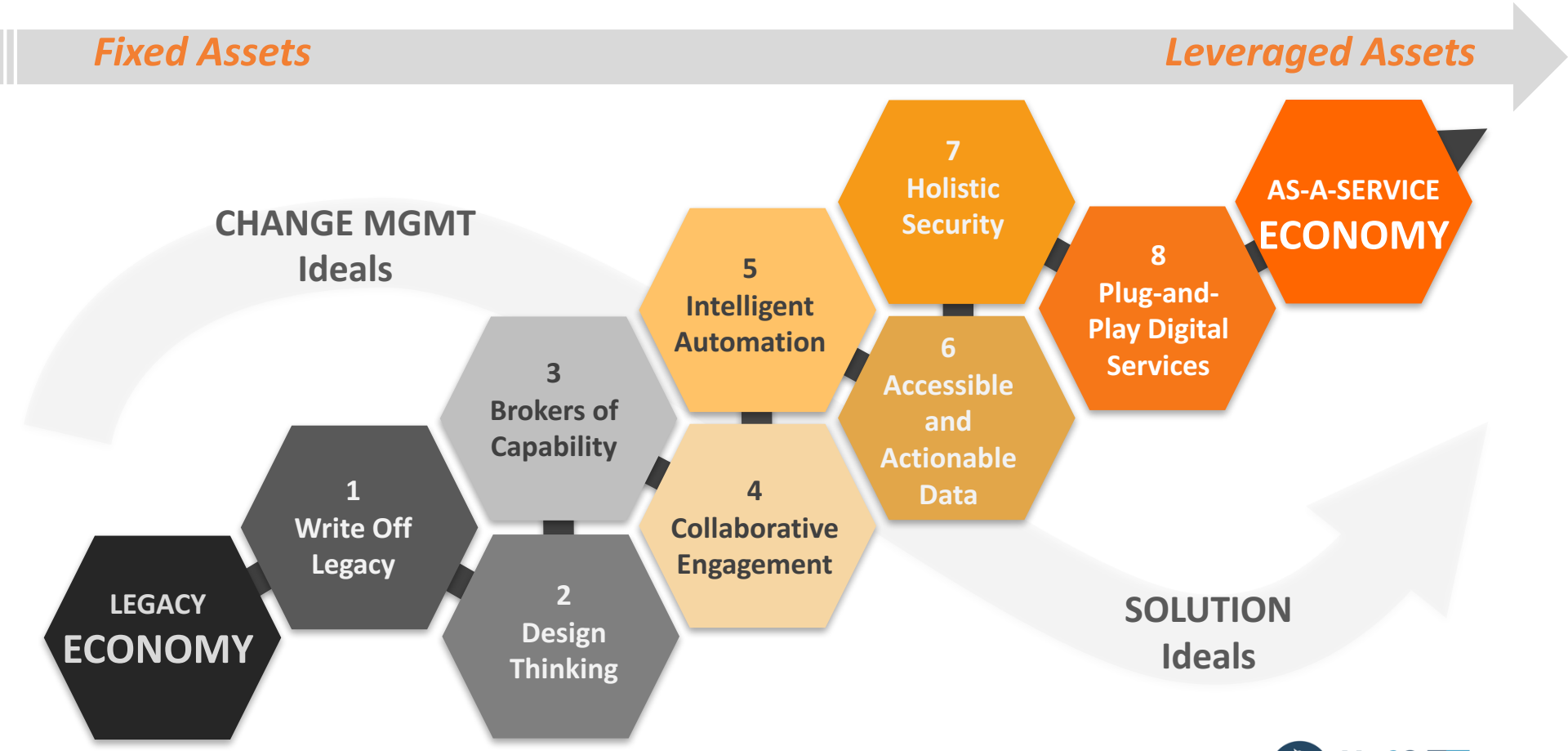
The As-a-Service Economy Sharpened Business Focus on the Customer

Operating in the As-a-Service Economy means architecting use of increasingly mature operating models, enabling technologies and talent to drive targeted business outcomes. **The focus is on value to the consumer.**



Operating in the As-a-Service Economy Requires Adoption of 8 Ideals

- Moving into the As-a-Service Economy means **changing the nature and focus of engagement** among enterprise buyers, service providers, and advisors
- "As-a-Service" unleashes people talent to drive new value through smarter technology and automation



The 8 Ideals Affect What Firms Need From Security

IDEAL	DEFINITION	SECURITY IMPACT
Write Off Legacy	Using platform-based solutions, DevOps, and API ecosystems for more agile, less exception-oriented systems	As companies write off legacy, there are security implications for removal and reuse of old equipment, plus new vulnerabilities brought into the environment with new applications and systems. The impact on security operations is more pressure to know about all of the new technologies in order to effectively mitigate vulnerabilities.
Design Thinking	Understanding the business context to reimagine processes aligned with meeting client needs	To strategically protect the business as it changes and grows, organizations will see more design thinking in security environments. This includes doing workshops to understand potential new threat actors and the culture, process, and technology changes needed to protect the business from new threats.
Brokers of Capability	Orienting governance to source expertise from all available sources, both internally and externally, to address capability gaps	Digital trust is the key for brokers – companies work with outsourcers and providers they trust. Addressing the ability to protect data is a shared responsibility among trading partners and outsourcers in multiparty engagements.
Collaborative Engagement	Ensuring relationships are contracted to drive sustained expertise and defined outcomes	Trading partners need to trust each other's ability to protect their data and intellectual property in outcomes and transactions. Security then enables business growth.
Intelligent Automation	Using automation and cognitive computing to blend analytics, talent, and technology	The number of threats and threat actors – plus the strain on security talent – makes automation a requirement. And protecting automated systems is the difference between success and failure.
Accessible and Actionable Data	Applying analytics models, techniques, and insights from big data in real-time	Analytics helps security get better, but security teams also need to protect analytics in other functions to make sure algorithms and data aren't hacked to create false results and cause business chaos.
Holistic Security	Proactively managing digital data across the service chain of people, systems, and processes	Security can't be a silo, relegated to a small set of specialists in the corporate data center. Instead, security needs to be incorporated across the entire enterprise and understood by business stakeholders at all levels.
Plug and Play Digital Business Services	Plugging into "ready to go" business-outcome-focused people, process, and technology solutions with security measures	The speed of business means companies want to connect to each other quickly – and that requires that they trust the players they're connecting to. So security needs to be embedded in all offerings to allow transactions to happen quickly, reducing the friction that comes when parties have to slow down to evaluate security procedures.

Traditional Security Needs to Adapt to Support the 8 Ideals

Moving to the As-a-Service economy and Digital OneOffice™ requires firms to adopt holistic security that's integrated with business operations. Organizations need to shift their thinking in a few key areas:

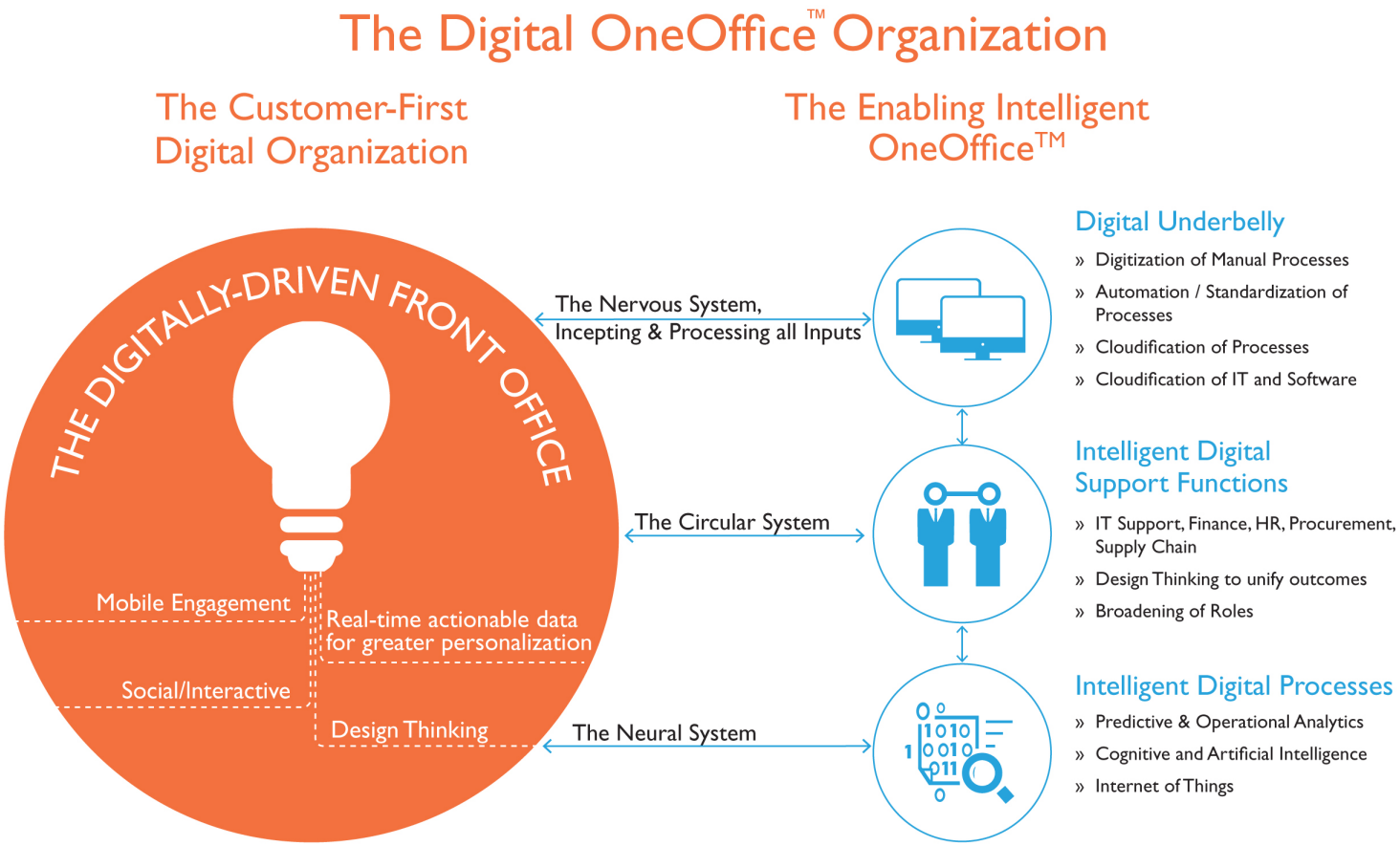
- **Stop treating security as a standalone capability and integrate into business processes.** Traditional security teams focus on security alone, assuming that highly efficient security by default will protect the business and add value. However, the move to Digital OneOffice changes that mindset. The providers and clients we spoke with for this report agreed that security needed to understand the business, so security can become part of the business instead of an afterthought. Leading-edge organizations think about security in the context of which assets are most critical to the business and which risks have the greatest impact. Then they educate stakeholders on security in this business context, gaining better adoption of best practices and support from all parts of the business.

- **Focus on behavior more than technology.** While client references wanted providers to have expertise in the specific technologies being used, they said to protect the business better, you need to focus on behaviors before technologies. The best firewall in the world can't stop a hacker from getting in through a password he got from phishing an employee, for example.

- **Resist being so comfortable in their operations that they miss changes in the market.** Of course, you should get value from existing investments. However, several client references noted that they want security operations teams to look outside their existing approaches. As one reference said, "If security teams just do their jobs every day by rote and never really think about what they're doing or why, we'll miss new threats and potentially hurt our business."

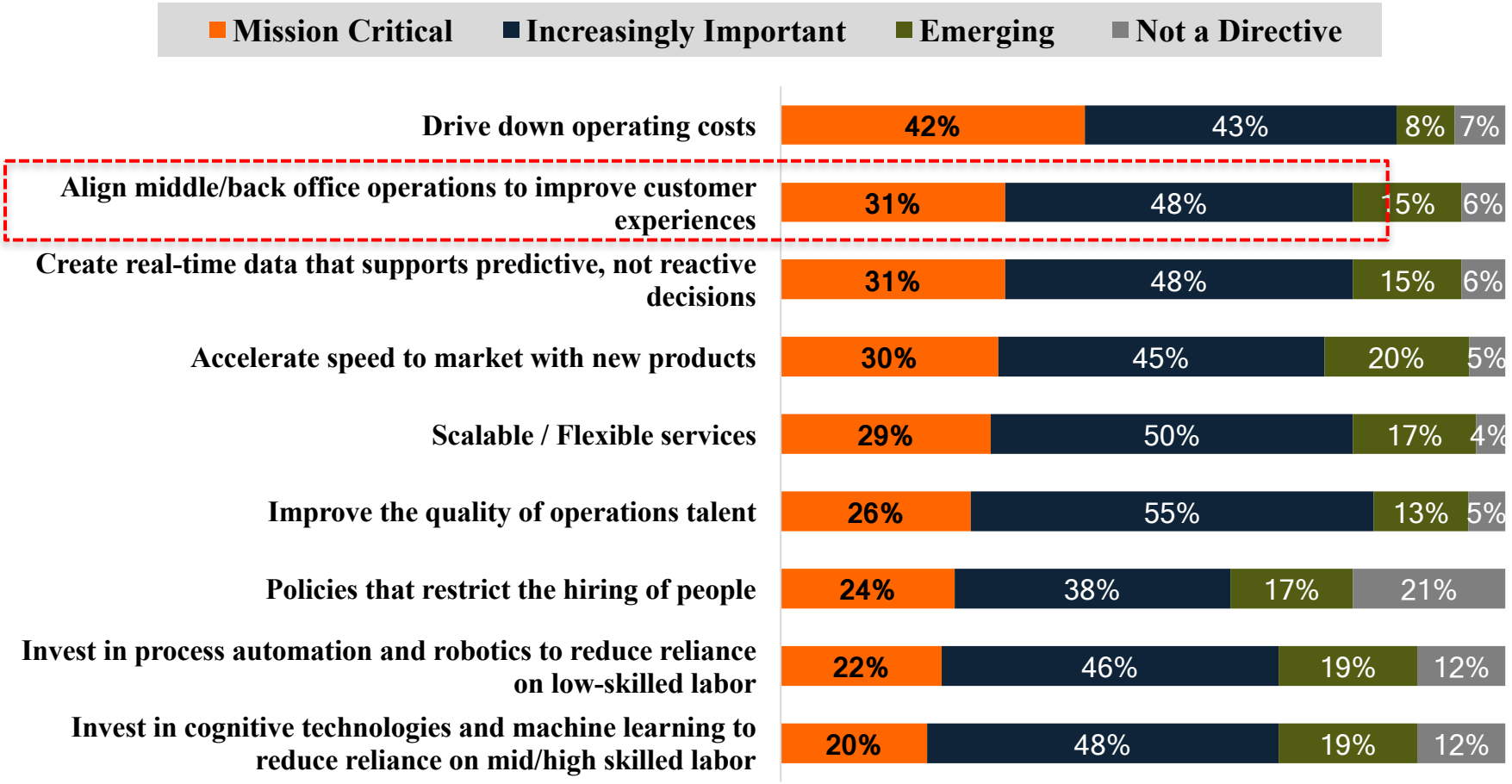
Digital OneOffice Is the Operating Model for the As-a-Service Economy

To effectively participate in the As-a-Service economy, organizations need to align their operations to support customers. This alignment means that distinctions between front-office and back-office processes go away. This pushes security out of its silo as a standalone discipline and embeds it in all processes in order to ensure the quality of the customer's experience.



Security Underpins the Alignment of All Operations to Improve Customer Experiences

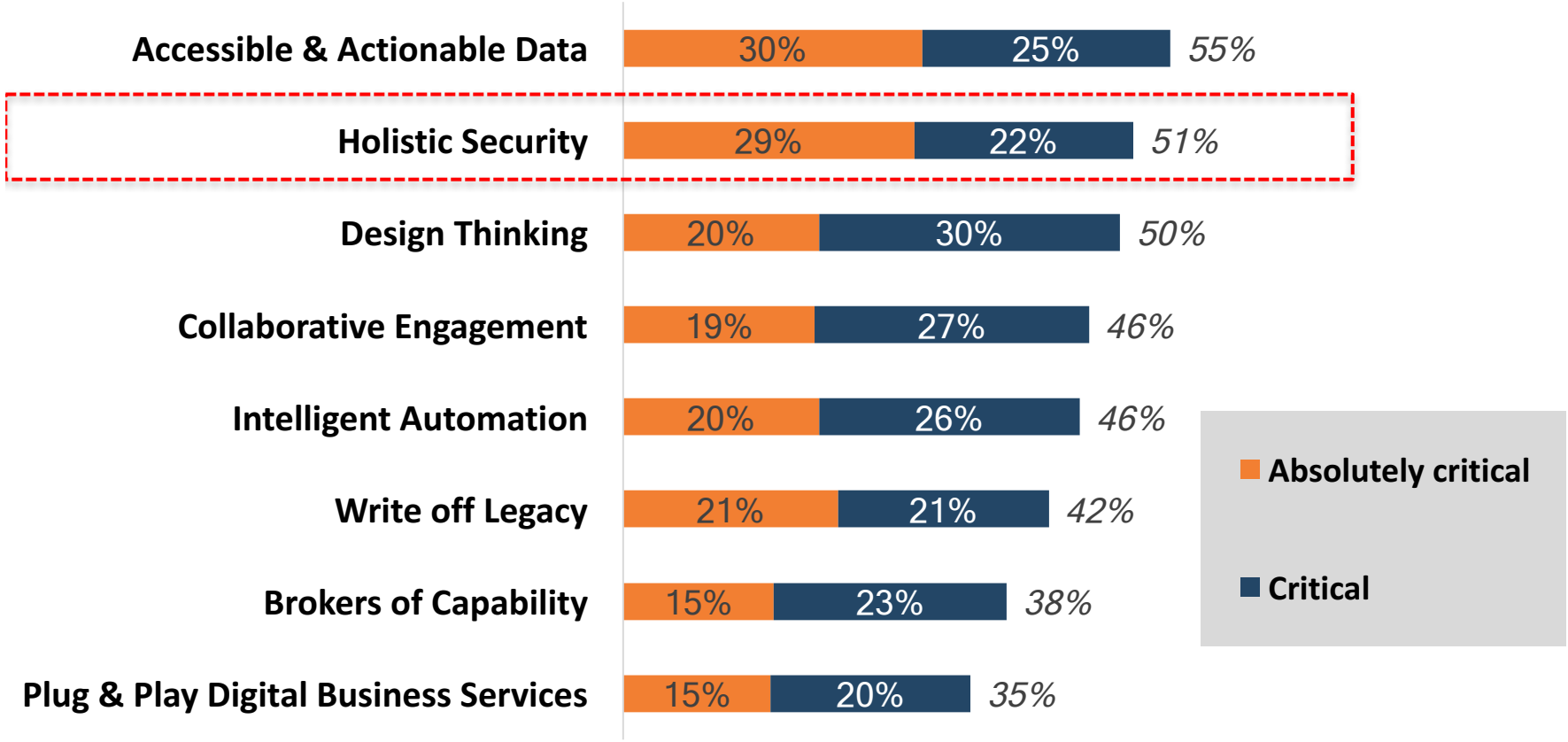
How critical are the following C-Suite directives to your operations strategy? (SVPs and above)



Source: HfS Research in Conjunction with KPMG, "State of Operations and Outsourcing 2017"
Sample: n=454 Enterprise Buyers

Business Executives Recognize Security's Importance in Their OneOffice Transformations

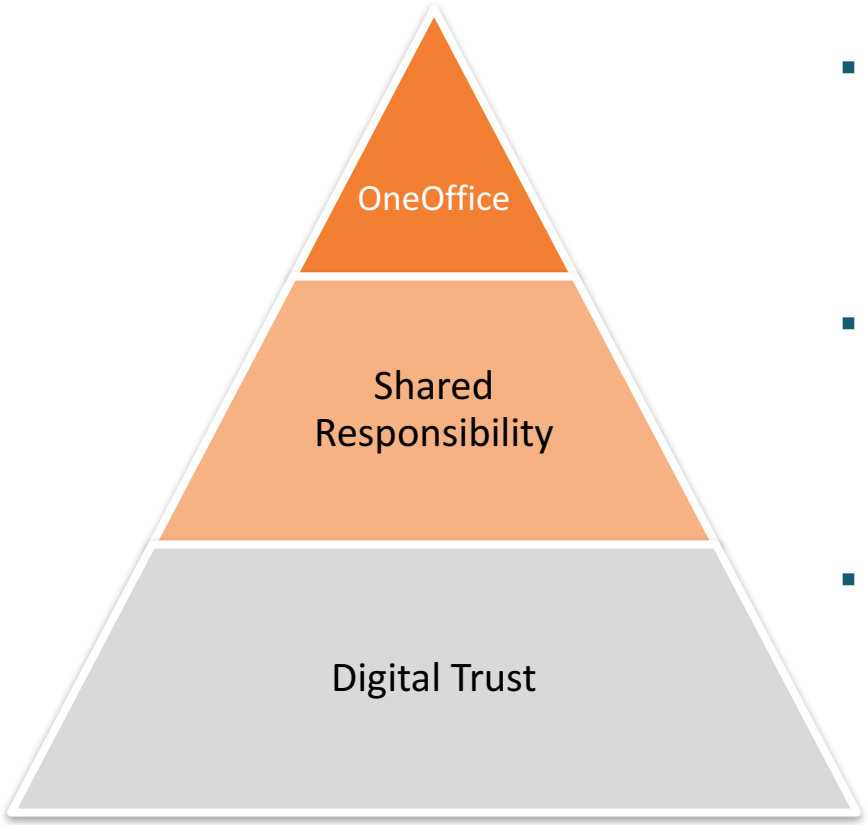
Please state how significant you see the "As-a-Service Economy" ideals and the shift to more intelligent operations for your organization? (Just absolutely critical / critical responses)



Source: "Intelligent Operations" Study, HfS Research 2017
Sample: Buyers = 371

How Security Improves Customer Experience in the OneOffice Operating Model

Businesses need to elevate security so customer-facing employees can help customers and other trading partners feel comfortable working with the firm. It then becomes part of the business strategy and a facilitator of differentiated customer experiences.



- **Ensuring OneOffice:** Digitization and the renewed rise of customer-centricity mean that the wall between the back office and front office has collapsed – everyone in a company is customer facing in this age where customers have significant visibility into our internal operations. That means your security policies, procedures, and risk approaches need to be brought up from the basement and shared across your entire organization.

- **Facilitating shared responsibility:** Security isn't just something you worry about within your four walls anymore. As data and IP get shared across trading partners, the need for a shared view on securing digital assets becomes critical. This means moving beyond "protect the perimeter" approach to a collaboration among partners to share best practices, insights, and metrics to create a shared responsibility for protecting data in transactions.

- **Creating digital trust:** Your ability to succeed in the digital environment requires that your trading partners (customers, suppliers, external stakeholders) trust you to be ethical, legally operating, and practicing up-to-date security procedures to protect their data and IP. If others start to doubt your ability to secure your own data or theirs, you are dead as a business. It's pretty simple as a concept and amazingly complex to execute. To be trusted, you need to demonstrate that your security operations are effective, automated, and current with evolving threats.

Managed Security Services Value Chain – The Process Needed to Support OneOffice

Strategy, Architecture, and Infrastructure	Risk and Threat and Prevention	Risk and Threat Monitoring	Incident Detection and Reporting	Remediation
• Security posture needs assessment and execution • Application and infrastructure security implementation and integration • Support for board-level security discussions	• Threat intelligence • Application and infrastructure testing for security issues • Process change to embed security in business operations	• Ongoing monitoring of systems and logs, including updates based on changing security posture • Analytics for trends, patterns, and behaviors	• Reporting and analysis of detected incidents and threats • Support for board-level discussions of detected incidents	• Recommendations and actions to address threats and incidents • Recommendations for ways to enhance response in the future

SERVICE-ENABLING TECHNOLOGIES

Digitization and Robotic Automation • Analytics • Mobility • Social Media • Cognitive Computing • Artificial Intelligence

SECURITY TECHNOLOGIES AND PLATFORMS

Firewalls • Endpoint Protection • Network Monitoring • Intrusion Detection • Application Security • Device Security • Data Protection • Identity and Access Management • Mobile Security • Threat Intelligence • Predictive Analytics • Antivirus • Log Management

Note: HfS' value chain of work follows a process flow of activities, but this isn't necessarily the way clients buy services. Clients often ask for specific point solutions, like identity management. But within that offering, the workflow often still follows the value chain process above. See the security services grid for a specific list of specific services we included as part of managed services.

Managed Security Services in the OneOffice Context

The move to OneOffice operations places a tremendous strain on security operations teams. The shift in strategy and daily operations will push many organizations to look for outside help. Clients will look for providers that can operate security effectively while putting security in a customer-centric context and helping internal security teams communicate better with the business. Some ways to identify leading-edge providers:

- **Mapping specific services into the bigger picture.** You aren't going to go out and ask for "OneOffice security" or "digital trust." You're more likely to ask a provider for threat intelligence services or application security services. However, focusing on those point solutions will suboptimize your efforts. Leading providers are bridging the gap by showing prospective clients how these point solutions fit into broader efforts and support overall security programs.
- **Demonstrated passion for learning and innovation.** Every provider says it's innovative and has approaches to stay current in dynamic environments. But we all know that once cost pressure hits and negotiations begin to drag, it's easy to let go of big picture ideals like innovation to focus on daily nitpicky details. Leading providers will be able to show you their change management processes, design thinking capabilities, and references from long-term clients that detail how the provider brings innovation and change into the engagement.
- **Commitment to business stakeholders.** Security is very technical, and smart providers can show you how they avoid the jargon and unnecessary details to tell a security story that senior executives will understand and value. Some very strategic providers can help you build an investment and return model that you'll be able to use to justify spend and gain credibility with business owners.

Research Methodology

Research Methodology

Data Summary

- Data was collected in Q4 2017 and Q1 2017, from buyers and service providers of Managed Security Services

Participating Service Providers

accenture
Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING
Cognizant
CSS CORP
EY
IBM
Infosys
LUXOFT
SecureWorks
TATA CONSULTANCY SERVICES
Tech Mahindra
UNISYS
WIPRO Applying Thought

This Report Is Based On:

- **Tales from the Trenches:** Interviews with buyers who have evaluated service providers and experienced their services. Some contacts were provided by service providers, and others were interviews conducted with HfS Executive Council members and participants in our extensive market research.
- **Sell-Side Executive Briefings:** Structured discussions with service providers regarding their vision, strategy, capability, and examples of innovation and execution.
- **Publicly Available Information:** Thought leadership, investor analyst materials, website information, presentations given by senior executives, industry events, etc.

HfS BLUEPRINT REPORTS

HfS Blueprint Scoring for Managed Security Services 2017

EXECUTION	100%
Scope of services across the value chain	25%
Depth and quality of services (including geographic coverage)	25%
Automation and analytics embedded in current engagements	20%
Pricing flexibility	10%
Client references (number given, number responding, satisfaction of respondents)	20%

INNOVATION	100%
Vision for security within the enterprise	20%
Industry expertise being used to add context and value beyond standards	20%
Predictive analytics and remediation	20%
Talent strategy	15%
Differentiated thought leadership	25%

Execution Definitions

EXECUTION	How well does the service provider execute on its contractual agreement, and how well does the provider manage the client/provider relationship?
Scope of services	Across the value chain of services we included in the evaluation, how many does the provider offer? (See the offerings grid in the provider profile section for specifics of each provider.)
Depth and quality of services (including geographic coverage)	How well does the provider deliver the services it offers? Does the provider have deep offerings delivered with high quality? Does the provider offer global capabilities in its offerings?
Automation and analytics embedded in current engagements	To what extent does the provider include automation as part of its service delivery? Are these capabilities embedded in engagements automatically, or must the client ask explicitly for them?
Pricing flexibility	Does the provider offer multiple engagement pricing models, such as fixed price, outcome-based, etc., based on client needs and scope/requirements?
Client references (number given, number responding, satisfaction of respondents)	How many client references did the provider offer? How responsive were those references? How many were we able to interview in the research cycle? How satisfied were the references with service delivery, account management, innovation, automation, and analytics, among other criteria?

Innovation Definitions

INNOVATION	Innovation is the combination of improving services and business outcomes.
Vision for security within the enterprise	Does the provider offer a vision for security's role within the enterprise that's compelling, shows business value, and demonstrates an understanding of issues facing clients' organizations?
Industry expertise being used to add context and value beyond standards	Does the provider demonstrate industry-specific understanding of security regulations and client security postures? Does the provider offer industry-based business insight and place security in the context of business impact based on industry knowledge?
Predictive analytics and remediation	What is the provider's strategy for incorporating predictive analytics into client engagements to help clients become more strategic about discovering and remediating threats? What investments is the provider making in predictive analytics?
Talent strategy	What is the provider doing to ensure it wins the war for talent? How is the provider adapting its training and development to bring in a wider pool of talent and retain high-value employees?
Differentiated thought leadership	How is the provider differentiating itself in the market? What intellectual property is the provider developing that sets it apart from other providers? What value does this thought leadership add to the security industry overall?

Maturity of OneOffice Vision Within Managed Security Services

In addition to the formal criteria we used during the evaluation, we also noted how mature we believe each provider's Managed Security Services map into the HfS vision for security in OneOffice operations. We rated providers as strong, medium, or weak on the three main dimensions.

Security for OneOffice Operations
OneOffice
Shared Responsibility
Digital Trust

Grading Scale

Strong	Medium	Weak

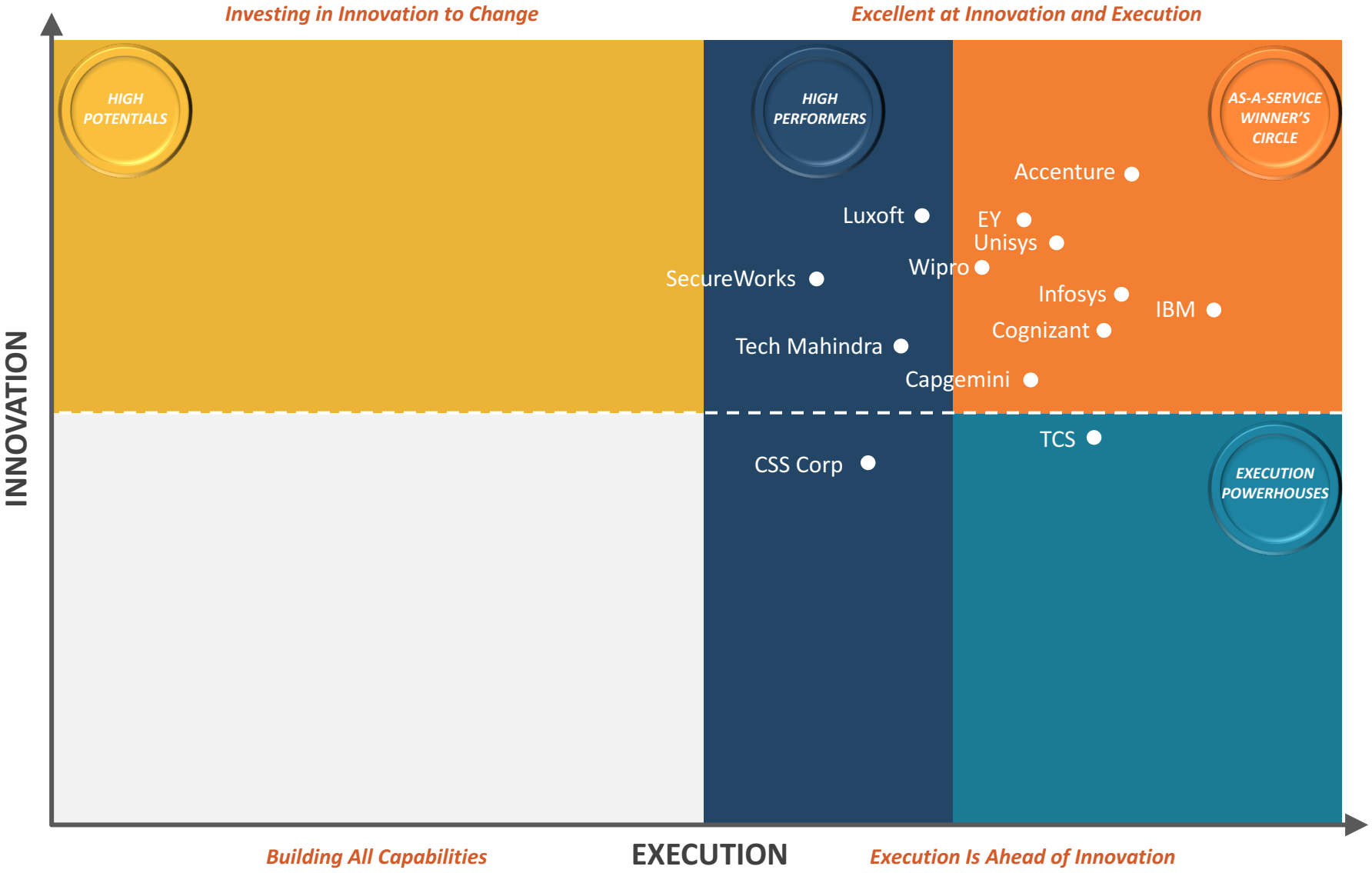
Service Provider Grid

Guide to the Blueprint Grid

To distinguish service providers that show competitive differentiation in a particular line of delivery with progress in realizing the As-a-Service Economy of business outcome–oriented, on-demand talent and technology services, HfS awards these providers the "As-a-Service Winner's Circle" designation.

	EXECUTION	INNOVATION
As-a-Service Winner's Circle show excellence recognized by clients in the 8 Ideals in execution and innovation	Collaborative relationships with clients, services executed with a combination of talent and technology as appropriate, and flexible arrangements.	Articulate vision and a "new way of thinking," have recognizable investments in future capabilities, strong client feedback, and are driving new insights and models.
High Performers demonstrate strong capabilities but lack an innovative vision or momentum in execution of the vision	Execute some of the following areas with excellence: worthwhile relationships with clients, services executed with "green lights," and flexibility when meeting clients' needs.	Typically, describe a vision and plans to invest in future capabilities and partnerships for As-a-Service, and illustrate an ability to leverage digital technologies and/or develop new insights with clients.
High Potentials demonstrate vision and strategy but have yet to gain momentum in execution of it	Early results and proof points from examples in new service areas or innovative service models, but lack scale, broad impact, and momentum in the capability under review.	Well-plotted strategy and thought leadership, showcased use of newer technologies and/or roadmap, and talent development plans.
Execution Powerhouses demonstrate solid, reliable execution but have yet to show significant innovation or vision	Evidence of operational excellence; however, still more of a directive engagement between a service provider and its clients.	Lack of evident vision and investment in future-oriented capability, such as skills development, "intelligent operations," or digital technologies.

HfS Blueprint Grid: Managed Security Services 2017



Major Service Provider Dynamics – Highlights

EXECUTION

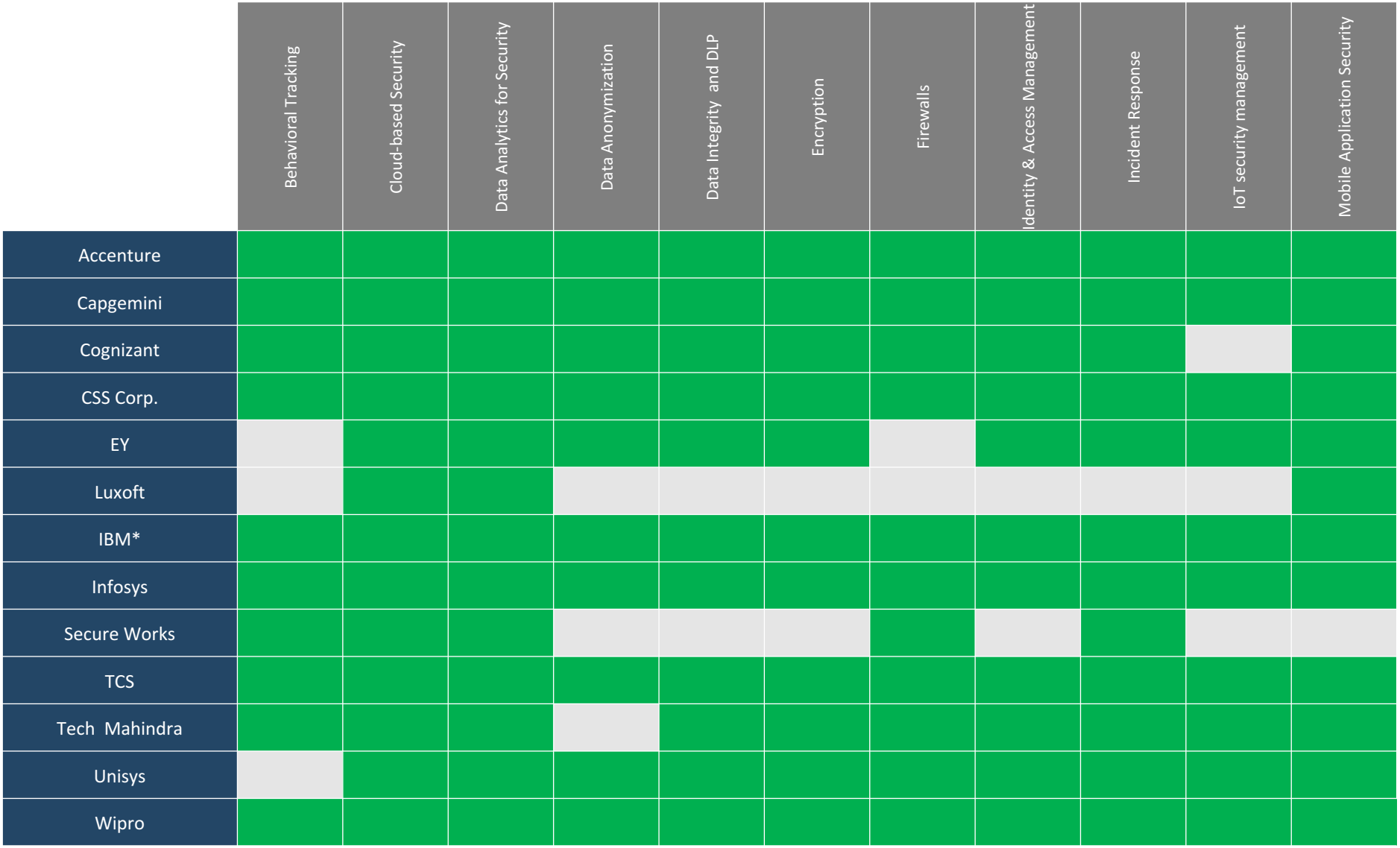
- **Scope of Services:** We evaluated 21 services (see the chart in the Service Provider Profiles section). **Accenture, Capgemini, Infosys, TCS,** and **Wipro** had the most complete portfolios. Physical security and virtual desktops were the two services more likely to be missing from provider offerings.
- **Depth and Quality of Services:** **Accenture, Unisys, Wipro,** and **Infosys** all demonstrated good references here. **Luxoft** also demonstrated good depth with client references in the provider's narrower portfolio.
- **Automation and Analytics Embedded in Current Engagements:** All providers offer data analytics as an offering, and our research shows it's critical to having a successful program. **SecureWorks'** Counterthreat platform is an example of analytics used in daily client engagements. **Cognizant** and **Infosys** also demonstrated strong investments. Automation, although less productized than analytics, also is showing up in engagements. **Tech Mahindra** and **CSS Corp** showed specific ways they are automating threat detection and quarantine techniques.
- **Pricing Flexibility:** **CCS Corp** and **Capgemini** offer tiered services options to fit multiple client needs and pricing structures. **Infosys** also offered a variety of pricing options, including fixed, outcome-based, and hybrid.
- **Client References:** **Luxoft's** client mentioned the provider's work being praised by external auditors. **Accenture** and **EY** were praised for their business acumen in addition to security.

INNOVATION

- **Vision for Security in the Enterprise:** **Unisys** explains security as tool to ensure a company's growth. **Luxoft** explicitly works with clients to show how security has an impact on clients' customers. These are ways providers help stakeholders understand the importance of security. Several providers also developed points of view on shared responsibilities among trading partners, typically described as expanding security beyond the perimeter.
- **Industry Expertise Being Used to Add Context and Value Beyond Standards:** **Accenture** has been focusing heavily on integrating a vertical-industry business story with its security practice to increase the relevance of its offerings. **Unisys** also developed industry points of view beyond industry-specific regulatory standards. **EY** also invests here.
- **Predictive Analytics and Remediation:** All of the providers are developing further predictive analytics capabilities, with **Accenture** and **SecureWorks** showing specific techniques that are already coming to fruition.
- **Talent Strategy:** Most providers have well-developed talent strategies, although **Unisys** did a good job of explaining that it also recruits with its vision of security's role in the world, not just on traditional hiring tactics.
- **Differentiated Thought Leadership:** **Wipro's** outline of a clear vision for security as a customer-experience component and **Accenture's** focus on data ethics as the next step in security best practices were particularly unique.

Service Provider Profile

Managed Security Services Offerings (green means offered)



* IBM did not participate in the blueprint research process. HfS used public information, insights from other provider references, and our own assessment of the firm's performance.

Managed Security Services Offerings, Continued (green means offered)

	Physical Security (Access Control, Geolocation Awareness)	Security Architecture & Planning	Security Tools Utilizing Autonomics & RPA	Security Tools Utilizing Cognitive/AI	Segmentation/Micro-segmentation	Threat/ Breach Detection	User Education/ Awareness Campaigns	Virtual Desktops	VPNs	Vulnerability Assessment
Accenture										
Capgemini										
Cognizant										
CSS Corp.										
EY										
Luxoft										
IBM*										
Infosys										
Secure Works										
TCS										
Tech Mahindra										
Unisys										
Wipro										

* IBM did not participate in the blueprint research process. HfS used public information, insights from other provider references, and our own assessment of the firm's performance.

Capgemini

As-a-Service Winner's Circle

Capgemini's multi-tiered SOC strategy is a differentiator in this market

Blueprint Leading Highlights
• Scope of services • Pricing flexibility

Alignment with OneOffice

- OneOffice
- Shared Responsibility
- Digital Trust

Strengths	Challenges
• **Integration of security into broader infrastructure services:** Capgemini has many security engagements embedded in larger contracts, allowing the firm to have broader visibility into potential threats and knowledge of potential preferred remediation steps. • **Security beyond the perimeter:** The provider's view of security is technical, with a strong understanding of how traditional approaches to "protect the perimeter" are less effective in connected environments. • **Productized multi-tiered SOC delivery and service models:** Capgemini has productized easy to understand Bronze-, Silver-, or Gold-tiered SOC models, dependent on clients' service requirements and budget.	• **Missing the broader business context (and client audience):** Capgemini tends to have its audience in IT security and at lower levels than the CIO or CISO. The company needs to move its messaging to a more business-oriented story to resonate more strongly with senior executives. • **Lack of unique business differentiator:** Capgemini's offering is solid; the company is in the Winner's Circle. But it lacks something unique or different enough in its business story compared to competitors. The firm needs to spend more time thinking about how its security offering fits into the bigger business picture and presenting a vision for security that prospective clients can distinguish from the other offerings available.

Relevant Acquisitions / Partnerships	Client Profile	Service Delivery Operations	Proprietary Technologies
Acquisitions: • Euriware (2014) **Partnerships:** • SIEM: IBM, Huntsman • APP: HPE • Database: Oracle, IBM • Encryption: Gemalto • Endpoint: TrendMicro • Firewall: Fortinet, Palo Alto • Vulnerability management: Nessus and Qualys • Malware analysis: FireEye • IAM: RSA, Forgerock and CyberArk • Cloud Access • Security Broker: Microsoft • SOC: RSA, IBM	More than 100 MSS clients, including: • Renault Group • Alstom link • Areva • French Bank • Crédit Agricole S.A. • Public sector agencies • Multiple global financial institutions • Global professional services firm • Larger European insurer • Large US-based cruise line • A German Retailer • A German Utility company • UK-based Energy company • Major investment bank • An Australian oil company	• Total MSS Employees: ~3000 • Delivery Personnel in SOCs: ~600 Delivery from 10 SOCs in: • Indianapolis • Inverness • Derby • Luxembourg • Toulouse • Brussels • Asturias • Mumbai (2) • Bengaluru	• Capgemini prefers to use existing technologies, regularly reviewing the market to ensure the most relevant solutions for clients

Buyer and Provider Recommendations

Buyer Recommendations: Sourcing Managed Security Services

Key actions and considerations moving forward

- **Ask many questions about automation.** In what context will the provider use automation, e.g., for monitoring, labor augmentation? Will the automation be applied directly at the beginning or across the span of the engagement?
- **Spend a lot of time on the details of how the provider will ensure you stay protected as your security posture changes.** This may include regular, formal re-assessments. It should definitely include clear steps on the provider's part to alert you of new threats. Get into details such as, Do you flag new threats after the first evidence, or do you wait for a pattern to emerge before notifying? How do you define new threats compared to existing threats that may just have evolved?
- **Focus relentlessly on remediation.** Monitoring is simple. Taking action on incidents isn't. And your possible actions are often determined by when the threat is detected and how much time you have to respond. You also need to understand how much advice your provider will give in remediation. Is it general best practices? Specific advice based on your environment? Some combination?
- **Evaluate predictive analytics.** Most of the providers we evaluated used analytics to provide key process improvements like reducing the number of false positives and finding internal employee behavior changes faster. However, if you're looking to get ahead of the curve and implement predictive analytics, make sure you have several deep and critical conversations about when and how you might take action on threats that appear likely to happen but haven't happened yet.

Buyer Recommendations: Sourcing Managed Security Services, Continued

Key actions and considerations moving forward

- **Review data integrity responsibilities.** Protecting data is only part of the story. Security algorithms and predictive analytics can't help if you haven't focused on data quality. The accuracy and integrity of data are as important as the steps you take to protect data. Make data integrity a key discussion point during negotiations. Even if it's out of scope, it's important to know the provider's view on its role in this important activity.
- **Consider alternative pricing options.** Although providers didn't offer many examples of outcome-based pricing, it's clear that the market is moving in that direction. As you look for business-based security services, don't forget to match your pricing model to your goals. For example, although flat-fee managed services may sound practical and attractive, they may incent your provider to maintain the status quo rather than innovating on your behalf.
- **Ask how the provider can help you talk to business stakeholders.** This likely will be beyond the capabilities of your daily team. So you'll need to ensure that you have access to senior security experts in the provider organization that can help you prepare board presentations, create business cases for new security investment, and educate non-technical stakeholders on their role in protecting the company's assets.

Buyer Recommendations: Ensuring Your Engagement Keeps Up with the Changing Threat Environment

Key actions and considerations moving forward

- **First, monitor news and trends in security and threat intelligence.** Don't wait for your provider to flag new threat types to you. Yes, as mentioned above, you want your provider to proactively alert you to potential new threats. But don't let that stop you from protecting yourself. You still need ownership of your security insights.
- **Be proactive in asking questions about changes and new threats.** Sometimes, even a quick email asking the provider about a new ransomware technique that you read about will spur discussion about making changes to the service scope or approach.
- **Include security market changes and news as part of monthly meetings.** Make it an agenda item to discuss what's happening in the market. And build into the provider's mindset not to wait for the regular meetings to bring up new events.
- **Expand the scope of your engagement to include regular security posture re-assessments.** This can depend on your industry and other factors, but it might be quarterly, semi-annual, or annual.
- **Include a new engagement metric on the provider's ability to find and address new threats.** The provider's ability to keep your data and organization protected from threats even as those threats change needs to be part of the provider's success metrics if it isn't already.

Provider Recommendations

Key actions and considerations moving forward

- **Help security buyers win over their business stakeholders.** Your direct buyers may be technical and deeply knowledgeable about security, but their colleagues are not. Help your buyers be successful by giving them insights into security threats and the potential impact that are anchored in their organizations' business context. When your buyers tell the security story in business language, they'll be better able to get buy-in and fund appropriate new efforts.
- **Make your automation messaging stronger and clearer.** Automating security has clear benefits for you and your clients – fewer false positives, faster detection of new threats, and better remediation results, among others. And given the talent shortage in security, making the daily jobs of security staff less tedious is high on organizations' lists of to do's. But don't assume prospective clients know your automation approach. Tell clients up front your strategy to automate security and how that strategy will get demonstrated during an engagement.
- **Rethink talent strategy to cast a wider net.** There's no evidence that the security talent wars will get less intense in the next few years. It's important to break out of standard best practices and think more about how to bring in nontraditional talent. What would it take to bring in sociology majors and train them, as an example? What about other non-technical roles that might have some affinity for security work? Work with your internal talent teams to redesign hiring and retention to focus on how to successfully bring in new types of people so you're not always fighting for the same people as your competitors.

Provider Recommendations, Continued

Key actions and considerations moving forward

- **Collaborate more proactively with clients on emerging threats.** Too few of the providers evaluated have clear, step-by-step processes to make sure they stay current with clients' changing security postures. And keep in mind that you may have to take the lead in helping the client know that its security posture changed. Create better approaches for evolving engagement scope to keep up with changes and then educate clients on those approaches.
- **Spend more time answering the differentiation issue.** On the one hand, Managed Security Services can seem commoditized. But that's true only if you don't clearly articulate what makes you different. And it's often not a technical capability or delivery methodology that will show prospective clients what makes your offering unique. You need to spend more time telling prospects your vision for security in the enterprise, how security done well changes the client's business, and what kinds of security innovations you're investing in over the next few years.

About The Author

Christine Ferrusi Ross

Research Vice President, Security, and Blockchain, HfS Research – MA, United States

christine.ferrusi.ross@hfsresearch.com

@ferrusi

Overview

- Christine Ferrusi Ross focuses on helping firms solve complex client problems by developing new service offerings and products to meet new market demands. She's currently focused on building HfS' practices in blockchain and security.
- Christine is a veteran of the IT services industry and the analyst community. She pioneered some of the industry's first research into vendor management and supplier risk, as well as building blockbuster sourcing conferences and peer communities. Christine has helped some of the largest companies in the world operationalize their sourcing strategies and supplier risk efforts.
- From a domain perspective, Christine's passionate about how blockchain will change economies, business models, and supply chains. She's also focused on elevating security from a siloed technology discussion to a business conversation that spans enterprises. She also stays current on supplier and supply chain risk, Internet of Things, democratizing big data, and analytics.
- She's been quoted in the Wall Street Journal, on CNBC, and other national media regarding IT services, vendor management, supplier risk, outsourcing, and globalization.

Previous Experience

- Christine led product strategy at Neo Group, focusing on the company's supplier risk product before coming to HfS. Prior to Neo Group, Christine had several senior roles at Forrester Research, where she created the Sourcing & Vendor Management practice, as well as leading the company's widely praised Sourcing peer council.

Education

- Christine holds a dual degree from Boston University: a BA in International Relations and a BS in Mass Communications.

About HfS Research

HfS Research is The Services Research Company™—the leading analyst authority and global community for business operations and IT services. The firm helps organizations validate and improve their global operations with world-class research, benchmarking and peer networking. HfS Research was named "Independent Analyst Firm of the Year for 2016" by the Institute of Industry Analyst Relations which voted on 170 other leading analysts. HfS Chief Analyst, Phil Fersht, was named Analyst of the Year in 2016 for the third time.

HfS coined the terms "The As-a-Service Economy" and "OneOffice™", which describe HfS Research's vision for the future of global operations and the impact of cognitive automation and digital technologies. HfS' vision is centered on creating the digital customer experience and an intelligent, single office to enable and support it. HfS' core mission is about helping clients achieve an integrated support operation that has the digital prowess to enable its organization to meet customer demand - as and when that demand happens. With specific practice areas focused on the Digitization of business processes and Design Thinking, Intelligent Automation and Outsourcing, HfS analysts apply industry knowledge in healthcare, life sciences, retail, manufacturing, energy, utilities, telecommunications and financial services to form a real viewpoint of the future of business operations.

HfS facilitates a thriving and dynamic global community which contributes to its research and stages several OneOffice™ Summits each year, bringing together senior service buyers, advisors, providers and technology suppliers in an intimate forum to develop collective recommendations for the industry and add depth to the firm's research publications and analyst offerings.

Now in its tenth year of publication, HfS Research's acclaimed blog Horses for Sources is the most widely read and trusted destination for unfettered collective insight, research and open debate about sourcing industry issues and developments.

HfS was named Analyst Firm of the Year for 2016, alongside Gartner and Forrester, by leading analyst observer InfluencerRelations.