May 4, 2011

Market Overview: Intrusion Prevention Systems, Q2 2011

by John Kindervag
for Security & Risk Professionals

May 4, 2011

Market Overview: Intrusion Prevention Systems, Q2 2011

A Mature Space, IPS Is Still The Bulwark Of Network Security

by John Kindervag
with Stephanie Balaouras and Lindsey Coit

EXECUTIVE SUMMARY

An intrusion prevention system (IPS) complements traditional firewalls by inspecting the entire network packet looking for malicious traffic that is often invisible to Layer 3 firewalls. While firewalls are the cornerstone of any network security design, IPS appliances are the bulwark. Within the time-honored security approach known as defense-in-depth (DiD), IPS devices are the second line of network defense. In the future, however, IPS may transform from a standalone appliance sitting behind a firewall to a feature integrated within firewalls, creating a more intelligent, multifunction security gateway.

TABLE OF CONTENTS

NOTES & RESOURCES

Forrester interviewed 14 vendor companies, including Cisco Systems, Check Point Software, Enterasys Networks, HP TippingPoint, IBM, Juniper Networks, McAfee, Palo Alto Networks, Radware, and Top Layer Security.

Related Research Documents

"Build Security Into Your Network's DNA: The Zero Trust Network Architecture"
November 5, 2010

"TechRadar™ For Security & Risk Professionals: Network Threat Mitigation, Q3 2009"
July 22, 2009

"If You Don't Have IPS, You Deserve To Be Hacked"
April 8, 2009

IPS: FROM STANDALONE APPLIANCES TO MORE INTEGRATED MULTIFUNCTION GATEWAYS

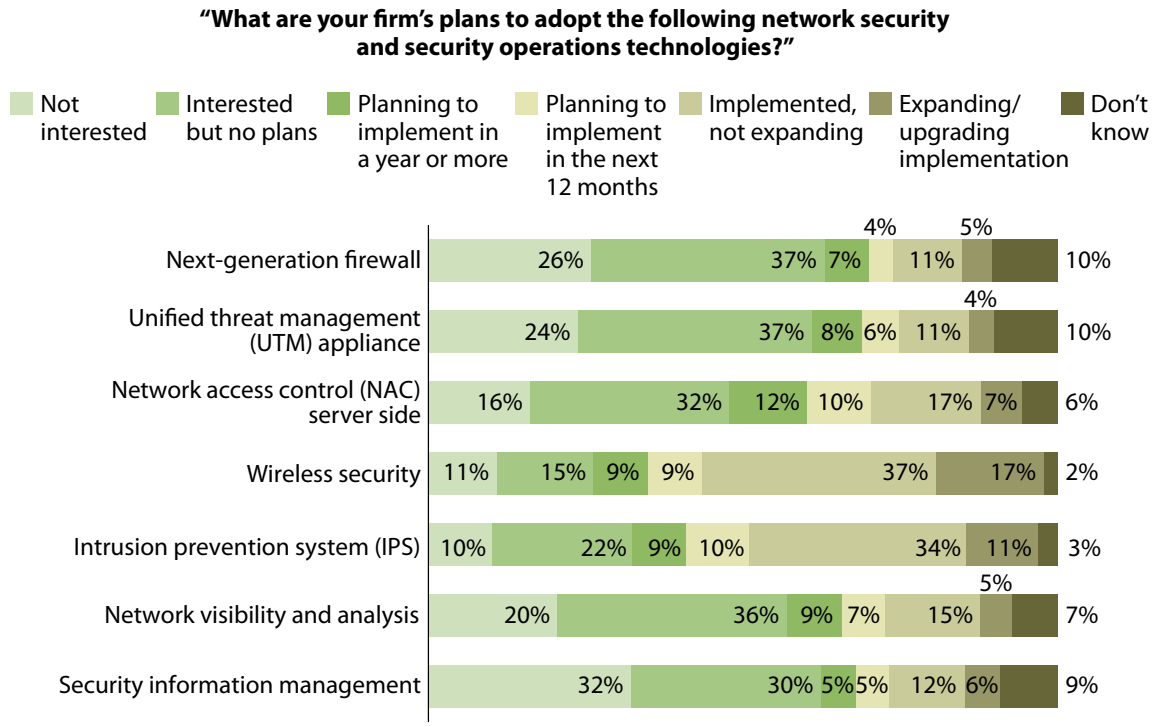
The intrusion prevention market has traditionally been defined as in-line, standalone appliances designed to block malicious traffic on the wire before it can reach vulnerable network subsystems. IPS systems had to be low latency and high performance and provide proactive security without negatively affecting the network.[1] Overall, IPS vendors have succeeded at these goals.

Today, however, an intersection of unified threat management (UTM) and network firewalls with traditional IPS systems is creating a more integrated multifunction gateway where firewall and intrusion prevention are just two of the many features served by these gateways.[2] This market overview looks at standalone IPS devices as well as those products that have IPS functionality within what has traditionally been called UTM or next-generation firewalls.

At Forrester, we have been anticipating this merger of technologies, and we see a bright future for integrated multifunction gateways. In fact, we anticipate that the speed and power of these devices will enable future security professionals to use these types of devices in the very core of their network to create a future state architecture we call the Zero Trust network architecture. In this proposed network architecture, we call these multifunction appliances "segmentation gateways" because they provide security functionality and network segmentation within a single solution.[3]

Recent data from Forrester's Forrsights Security Survey indicates that the standalone IPS market is a relatively mature space but that the next-generation firewall and UTM markets are expanding (see Figure 1). Given that the line between next-gen firewalls and UTM is heavily blurring, we anticipate a consolidation of firewalls and IPS to create an even more advanced multifunction security gateway. The ready availability of dense multicore CPU appliance architectures and the rise of low-cost merchant silicon to meet specialized processing demands (such as SSL offloading and inspection) means that hardware now has the horsepower to put best-of-breed firewall and IPS functionality on the same box.

Figure 1 Customers Are Interested In Multifunction Security Gateways



Base: 1,025 North American and European security decision-makers
(percentages may not total 100 due to rounding)

Source: Forrsights Security Survey, Q3 2010

57031 Source: Forrester Research, Inc.

TEN TECHNOLOGIES MAKE UP THE IPS LANDSCAPE

In this market overview, we are not distinguishing between traditional standalone IPS appliances and next-generation firewalls or UTM devices. The purpose is to provide a quantitative overview of the range of choices available to information security professionals when choosing a solution to help proactively mitigate attacks. For the foreseeable future, we anticipate that most organizations will have a mixture of standalone appliances and integrated multifunction gateways.

Today's Established Features Support 10 GbE, Auto Updates, Ease Of Use, And Testing

There are several important features that should be found in any modern intrusion prevention system. When choosing an IPS product, the basic features should include:

- **10 GbE capacity and interfaces.** Modern networks are fast. In order to protect any investment, make certain that the IPS can handle multigig traffic loads. In most cases, you will look for a product that has multiple 10 Gig interfaces and that has a backplane that can handle the aggregate throughput of all device interfaces. Right now, one finds 10 Gig links between core/distribution uplinks. In the future, however, networks may have multiple 10 Gig switching zones similar to those found in Forrester's Zero Trust network architecture.

- **Auto signature updates.** Threats change and evolve quickly. IPS vendors must be able to react to these new and dangerous threats. Therefore, a base feature of all IPS solutions should be a way to automatically download and deploy new signatures or filters that vendors have created to meet this challenge. In general, these updates will have some type of recommended setting so they can be deployed quickly to prevent a new attack from damaging your network. Make certain that potential vendors have a strong track record of generating new signature updates on a regular basis — usually weekly.

- **Web-based management.** Threat protection is complex, and management can be difficult. Modern IPS solutions should have an intuitive, web-based management interface that allows for the rapid response to any new threat or attack.

- **Third-party testing.** There are quality testing labs that specialize in putting IPS systems through their paces. These labs try to emulate real-world conditions and simulate current attacks as closely as possible to help organizations make informed decisions. Notable labs specializing in IPS testing include NSS Labs and ICSA Labs.[4]

Differentiating Features Offer Access Control, Management, Compliance, Inspection, Scale

When choosing an IPS, there are other features that can help determine which product fits your organization's specific needs. These differentiating features include:

- **Active Directory integration.** To understand user behavior, it's important to tie into the organization's main directory infrastructure. This is often Microsoft's Active Directory, but it could be any other LDAP-based directory system.

- **Access control lists/firewall features.** As the boundaries between traditional IPS and firewall products become fuzzy, there is increased need for firewall features or even simple access control lists (ACLs). The ability to restrict traffic to a resource can provide an important uplift to your company's overall security posture.

- **Central management console.** Most large organizations will require the deployment of more than one IPS if the network is to properly protect it. The management of any product is a long-term issue that security professionals often overlook during the excitement of the purchasing phase of the new technology. If you anticipate multiple IPSes in your network, make certain that you can manage them centrally from a single console.

- **Compliance reporting capability.** Like it or not, compliance drives much of security today. Hedge your bets by choosing an IPS system with good reporting capabilities that you provide to any of the myriad auditors or assessors who regularly prowl your data center.

- **Ability to inspect encrypted traffic.** As cyberthreats increase, it's natural to try to protect sensitive traffic with encryption. Information security professionals generally agree that there has been a substantial increase in encrypted traffic flowing to and from the network. SSL is becoming a ubiquitous protocol, but these secure tunnels could contain malicious traffic or stolen data. Therefore, it's important to be able to inspect encrypted traffic such as SSL for known threats.

- **Purpose-built hardware.** The increased number of threats intersecting with the overall increased network traffic is combining to create a perfect storm of potential performance backlogs. There is a real fear commonly expressed by infrastructure and operations professionals that security devices will impede traffic flow. An IPS device is very similar to a muscle car. You have to open the hood and see what kind of engine it has. Vendors who skimp on the hardware side and try to use commodity, industry-standard servers may not have the horsepower necessary to effectively process packets in near real time. Choose products that have a finely tuned racing engine under the hood.

IPS Is The Swiss Army Knife Of Information Security

Deploying IPS in your organization can solve multiple problems with a single tool (see Figure 2). The most significant feature of IPS is the ability to block malicious traffic "on the wire." This provides a twofold benefit:

- **Bad "stuff" is dropped before it can impact resources.** This means that security engineers are no longer chasing their tails trying to remediate attacks and hunt down infected machines. While not 100% effective, IPS solutions should be able to provide for a significant reduction in incident response efforts.

- **Resource availability is increased.** Infrastructure and operations professionals fear downtime. In the past, they have been worried that IPS devices would block or interrupt good traffic. IPS has turned the tables; IPS has the ability to ensure network uptime because it's blocking malicious traffic from bringing down critical resources.

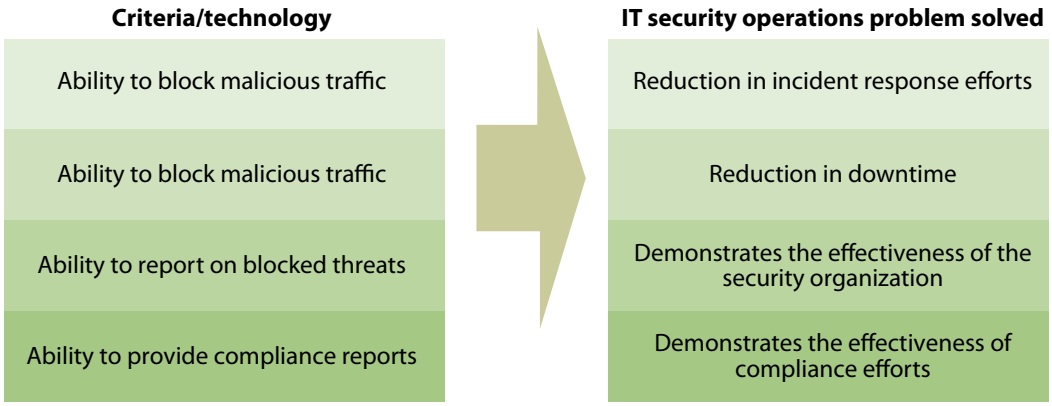
The comprehensive reporting capability of most IPS devices is another, often overlooked, benefit of deploying IPS devices in your network. Reporting is important in two significant ways:

- **IPS reports prove that security is working.** Security organizations now have an actionable way to prove that they are effective. The ability to provide a report that shows all the dropped bad packets can be immeasurable in its importance. Our research indicates that security organizations are

constantly struggling to demonstrate the effectiveness of their security efforts, and IPS reports go a long way in proving to executives that powerful and proactive security controls are in place.

- **IPS reports demonstrate the effectiveness of compliance efforts.** Most organizations now have numerous compliance obligations that they struggle to achieve and maintain on a consistent basis. The ability to show that security is proactive goes a long way in helping assessors and auditors see that compliance initiatives are important in your organization.

Figure 2 Emerging IPS Technologies Are Solving Security Challenges



57031 Source: Forrester Research, Inc.

THE IPS MARKET IS CONSOLIDATING QUICKLY

While there remains a significant demand for standalone IPS appliances, there is clearly a trend to create integrated gateways where intrusion prevention is a function of the appliance. This is especially effective when replacing main ingress points like Internet connections and wireless aggregation chokepoints — where both a firewall and an intrusion prevention device are necessary. Forrester recommends that you enable intrusion prevention at each point of ingress in the network, at minimum. This means there will remain a need for dedicated IPS appliances for the foreseeable future to protect network segments that may not need a full stateful, packet-filtering firewall, such as behind a WAN router.[5]

Vendor Overview

For those trying to keep this all straight, the good news is the market is consolidating very quickly — taking the best, most innovative technologies and marrying them with much larger suites. While there are numerous vendors offering IPS functionality, we've included a selection of vendors worth noting (see Figure 3):

- **Check Point Software.** Check Point acquired NFR Security, an intrusion detection system (IDS) vendor, in 2006 following the failed acquisition attempt of Sourcefire.[6] Check Point has transformed that code into its IPS-1 intrusion prevention offering. It's available as a standalone product or as a "software blade" as part of the latest versions of the Check Point firewall offering. One advantage that Check Point has is its excellent, intuitive management platforms: SmartCenter and Provider-1.

- **Cisco Systems.** Cisco is one of the most established IDS vendors in the space. It has updated its IDS solution to function as an IPS device. However, our experience leads us to believe that its standalone offerings are not attractive to organizations that don't have a Cisco bias. Cisco lacks robust Active Directory integration, and its management is long-in-the-tooth. Cisco's IPS offerings are due for an overhaul. There are positive indications coming out of Cisco that it understands the need for more focus in this area, but the market will decide if new offerings get any significant traction beyond "Cisco shops."

- **Enterasys Networks.** Enterasys offers an IPS solution colloquially known as Dragon. It was one of the first enterprise IDS products, and the company has repositioned it as an IPS. Enterasys also offers infrastructure products in its portfolio. For companies using Enterasys for their network infrastructure, the Enterasys IPS product could be compelling, as there is potential for more integrated device management using this vendor's solutions. Additionally, Enterasys IPS supports open standards for interoperability with multivendor environments, and the solution has been deployed widely at customer sites with existing third-party infrastructures.

- **Fortinet.** Fortinet was one of the creators of the UTM space. As its solutions developed and move more toward becoming next-generation firewalls, there is an increased product focus on the IPS functionality of their gateways. Organizations that already have deployments should scrutinize the road map to determine if Fortinet will meet their long-term objectives.

- **HP TippingPoint.** TippingPoint is now part of HP via the 3Com acquisition.[7] Already a market leader, HP TippingPoint now has deeper pockets and a large consulting organization — the former EDS — to help drive even more business. Its success will hinge on the execution of the integration with the larger HP Networking portfolio.

- **IBM.** IBM acquired Internet Security Systems in 2006.[8] ISS had long been an innovator and leader in both intrusion detection and intrusion prevention. The acquisition gave IBM a critical offering (Proventia IPS) in its burgeoning security portfolio but also gave it an offering that it could deliver as a managed service using its huge Global Services arm. Like most acquisitions, there have been challenges: Several individuals from ISS's management team left IBM after the acquisition, and several Forrester clients have told us they plan to replace their IBM Proventia

products. However, IBM is working to prioritize security. In 2010, the company appointed a general manager to oversee IBM's security portfolio across its various groups (Tivoli, Rational, Global Services etc.). This is an important indicator of security's strategic importance within the company. In addition, the company still has a major Proventia install base and has made significant investments in its recently announced 10 Gigabit appliance. The GX7800 is capable of performing inspection for more than 23 Gbps of traffic.

- **Juniper Networks.** Juniper's recent entry into the enterprise switch market makes it one of the few players that cover most of the bases in both infrastructure and security. Juniper makes both a standalone IPS product and a gateway that integrates IPS and firewall functionality. It has put significant resources into rebuilding a unified code base that should facilitate easier management of homogeneous Juniper networks.

- **McAfee.** McAfee has made a splash recently with the Intel acquisition. It has an existing IPS formerly known as IntruShield. Combined with the firewall capabilities it gains from its acquisition of Secure Computing, the firm is clearly headed along the path of creating its own take on the next-generation firewall concept. By integrating its network security products with its desktop management system, ePO, McAfee is banking on the fact that customers using its endpoint products will appreciate integrating network security devices into a single view.

- **Palo Alto Networks.** Palo Alto Networks has shaken up the network security market by developing the new space known as next-generation firewalls. Its products have disrupted the detente between IPS and firewalls. Customers are benefiting from buying a single box instead of two separate devices. The unanticipated and unparalleled success of Palo Alto Networks is pushing the entire vendor community toward further innovation.

- **Radware.** Radware offers application delivery controllers as well as IPS devices. Additionally, its IPS devices have integrated denial-of-service (DoS) protection as well as network behavior analysis (NBA) capabilities. For companies that have a need to consolidate these features, these offerings may be a scalable solution.

- **SonicWall.** Traditionally known for its chokehold on small and midsize markets, SonicWall made a splash with the release of a very high-speed hardware platform in 2010. The firm has also developed a unique way of performing IPS functionality and is now seeing interest from larger enterprise organizations.

- **Sourcefire.** Famous for its Snort open source IDS software, Sourcefire has packaged that engine for use in enterprise networks. Its solution is very popular among security engineers who cut their teeth on Snort. In Q2 2011, Sourcefire delivered appliance hardware that will support

throughput ranging from 5 Mbps to 40 Gbps, with true IPS protection at 20 Gbps speeds. The company also offers a virtual IPS for the VMware and Xen platforms. In addition, Sourcefire has a Network Access and Visibility add-on called RNA, which delivers passive vulnerability detection, and OS, network, device, application, and user awareness, so that the IPS can automatically take informed actions. The company recently announced that it is creating a next-generation firewall, available later this year.

- **Stonesoft.** Stonesoft offers multiple different solutions through its StoneGate branded line of firewalls, VPNs, and IPSes. The company also offers a centralized management console designed to pull them all together.

- **Top Layer Security.** Top Layer Security is a standalone IPS vendor struggling to find its identity. With a focus on hardware horsepower, it has developed a reputation as an anti-DDoS tool among security aficionados.

Figure 3 Today's IPS Market Offers A Wide Variety Of Solutions

Vendor	10 G interfaces	Active directory integration	ACL/FW features	Auto signature updates	Central management console	Compliance reporting capability	Inspect encrypted traffic	Purpose-built hardware	Third-party testing	Web-based management	Max. throughput in GB/sec
Check Point	✓	✓	✓	✓	✓	✓	[1]	✓	✓	✓	15
Cisco			✓	✓	✓	✓		✓	✓		*
Enterasys	✓	[2]	✓	✓	✓	✓		✓		✓	6
Fortinet	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	12.5
HP TippingPoint	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	16
IBM	✓	✓	✓	✓	✓	✓		✓	✓	✓	23
Juniper	✓	[3]	✓	✓	✓	✓	✓	✓	✓	✓	30
McAfee	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10
Palo Alto Networks	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	20
Radware	✓		[4]	✓	✓	✓		✓	✓	✓	12
SonicWall	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	*
Sourcefire	✓	✓	[5]	✓	✓	✓	✓	✓	✓	✓	40
Stonesoft	✓	✓	✓	✓	✓	✓	✓	✓	✓		13
Top Layer Security	✓		✓	✓	✓	✓		✓	✓	✓	8

✓ Vendor offers the technology ☐ Vendor does not offer the technology

*Vendor did not provide figure

[1] This capability is planned

[2] Product integrates with LDAP or RADIUS

[3] AD integration can be supported using Juniper's unified access control product

[4] Radware has ACL features including black and white lists

[5] Sourcefire's firewall features are planned

57031 Source: Forrester Research, Inc.

RECOMMENDATIONS

CHOOSE AN IPS THAT CAN BECOME "ONE" WITH YOUR NETWORK

A network is a system. It contains infrastructure elements, application elements, and security elements. The system interacts with users and customers. IPS devices are very powerful. Harness this power by carefully choosing an IPS solution that will fully integrate with your entire network system. By thinking of IPS as one element in the system, you can design your solution and choose effective products that will provide manageable and scalable security for your network now and in the future. Forrester recommends that you:

- **Consider networking and security holistically when making a buying decision.** Too often, security professionals make security decisions in a vacuum. While best-of-breed tools are important, the ability to implement and integrate your chosen solution is equally important. Look for IPS devices that have the ability to integrate with other IT systems. For example, a client security suite may be able to share data with an IPS so that both subsystems can act more intelligently. Also, choosing an IPS product offered by your infrastructure vendor can provide significant value, if the IPS is robust and integrates well with the rest of the vendor's product line.
- **Plan for the future of your network.** Threats change. Networks change. Packets move faster and the business expects your infrastructures to do more. It's important to take a lasting view of your network and anticipate how increased speeds or new attacks might affect how you deploy the devices today. Take off any legacy blinders and expand your vision. Look at your network and your security road map objectively — as if you were an attacker — and ask if the technologies and processes you are about to deploy will be effective.
- **Factor in the costs of device management.** The long-term care and feeding is the most costly part of any product purchase. Security professionals usually don't consider these factors when calculating the total cost of the product. Too often, security professionals focus only on the capital acquisition cost of the product. A product that seems cheap today may turn out to be very expensive in the end if it's difficult to manage and maintain. Look for IPS devices that are intuitive and automated. The best solutions will feel as if they are "self-managing."
- **Open up the hood.** Horsepower. Horsepower. Horsepower. Like a racecar, IPS devices are about speed. Speed to process packets and to make a security decision in near real time. Speed to provide low latency and near transparent connectivity so that circle protocols such as voice and video don't experience jitter or breakups. Make sure your chosen IPS vendor can articulate the horsepower story on its devices. Be careful of trickery and vendors who won't open up the hood and show off their big block engine.

SUPPLEMENTAL MATERIAL

Companies Interviewed For This Document

Check Point Software	McAfee
Cisco Systems	Palo Alto Networks
Enterasys Networks	Radware
Fortinet	SonicWall
HP TippingPoint	Sourcefire
IBM	Stonesoft
Juniper Networks	Top Layer Security

ENDNOTES

[1] For a detailed look at intrusion prevention systems, see the April 8, 2009, "If You Don't Have IPS, You Deserve To Be Hacked" report.

[2] At Forrester, we have been seeing evidence that this type of integration would occur. In another report we noted that the "UTM category may eventually become extinct as next generation firewalls evolve and add UTM-like features to their core functionality." See the July 22, 2009, "TechRadar™ For Security & Risk Professionals: Network Threat Mitigation, Q3 2009" report.

[3] Forrester has created a reference architecture based on the Zero Trust Model. See the November 5, 2010, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture" report.

[4] NSS Labs (http://nsslabs.com/) and ICSA Labs (https://www.icsalabs.com/) have tested numerous IPS and other security devices. Their methodologies are well-known and respected in the infosec community.

[5] For an overview of recommended IPS deployment scenarios, see the April 8, 2009, "If You Don't Have IPS, You Deserve To Be Hacked" report.

[6] Source: "Check Point to Acquire NFR Security; Expands Intrusion Prevention Capabilities to Fortify Enterprise Networks," Check Point Software Technologies press release, December 19, 2006 (http://www.checkpoint.com/press/2006/nfrsecurity121906.html).

[7] Source: "HP to Acquire 3Com for $2.7 Billion," HP press release, November 11, 2009 (http://www.hp.com/hpinfo/newsroom/press/2009/091111xa.html).

[8] Source: "IBM to Acquire Internet Security Systems," IBM press release, August 23, 2006 (http://www-03.ibm.com/press/us/en/pressrelease/20164.wss).

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Forrester has research centers and sales offices in more than 27 cities internationally, including Amsterdam; Cambridge, Mass.; Dallas; Dubai; Foster City, Calif.; Frankfurt; London; Madrid; Sydney; Tel Aviv; and Toronto.

For a complete list of worldwide locations visit www.forrester.com/about.

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com.
We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, customer insight, consulting, events, and peer-to-peer executive programs. For more than 27 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.

FORRESTER®