January 24, 2011

Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility

by John Kindervag

for Security & Risk Professionals

FORRESTER® Making Leaders Successful Every Day

January 24, 2011

Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility

Essential Functionality For The Zero Trust Model Of Information Security

by John Kindervag
with Stephanie Balaouras and Lindsey Coit

EXECUTIVE SUMMARY

In today's threat environment, the network perimeter has disappeared. Insiders are as insidious a threat as outsiders. In the past, the "trust but verify" model did not facilitate insight into internal and nontraditional threats. Forrester's new Zero Trust Model of information security demands that organizations know what types of activities take place on their internal network as well as their external network. To provide this type of deep insight into internal and external networks, Forrester has defined a new functional space called network analysis and visibility (NAV). NAV is comprised of a diverse tool set designed to provide situational awareness for networking and information security professionals.

TABLE OF CONTENTS

2 **Forrester's Zero Trust Network Security Report Collection**

2 **Wikileaks Testifies To The Need For Improved Network Visibility**

4 **Current Networks Are Blind To Insider Abuse**

5 **NAV Provides Insight Into Insider Threats**

8 **NAV Will Assist With Insider Threats, External Threats, And Compliance**

RECOMMENDATIONS

9 **Put Your Head On A Swivel And Develop Network Situational Awareness**

10 **Supplemental Material**

NOTES & RESOURCES

Forrester interviewed 22 vendor companies, including Arbor Networks, Fidelis Security Systems, Gigamon, HBGary, Lancope, LogRhythm, Lumeta, McAfee, Narus, NetOptics, NetScout, netWitness, Niksun, NitroSecurity, PacketMotion, Q1 Labs, Qosmos, Solera Networks, SolarWinds, Sourcefire, Trend Micro, and Vitria.

Related Research Documents

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

"No More Chewy Centers: Introducing The Zero Trust Model Of Information Security"
September 14, 2010

"The New Threat Landscape: Proceed With Caution"
August 13, 2010

FORRESTER'S ZERO TRUST NETWORK SECURITY REPORT COLLECTION

This is the third in a collection of reports that describe the concept, architecture, and benefits of Forrester's Zero Trust Model of information security. There is a simple philosophy at the core of Zero Trust: Security professionals must stop trusting packets as if they were people. Instead, they must eliminate the idea of a trusted network (usually the internal network) and an untrusted network (external networks). In Zero Trust, all network traffic is untrusted. Thus, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic.

The Zero Trust network security report collection will consist of the following reports:

- **Concept.** This report introduces the necessity and essential concepts of the Zero Trust Model of information security.[1]
- **Architecture.** This report outlines the key architectural components, capabilities, and required technologies of the Zero Trust Model.[2] This third report supports the architecture report. It details a set of functions and capabilities (that we call network analysis and visibility) essential to the Zero Trust Model and architecture.
- **Case studies.** In a series of case studies, Forrester will highlight security organizations that have adopted or applied concepts of the Zero Trust Model in their environment. Included in the case studies will be a discussion of best practices and benefits.

WIKILEAKS TESTIFIES TO THE NEED FOR IMPROVED NETWORK VISIBILITY

The recent firestorm created by the Wikileaks disclosure of more than 250,000 sensitive US government documents has put a spotlight on our current broken trust model and how it facilitates the theft and leakage of various types of toxic data. According to chat logs that have been published in reputable news sources, Pfc. Bradley Manning, a 22-year-old Army Intelligence analyst stationed in Iraq, admitted to surreptitiously downloading thousands of sensitive military and State Department documents during online chats with convicted hacker Adrian Lamo. Manning allegedly had nearly unrestricted access to the United States Department of Defense (DoD) Network known as SIPRNet (Secret Internet Protocol Router Network). According to the logs, Manning himself seemed surprised by the ease with which he compromised a "secret" network:

> (02:12:23 PM) Manning: so . . . it was a massive data spillage . . . facilitated by numerous factors . . . both physically, technically, and culturally
>
> (02:13:02 PM) Manning: perfect example of how not to do INFOSEC

> (02:14:21 PM) Manning: listened and lip-synced to Lady Gaga's Telephone while exfiltratrating [sic] possibly the largest data spillage in American history
>
> (02:15:03 PM) Manning: pretty simple, and unglamorous
>
> (02:16:37 PM) Manning: *exfiltrating
>
> (02:17:56 PM) Manning: weak servers, weak logging, weak physical security, weak counter-intelligence, inattentive signal analysis . . . a perfect storm
>
> (02:19:03 PM) Manning: >sigh<[3]

Regardless of the legal, constitutional, and free speech questions raised by the Wikileaks scandal, it is clear that Pfc. Manning was "trusted" and not "verified."

Recent Data Breach Statistics Show An Alarming Increase In Insider Data Breaches

According to the Verizon 2010 Data Breach Investigations Report, insider threats are increasing. This report noted that insiders were responsible for 48% of data breaches in 2009, which is up 26%.[4] Also, this was the first year that United States Secret Service (USSS) data was included in the report. Not surprisingly, insider breaches were more common in those cases because contacting law enforcement, such as the USSS, is protocol for insider theft or misuse at many organizations. As a threat vector, 48% of data breaches were the result of privileged insiders who misuse. This is up 28% from the previous year, signifying a dramatic and worrisome trend.

Sadly, the report data confirms what Forrester has seen: Most organizations are not properly monitoring their environment for these types of threats. In 86% of breaches, the victims had evidence of the breach in their log files. This demonstrates that most breached organizations were not actively looking at their logs or monitoring the network for potential breaches or other malicious activity.

Insider Threats: Your Intellectual Property Is At Also Risk

A less-publicized type of data breach targets intellectual property. One recent example of intellectual property theft occurred when a Ford Motor Company product engineer, Mike Yu, absconded with approximately 4,000 sensitive Ford documents, which he took with him to his new job at Beijing Automotive Company. The files included 41 system design specification documents that Yu appears to have accessed while an employee of Beijing Automotive Company. Authorities arrested Yu when he returned to the United States, and they found the documents on his Beijing Automotive Company corporate laptop. Yu pleaded guilty to two counts of theft of trade secrets and faces up to 78 months in prison and a fine of up to $150,000. Yu will also be deported once he completes his prison sentence.[5]

CURRENT NETWORKS ARE BLIND TO INSIDER ABUSE

As one global CIO recently told Forrester, "I don't know what's going on in my internal network, and I don't want to know. If I knew, then I would have to fix it." This CIO is not atypical, as the old trust model defined internal users as "trusted" and, therefore, their activities were not subject to the same level of scrutiny as external or "untrusted" users. This flawed trust model allowed executives to hide from potential insider threats. This was not necessarily their intention, however. A trust model that defines trusted and untrusted users does not give organizations incentives to put the type of controls on their internal network that would give them the necessary level of awareness about so-called "trusted user" activity.

The Current State Of Network Visibility Is Equivalent To Putting Your Head In The Sand

Our experience leads us to believe that most networking or information security professionals have no insight regarding the behavior of internal traffic and the potential threats incumbent with that traffic. According to the Bradley Manning chat logs, "i even asked the NSA [National Security Agency] guy if he could find any suspicious activity coming out of local networks . . . he shrugged and said . . . "its [sic] not a priority."[6]

Evidence suggests that most breached entities or organizations do not discover their own breaches. The Verizon report indicates that third parties discover 61% of data breaches.[7] We can explain this by examining how breaches are usually exposed. One typical way breaches are discovered is through something known as common point-of-purchase. This is a technique where card brands and credit card processors can compare fraudulent credit card or other financial activity with purchase activity and then triangulate activity back to a single point, such as a retail store or eCommerce website. The common point-of-purchase is the place in which the credit cards were originally breached. For example, Heartland Payment Systems, a credit card processor, was notified of its breach by the card brands. The infamous Philip Cummings case, where a software company help desk employee was providing credit reports to organized crime figures, was not discovered by his employer or even the credit bureaus whose data was being stolen, but by one of the credit bureaus' clients.[8] As Verizon notes in its report: "Most breaches are discovered by external parties and only then after a considerable amount of time."[9]

In The Future, Your Organization Must Pull Its Head Out Of The Sand And Put It On A Swivel

The term "put your head on a swivel" is fighter pilot lingo describing the act of a combat pilot constantly moving his head and scanning the skies looking for potential threats or "bogeys." New tools will help the entire network function like a fighter pilot on alert, constantly scanning the network for malicious activity, behaviors, and potential attacks. The more clinical term is "situational awareness," or SA. In information security, we can use the same term, SA, to mean that an enterprise should know what traffic is doing on all of its networks, not just the perimeter, at all times. Today, the external network is typically logged and sometimes monitored, but tomorrow, internal networks must also be inspected, logged, and monitored so that companies will have situational awareness regarding their internal users. By changing to the Zero Trust Model, organizations will demand to know what their internal users are doing because that traffic is no longer trusted. Zero Trust provides a business case to bring internal controls up to a level necessary to meet modern threats. When a company adopts a Zero Trust mentality, it will quickly find that it wants to know what is going on inside its network.

NAV PROVIDES INSIGHT INTO INSIDER THREATS

Architecturally, there are multiple ways to put your head on a swivel and meet the Zero Trust inspection and logging mandates. For example, an organization could deploy traditional perimeter controls, such as firewalls and intrusion prevention devices, throughout the internal network to inspect traffic and create the logs that make this part of Zero Trust actionable. This would prove difficult to do in many environments. As part of our Zero Trust Model, Forrester has defined a set of new functions and capabilities called network analysis and visibility, or NAV. It allows information security professionals to pull their heads out of the sand and put them on a swivel.

NAV Provides Scalable And Nondisruptive Situational Awareness

NAV tools have the capacity to uplift visibility in a highly scalable manner. These tools generally work by passively sniffing traffic traversing the network. Whenever a user accesses a resource, traffic moves across the network. By capturing and analyzing network traffic, NAV tools can look deep inside the moving packets and examine those packets and their traffic flows to look for potential attacks or malicious insider abuse. In fact, most of the transactional information that would be seen by monitoring application logs can be reconstructed and reviewed at the application level by analyzing network traffic. When a user accesses a resource, traffic traverses the network and leaves a trail. Therefore, info sec pros can view user activity in near-real time with NAV tools. Audit trails can be studied. NAV makes it difficult for attackers to be invisible and still achieve their objectives. NAV is a function or an objective for organizations adopting Zero Trust. It is not a single tool but a diverse collection of tools that have similar functionality.[10] These tools include:

- **Network discovery tools for finding and tracking assets.** Modern networks are dynamic, and the only constant is change. Information security professionals are usually not notified about changes in the network or resources. This is especially true with the rise of virtualization. IT ops professionals can spin up or move virtual hosts with little effort. In a world marked by internal threats and compliance mandates, it is imperative that organizations have insight into dynamic network changes that could affect risk and compliance initiatives. Companies such as Lumeta and Sourcefire make products that specialize in network discovery. Additionally, many vulnerability scanners can provide this functionality as well.

- **Flow data analysis tools to analyze traffic patterns and user behaviors.** Many network devices, such as routers, generate a type of data known as flow data. A flow is defined in various ways by various vendors, but Cisco NetFlow is the most commonly supported flow protocol. NetFlow defines a flow as a combination of multiple network traffic variables, including the IP source and destination addresses, the source and destination ports, the Layer 3 protocol type, the class of service, and the interface of the router or switch that generated the flow.[11] By statistically analyzing flow data on a network, anomalous (and potentially malicious) behavior, such as downloading more than 250,000 documents, can be identified.

For example, a flow data analysis tool can look at outbound traffic for large amounts of data leaving the network boundary — this could be an indicator that toxic data has been compromised and is destined for an attacker. Pfc. Manning himself notes, "hardest part is arguably internet access . . . uploading any sensitive data over the open internet is a bad idea . . . since networks are monitored for any insurgent/terrorist/militia/criminal types . . . tor + ssl + sftp."[12] Here he admits to using encrypted protocols to allegedly send the downloaded documents to Wikileaks. That alone should have fired off an alert, had the DOD been properly monitoring the SIPRNet network. Vendors such as Lancope, Arbor Networks, Riverbed Technology, and Vitria offer flow analysis tools that provide NAV functionality.

- **Packet capture and analysis tools that function like a network DVR.** As Pfc. Manning noted in his chat conversation with Adrian Lamo: "its [sic] impossible to trace much on these field networks . . . and who would honestly expect so much information to be exfiltrated from a field network?"[13] While it may be difficult in certain dynamic environments to fully trace and monitor packets, it should be possible to capture, analyze and replay packets to mitigate the risks inherent in these types of networks. Packet capture and analysis tools sniff traffic off the wire and store the captured packets on massive hard disks where sessions can be replayed, and websites can be displayed, long after the traffic was originally generated. This type of tool can be helpful both during and after malicious events, as the tools typically have the ability to alert on anomalous behavior as well as replay captured packets for later investigation. Niksun and AccessData make products that fulfill this need.

- **Network metadata analysis tools provide streamlined packet analysis.** Metadata analysis tools are similar to packet capture and analysis tools, except metadata tools do not store the complete packet. Instead, as the packet is sniffed, metadata such as user login, IP address, port, protocol, MAC address, timestamps, application requests, and even email subject lines are extracted, and the rest of the packet is discarded. For example, the IP address 192.168.1.1 is a metadata representation of binary data that traverses the network. In many instances, the full packet is not necessary to achieve NAV functionality. This reduces the storage needs for the tool and is a more cost-effective solution for many organizations. Each company must determine whether its use cases mandate full packet capture and storage or metadata capture and storage as part of its NAV tool selection process. Vendors such as PacketMotion, Narus, and Solera Networks specialize in this area.

- **Network forensics tools assist incident response and criminal investigation.** These tools are defined by their primary use case. Network forensics examination tools have functionality similar to some metadata analysis or packet capture tools but with a deeper tool set to help respond to incidents and do forensics investigations. In the Wikileaks case, it is certain that extensive forensics examinations were undertaken once the leak was made public. The stolen data traversed many paths that all require forensic examination. As Manning told Lamo:

  > "lets [sic] just say *someone* i know intimately well, has been penetrating US classified networks, mining data like the ones described . . . And been transferring that data from the classified networks over the "air gap" onto a commercial network computer . . . sorting the data, compressing it, encrypting it, and uploading it to a crazy white haired aussie who can't seem to stay in one country very long =L"[14]

  These tools may well be able to provide near real-time NAV functionality but will be especially useful for organizations that have frequent forensics investigation needs. Vendors such as NetWitness and Guidance Software have carved out an area for themselves in this important target market.

NAV And SIM Tools Will Be Tightly Integrated To Provide Maximum Visibility And Reporting

While security information management (SIM) is a mature technology, watching every single resource in the network can be problematic. Many organizations try to monitor applications in order to achieve a NAV-like objective, but gathering the log data from the myriad applications that exist on the network can be daunting. First, there is the issue of cost. Many SIM tools charge by device or number of events, so adding more devices, applications, or traffic can increase SIM costs. The second issue is manageability. Traditional SIM can be high-touch. For proper functionality, many servers and applications will require the deployment of an agent. At the very least, info sec pros must configure each application or device to send its logs to a specific log server.

There will, of course, be certain types of backend calls between applications and other resources that will not easily be seen by a NAV tool. This is why it is important to tie your SIM and NAV together. Using the correlation function of the most SIM products, you will be able to compare what is seen by your NAV tool with the information being reported by specific application logs. SIM tools remain an excellent aggregator of disparate security information. Feeding NAV information to your SIM tool will maximize visibility across all resources. In the future, we anticipate that SIM tools will provide even deeper data analytics capability, which may lead to a blending of SIM and NAV functionality into single tools. Some SIM vendors, such as NitroSecurity, Q1 Labs, and LogRhythm, already integrate flow data into their products by default and may function as an integrated SIM/NAV in certain environments today.

NAV WILL ASSIST WITH INSIDER THREATS, EXTERNAL THREATS, AND COMPLIANCE

While Bradley Manning and Mike Yu are quickly becoming the poster children of insider threats, there are other reasons that situational awareness is important in modern networks.

NAV Changes User Behaviors

By deploying NAV, you have the ability not only to find malicious insiders but to keep insiders from behaving maliciously in the first place. Make sure your users know that IT security will monitor and inspect all traffic as part of your adoption of the Zero Trust Model. This will reduce the temptation for insiders to behave maliciously. United States Secret Service data contained in the Verizon data breach report indicates that third parties are bribing or coercing insiders more frequently than ever before.[15] NAV can help mitigate this risk before it can get started. Individuals will behave differently when they know IT security is monitoring their traffic.

Changing Threat Vectors And Evolving Compliance Mandates Require Enhanced Visibility

There are many factors driving NAV adoption. Insider threats remain the most significant, but others include:

- **Custom malware designed to avoid traditional detection techniques.** Modern malware is more sophisticated than it has ever been. Highly skilled coders specialize in creating customized malware packages for a specific attack or attacker. This means that attackers are deploying malware that has never been seen in the wild, and therefore security vendors have not created signatures to detect it.

- **Advanced persistent threats (APT) signify a skilled and well-funded attacker.** While the term APT is used in many different ways, it generally means that the attacker has some type of sponsorship from organized cybercrime or a rogue nation state. The movement from "script kiddies" to APT is one of the most significant transitions in the history of the information security industry. These sophisticated attackers require the type of enhanced vigilance that comes from properly deployed NAV tools.

- **An increasing number of wide-ranging compliance initiatives require advanced reporting.** Most organizations are obligated to meet numerous different compliance objectives, such as PCI DSS or HIPAA/HITECH. Most auditors or assessors will demand reports that provide detail on internal user behaviors such as audit trails. NAV tools are uniquely positioned to provide this type of compliance information in an on-demand manner.

- **New government requirements that mandate continuous monitoring of security controls.** For example, NIST 800-37 is a risk management framework that mandates a function similar to NAV called "continuous monitoring."[16] While NIST is a set of recommendations for US federal government organizations only, it is common to find that private sector organizations adopt NIST recommendations as de facto standards. We anticipate that the NIST continuous monitoring recommendation will trickle down to enterprise policies, which will define another use case for NAV tools.

RECOMMENDATIONS

PUT YOUR HEAD ON A SWIVEL AND DEVELOP NETWORK SITUATIONAL AWARENESS

Just like a fighter pilot in a dogfight, today's information security professional must constantly scan the network looking for potential threats. Make no mistake about it: You have deadly enemies who can create havoc in your network if you don't see them. Make sure to put your head on a swivel so that you can see your enemies come out of the sun before they can get on your six. To help you get the networking site that you need and properly deploy your NAV tools, Forrester recommends that you:

- **Create a data acquisition network.** Inspecting and logging all network data can create a significant burden on current networks. This is why Forrester recommends creating a data acquisition network (DAN) to ease this burden and help automate SA functionality. To create a DAN, you must mirror or tap your various network segments so that they can be aggregated into a single feed that will become your DAN. While most switches can mirror traffic to a dedicated switch port, this is often ineffective because port density is at a premium and many networks cannot spare the ports to create a DAN. High-speed network taps that allow traffic to be split without a notable performance impact are readily available from vendors such as Gigamon, NetOptics, Datacom Systems, VSS Monitoring, and Network Critical. These purpose-built devices will facilitate DAN creation without interrupting mission-critical traffic.

- **Leverage NAV tools in your virtual SOC.** As part of an initiative known as SOC 2.0, Forrester is recommending the virtualization of security operation centers (VSOC). SIM tools have traditionally been the backbone of the security operations center (SOC), but NAV tools have the capacity to uplift security operations significantly. These tools have the capacity to use computer power to gain near real-time insight regarding an incident or attack that might take human analysts hours or days to solve. It is important that you integrate NAV tools into your VSOC workflows.

- **Anticipate the convergence of NAV and DLP.** NAV and data loss prevention (DLP) are looking at very similar information. Currently, DLP products are deployed at gateways or endpoints, but there is no reason that these functions cannot merge together into a single product. By adding regex pattern-matching to NAV tools, the DLP function can take place on the network instead of the edges. As the DLP lexicon within NAV tools matures, this may prove to be more effective, as the tools can discover data and sanitize it before it reaches the edges of the network. Companies such as Fidelis Security Systems have products that play in both the DLP and NAV markets.

- **Use data from you NAV deployment to justify a data classification project.** For many organizations, the visibility provided by their NAV tool will be the first time they have seen how much toxic data flows across their network. Forrester advocates a transformation from today's network-centric security to a future state that is data-centric. The first step in moving toward a data-centric model is to find and classify your data based upon its toxicity. Information gathered with NAV tools will be a motivational force in enterprisewide data classification initiatives.

SUPPLEMENTAL MATERIAL

Companies Interviewed For This Document

Arbor Networks

Fidelis Security Systems

Gigamon

HBGary

Lancope

LogRhythm

Lumeta

McAfee

Narus

NetOptics

NetScout

netWitness

Niksun

NitroSecurity

PacketMotion

Q1 Labs

Qosmos

Solera Networks

SolarWinds

Sourcefire

Trend Micro

Vitria

ENDNOTES

[1] The Zero Trust Model is introduced in the first report in this collection. See the September 14, 2010, “No More Chewy Centers: Introducing The Zero Trust Model Of Information Security” report.

[2] Forrester has created a reference architecture based upon the Zero Trust Model and discussed it in detail. See the November 5, 2010, “Build Security Into Your Network's DNA: The Zero Trust Network Architecture” report.

[3] Kevin Poulsen and Kim Zetter, “‘I Can't Believe What I'm Confessing to You’: The Wikileaks Chats,” *Wired*, June 10, 2010 (http://www.wired.com/threatlevel/2010/06/wikileaks-chat/)

[4] Source: Verizon RISK Team, “2010 Data Breach Investigations Report,” 2010 (http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf).

[5] Source: "Chinese National Pleads Guilty To Stealing Ford Trade Secrets," United States Attorney's Office, Eastern District of Michigan press release, November 17, 2010 (http://www.justice.gov/usao/mie/press/2010/2010-11-17_xyu.pdf).

[6] Source: Kevin Poulsen and Kim Zetter, "'I Can't Believe What I'm Confessing to You': The Wikileaks Chats" *Wired*, June 10, 2010 (http://www.wired.com/threatlevel/2010/06/wikileaks-chat/).

[7] Source: Verizon RISK Team, "2010 Data Breach Investigations Report," 2010 (http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf).

[8] For more information on the Philip Cummings case, see the September 14, 2010, "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security" report.

[9] Source: Verizon RISK Team, "2010 Data Breach Investigations Report," 2010 (http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf).

[10] NAV is not a product but a function. At its core, NAV defines an objective: the ability to have insight into all network traffic. Because of this, organizations will define multiple ways of achieving this objective. While Forrester looks at subsets of these tools to help our customers understand use cases and deployment options, many tools have overlapping features and functionality.

[11] Source: "Introduction to Cisco IOS NetFlow — A Technical Overview," Cisco (http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.html).

[12] Kevin Poulsen and Kim Zetter, "'I Can't Believe What I'm Confessing to You': The Wikileaks Chats," *Wired*, June 10, 2010 (http://www.wired.com/threatlevel/2010/06/wikileaks-chat/)

[13] Kevin Poulsen and Kim Zetter, "'I Can't Believe What I'm Confessing to You': The Wikileaks Chats," *Wired*, June 10, 2010 (http://www.wired.com/threatlevel/2010/06/wikileaks-chat/)

[14] Another version of the chat logs between Bradley Manning and Adrian Lamo is available. Source: Xeni Jardin, "Wikileaks: a somewhat less redacted version of the Lamo/Manning logs," *Boing Boing*, June 19, 2010 (http://boingboing.net/2010/06/19/wikileaks-a-somewhat.html).

[15] Source: Verizon RISK Team, "2010 Data Breach Investigations Report," 2010 (http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf).

[16] Source: National Institute of Standards and Technology, "Frequently Asked Questions: Continuous Monitoring," June 1, 2010 (http://csrc.nist.gov/groups/SMA/fisma/documents/faq-continuous-monitoring.pdf).

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®