A Custom Technology Adoption Profile Commissioned By IBM September 2013

Supporting The Zero Trust Model Of Information Security: The Important Role Of Today's Intrusion Prevention Systems

Introduction

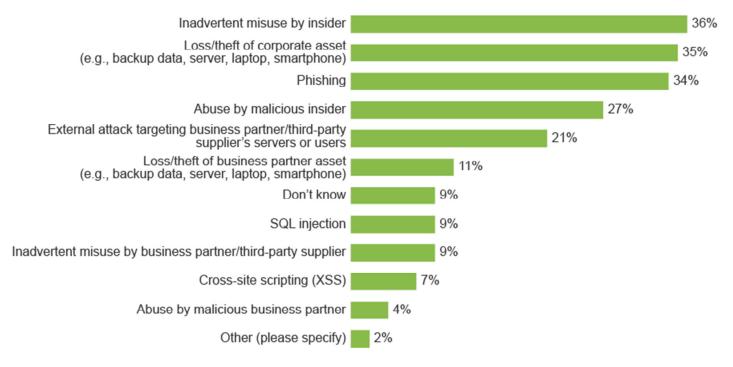
In today's new threat landscape, building a strong perimeter based on a hierarchical network design is no longer an effective approach to security. Notions of "trust but verify" are outdated and extremely vulnerable to a plethora of cyberattacks. Cybercriminals have found a multitude of ways to infiltrate the wall you have built, sometimes using malicious insiders in positions of trust in your network. According to the Forrsights Security Survey, Q2 2013, Forrester Research, Inc., inadvertent misuse by an insider is the most common cause of a security breach (36%), while abuse from a malicious insider accounts for 27% and external attacks on a business partner account for 21% of breaches (see Figure 1). US enterprise security professionals surveyed indicated that mobile device security and modern malware are the top perceived threats to the enterprise today. Insider abuse is also considered a dangerous threat, with a high number of respondents considering it to be the top threat that their organization faces today (see Figure 2).

Companies that are currently taking steps to shore-up their network security would benefit from adopting a model like Zero Trust and the next-generation tools for threat prevention that support it.

This IBM-commissioned profile of US enterprise IT security professionals evaluates the market's readiness for Zero Trust concepts and technologies, based on Forrester's own market data and a custom study of the same audience.

FIGURE 1 Security Breaches Can Occur In A Variety Of Ways

"What were the most common ways in which the breach(es) occurred in the past 12 months?"

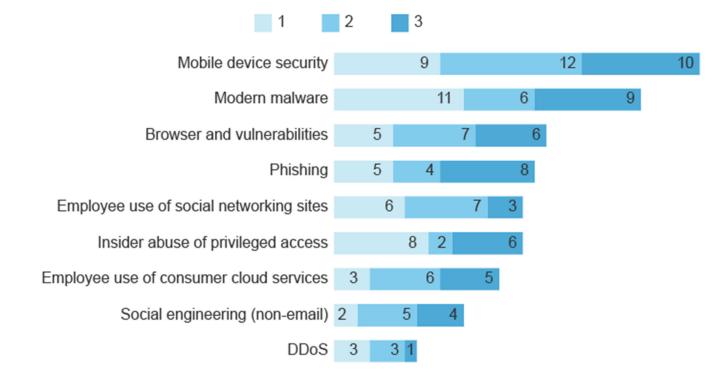


Base: 206 North American enterprise IT security decision-makers whohad a security breach in the past 12 months Source: Forrsights Security Survey, Q2 2013, Forrester Research, Inc.



FIGURE 2 Top Perceived Threats To Organizations Today Revolve Around Mobile And Malware

"What do you consider to be the top three threats to your organization today?"



Base: 52 US enterprise IT security professionals directly involved in purchasing, implementing, or managing intrusion prevention systems Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, July 2013

Introducing Forrester's Zero Trust Model Of Information Security

Forrester's Zero Trust Model of information security is a new approach to security that is needed today. The Zero Trust Model eliminates the idea of a trusted network (usually the internal network) and an untrusted network (external networks) to address both internal as well as external threats. In Zero Trust, networks are designed from the inside out in a modular, scalable way. This allows for the creation of pockets of protection throughout the organization. There are three main concepts to the Zero Trust Model:

1. All resources are securely accessed regardless of location. All traffic is treated as threat traffic until it is

verified that the traffic is authorized, inspected, and secured.

- 2. Strict least-privilege access control is mandatory. Properly implement and enforce access control to eliminate human temptation to access restricted resources. Look no further than the news to see the detrimental effects of poor access control in public data breaches perpetrated by individuals such as private first classBradley Manning or CIA contractor Edward Snowden.
- **3.** All network traffic is inspected and logged. Log and inspect all network traffic to gain network traffic visibility and verify that users are indeed doing the right thing, instead of simply trusting that they are doing the right thing.



Many Firms Today Are Already On The Path To Support Zero Trust

Respondents in our survey indicate that many have already adopted key Zero Trust concepts today, whether they are aware of Zero Trust or not. This is encouraging. Implementation of the Zero Trust Model then becomes less of a stretch for companies and more of an extension of the activities currently in place. Today, anywhere from 58% to 83% of respondents are already behaving in ways that support Zero Trust concepts, depending on activity (e.g., logging and inspecting all network traffic) (see Figure 3).

FIGURE 3

Many Respondents Are Already Performing ZeroTrust Activities Today

"For each of the activities below, please indicate what your organization is doing today"

We currently do this We plan to start doing this in the next 12 months	No plans to do this	Don	i't know/not sure
Use encrypted tunnels for accessing data on external networks		83%	13% 2%
Adopt a least-privilege strategy and strictly enforce access control to corporate resources	65%	19%	12% 4%
Log all internal network traffic	63%	21%	12% 4%
Inspect all internal network traffic	62%	21%	17%
Use encrypted tunnels for accessing data on internal networks	60%	21%	15% 4%
Focus more on security for the extended enterprise instead of security for our network perimeter	58%	;	35% 4%

Base: 52 US enterprise IT security professionals directly involved in purchasing, implementing, or managing intrusion prevention systems (percentages may not total 100 because of rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, July 2013

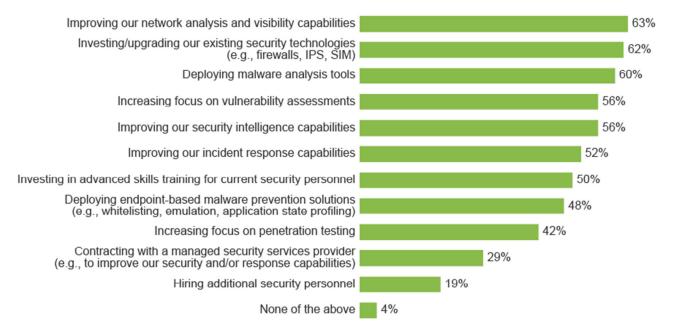
Organizations Are Beefing Up Technology Tools In Response To Critical Threats

When it comes to dealing with critical threats like advanced persistent threats (APTs), zero-day threats, and other unknown or custom threats, the top things that organizations are doing in response include investing in and upgrading their existing security technologies like firewall and intrusion prevention systems (IPS), improving network analysis and visibility (NAV) capabilities, and deploying malware analysis tools (see Figure 4). There is a greatly reduced focus on hiring more security professionals as a response to these types of malicious threats (19%) versus the focus on more technology-focused solutions. That's not to say that skilled staff is not important, but rather that these types of threats necessitate the capabilities provided via such tools.



FIGURE 4 Top Responses To APTs, Zero-Day Threats, And Unknown/Custom Threats

"What is your organization currently doing to detect and respond to advanced persistent threats (APTs), zero-day threats, and other unknown or custom threats against the organization today?"



Base: 52 US enterprise IT security professionals directly involved in purchasing, implementing, or managing intrusion prevention systems (multiple responses accepted)

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, July 2013

Today's Intrusion Prevention Systems Support Zero Trust

It's time to take a second look at updated requirements for key security technologies to effectively address today's threats. IPS is an example of an existing technology that has evolved to address a wider spectrum of security concerns— like providing visibility into what users are doing on the network—a best practice that supports Zero Trust concepts. IPS is a mature security technology today, with 59% of North American enterprises having already implemented or expanding their current IPS implementation today. Furthermore, an additional 20% have plans to implement IPS (see Figure 5).



FIGURE 5

IPS Technology Adoption, 2013 To 2014

"What are your firm's plans to adopt the following network security and security operations technologies?"

Expanding/upgrading implementation	ented, not expandi	ing	Planning to	implemer	nt in the next	12 months
Planning to implement in a year or more	Interested but no	plans	Not inter	rested	Don't kn	NOW
						2%
Wireless security	32%	%		42% 9	9 <mark>% 6% 6%</mark> ⊏29	4%
Network access control (NAC)	15%		46%	12% 9%	<mark>% 10% 6%</mark>	ó
Intrusion prevention system (IPS)	19%		40%	13% 7%	-4% 10% 7%	
Advanced malware detection capabilities embedded into existing security solutions	21%		33% 12%	6 11%	11% <mark>6%</mark>	
Virtualization-aware security technologies	18%	32	2% 15%	10%	13% 6% 7%	6
Security information management/security analytics	17%	32	% 13%	10% 12	2% 9% 7%	
Network analysis and visibility	12%	34%	13% 7%	6 18	3% 8% 8%	
Standalone advanced malware detection	12%	31%	11% 8%	17%	11% 10%	
Next-generation firewall	18%	22%	15% 11%	6 16%	% 8% 9%	
Unified threat management (UTM) appliance	12%	27%	17% 8%	15%	9% 11%	I
Base: 427 North American enterprise IT security decision-makers (percentages may not total 100 because of rounding)						

(percentages may not total 100 because of rounding)

Source: Forrsights Security Survey, Q2 2013, Forrester Research, Inc.

Today's IPS becomes an increasingly important tool for Zero Trust because of its visibility and alerting capabilities. Forrester's survey of 52 US enterprise IT security professionals directly involved in IPS decision-making shows that while most organizations are fairly confident in their ability to perform most common security activities today, they are least confident in the ability to detect a breach that is currently happening (see Figure 6). Knowing when you are in a breach state or about to enter one allows for timely and more proactive incident response. In addition, the ability to see how employees are accessing corporate resources and what they are accessing provides the necessary visibility for verifying access and behavior.

It is clear that legacy ways of protecting networks and the data flowing across them have proven to be ineffective. By adopting a Zero Trust approach to network security, companies can get the visibility they need to help prevent data breaches before they become newsworthy. The proper deployment of modern IPS controls can look deeply at traffic and the data it carries in order to help stop data breaches at their outset. Using IPS devices in a Zero Trust manner provides the traffic inspection necessary to properly enforce Zero Trust concepts and improve your overall security posture.



FIGURE 6

Many Organizations Feel Confident In Their Detection And Response Abilities

"How confident are you in your organization's ability to perform the following today?"

Very confident (5)	3 2	Not at all confident (1)	
Detect threats at the edge of our corporate network	29%	52%	15% 4%
Detect that a breach has already occurred	29%	50%	15% 6%
Detect vulnerabilities in our IT environment	25%	54%	19% 2%
Conduct a forensics investigation following a breach	29%	44%	23% 4%
See how employees are accessing corporate resources and what they are accessing	35%	37%	17% 10% 2%
See what types of third-party cloud applications employees are accessing	27%	40%	27% 2%
Detect that a breach is currently happening	27%	40%	27% 4%

Base: 52 US enterprise IT security professionals directly involved in purchasing, implementing, or managing intrusion prevention systems (percentages may not total 100 because of rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, July 2013

Methodology

This Technology Adoption Profile was commissioned by IBM. To create this profile, Forrester leveraged its Forrsights Security Survey, Q2 2013. Forrester Consulting supplemented this data with custom survey questions asked of US enterprise IT security professionals directly involved in purchasing, implementing, or managing IPS in their organization. The auxiliary custom survey was conducted in July 2013. For more information on Forrester's data panel and Tech Industry Consulting services, visit www.forrester.com.

ABOUT FORRESTER CONSULTING

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

© 2013, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester[®], Technographics[®], Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to www.forrester.com.1-MDUFDO

