

[Register](#)
[Login to your account](#)
Welcome Guest
[Advertise](#)
[About Us](#)

SECTIONS ▼



- [Authors](#)
- [Slideshows](#)
- [Video](#)
- [Reports](#)
- [White Papers](#)
- [Events](#)
- [Black Hat](#)
- [Attacks/Breaches](#)
- [App Sec](#)
- [Cloud](#)
- [Endpoint](#)
- [Mobile](#)
- [Perimeter](#)
- [Risk](#)
- [Operations](#)
- [Analytics](#)
- [Vulns/Threats](#)



- [Login to your account](#)
- [Register](#)
- [Login to your account](#)
- [Register](#)
- [About Us](#)
- [Advertise](#)



Search Dark Reading



- [Facebook](#)
- [Twitter](#)
- [LinkedIn](#)
- [Google+](#)
- [RSS](#)



CYLANCE

Millions of dollars saved
by preventing cyberattacks.*
*Source: Forrester

LEARN MORE

Symantec Endpoint Protection 14

LEARN
MORE

DARKReading

Join us live at

blackhat Interop **ITX**

Search Dark Reading



- [Analytics](#)
- [Attacks / Breaches](#)
- [App Sec](#)
- [Careers & People](#)
- [Cloud](#)
- [Endpoint](#)
- [IoT](#)
- [Mobile](#)
- [Operations](#)
- [Perimeter](#)

- [Threat Intelligence](#)
- [Vulns / Threats](#)

Attacks/Breaches



John Kindervag
Commentary

Connect Directly



5 comments

[Comment
Now](#)

[Login](#)



100%0%

[Tweet](#) [in](#) [Share](#) 827 [G+1](#) 25

'Zero Trust': The Way Forward in Cybersecurity

This approach to network design can cut the chance of a breach.

Data breaches are all over the news. Yahoo [admitted](#) that at least 500 million user accounts were affected by a 2014 cybersecurity breach. The 2016 election season was filled with revelations gleaned from stolen emails. The Justice Department, Internal Revenue Service, the US Navy, and Snapchat all suffered breaches in 2016. The list seems endless. Most significant, however, were the [2015 breaches of the Office of Personnel Management](#) (OPM), which experienced two separate cybersecurity incidents that resulted in stolen personnel files of almost 22 million people who had undergone background investigations.

While the technology and government sectors have endured arguably the largest breaches we've seen in recent history, other businesses aren't excluded from these security disasters. In fact, 15% of global businesses [estimate](#) their company's sensitive data was potentially compromised or breached over a 12-month period, according to Forrester data. This number may be low, however, as companies traditionally do not publicly report breaches if they can avoid it. Some breaches, such as at Target, get reported in the media and then the company must acknowledge the breach. Also, [new SEC rules](#) requiring a data breach report if the breach may have material impact on the stock price has revealed other breaches that might otherwise have flown under the radar. With breaches on the rise, how can today's security professionals transition from a reactive method of security to one that proactively identifies and eliminates threats?

In the wake of the OPM breach, the US House of Representatives Committee on Oversight and Government Reform issued a report containing a formal recommendation that federal agencies should adopt the Zero Trust Model of Cybersecurity, which centers on the belief that both internal and external networks cannot be trusted. "Zero Trust," a widely accepted term [originally coined by Forrester](#), is a data-centric network design that puts micro-perimeters around specific data or assets so that more-granular rules can be enforced. Zero Trust networks solve the "flat network" problem that helps attackers move undetected inside corporate networks so they can find and exfiltrate sensitive data. The shift to Zero Trust is applicable across all industries — from government to retail, healthcare, and everything in between. Here are five steps to get companies started on the path to Zero Trust.

1. **Identify Your Sensitive Data:** This may seem simple, but it's more challenging than you might think. It's impossible to protect data that you can't see. If you don't know where your enterprise stores data, who specifically uses it, how sensitive it is, or how employees, partners, and customers use it, then you're putting your organization

at risk. Before investing in security controls, companies must identify the data to protect. Once data is identified, it's necessary to make the data classification useful, and simplification is key.

2. **Map the Data Flows of Your Sensitive Data:** It's crucial to understand how data flows across the network and between users and resources. Engaging multiple stakeholders such as application and network architects to create a transaction flow map is important because they bring different information to the conversation. Additionally, security teams should streamline their flow diagrams by leveraging existing models. For example, the Payment Card Industry Data Security Standard requires organizations to create data flow diagrams to help them fully understand all cardholder data flows, and ensure that they're effective in securing the cardholder data environment.
3. **Architect Your Network:** The actual design of a Zero Trust network should be based on how transactions flow across a network and how users and applications access toxic data. With an optimized flow in mind, it's time to identify where microperimeters should be placed and segmented with physical or virtual appliances. For example, in a network where the compute environment is physical, the segmentation gateway usually will be physical as well. But if you've decided to adopt a highly virtualized compute environment, you may want to use a virtual segmentation gateway.
4. **Create Your Automated Rule Base:** Once the design team has determined the optimum traffic flow, the next step is to determine how to enforce access control and inspection policies at the segmentation gateway. One key principle of Zero Trust is that security pros must limit access on a need-to-know basis and strictly enforce this access control. To define these rules, the design team must have a detailed understanding of which users have access to which data. It's no longer enough to know the source address, destination address, port, and protocol. Security teams need to understand the asserted user identity as well as the application, which will often serve as a proxy for the data type in the modern segmentation gateway.
5. **Continuously Monitor the Ecosystem:** Another core tenet of the Zero Trust model is to log and inspect *all traffic*, not just external traffic, for both malicious activity and areas of improvement. In the old broken-trust model, traffic was logged only if it came primarily from the Internet and hit edge devices. The syslog protocol would then be used to capture information that would be analyzed in a security information management tool. However, that method doesn't provide enough context to make good security decisions — internal traffic must be held to the same standards. This is accomplished because a Zero Trust network is designed so that the segmentation gateway can send all of the data flowing through it, including traffic destined for both internal and external network segments, to a security analytics tool for closer inspection.

In today's threat landscape, skilled, well-funded, organized cybercriminals are constantly working to steal vital information from businesses. Where today's security approaches fail to protect data, Zero Trust is the best, most modern way to keep your network secure.

Related Content:

- [Ransomware Has Evolved, And Its Name Is Doxware](#)
- [Cyberrisk Through A Business Lens](#)
- [10 Things InfoSec Pros Can Celebrate About 2016](#)

John Kindervag is VP and principal analyst at Forrester, serving security and risk professionals. With more than 25 years of high tech experience, John is best known for creating the "Zero Trust" model of information security. He currently advises both public and private ... [View Full Bio](#)

[Comment](#) | [Email This](#) | [Print](#) | [RSS](#)

More Insights

Webcasts

[Cybersecurity] Costs, Risks, & Benefits

[Analytics] Make the Most of Your Data's Potential in 2017

More Webcasts

White Papers

Speed Up Incident Response & Discover Critical Attack Details

More White Papers
Reports

[Secure Application Development] New Best Practices
How Enterprises Are Attacking the IT Security Enterprise
More Reports



Sponsored Content

6 Requirements For Antivirus Replacement

Exploit kits obfuscate payloads when passing through the network, meaning you need protection on the endpoint. But antivirus isn't enough to prevent exploits. What should you look for in an antivirus replacement?

Sponsored By Palo Alto Networks



Sponsored Content

2016 Cyberthreat Defense Report

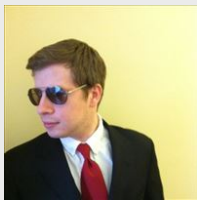
Download the 2016 Code42 CDR Executive Brief to gain insights:

- Why 62% of organizations expect to be breached this year
- Which cyberthreats concern organizations the most in 2016
 - The ineffectiveness of traditional endpoint security


Sponsored By Code42

Comments

Newest First | Oldest First | Threaded View



[Joe Stanganelli](#),
User Rank: Ninja
1/14/2017 | 2:44:11 PM

[Login](#)
 
50%50%

Nothing new except the name

This strategy is what top cybersecurity experts have recommended for years. Few listened.

The only difference now is that, as of sometime in the last year+, somebody came up with a catchy name ("Zero Trust") for it.

I guess buzzterms have their place.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)

[Shantaram](#),
User Rank: Strategist
1/13/2017 | 6:21:53 AM

[Login](#)
 
0% 100%



Re: [192.168.0.1](#)
Cool! i like it!

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[netwatcher](#),
User Rank: Apprentice
1/12/2017 | 3:25:21 PM

[Login](#)
 
50%50%

Re: Isn't this what we were supposed to be doing all along?
some reasons why...

- Executive is not aware of the risks – "We have a firewall and anti-virus so I think we are covered..."headinsand
- Executive has bad information – "Hackers only attack the big companies, what would they want from us?"
- Executive is a risk taker – "I'll take the risk, the probability for us getting attacked is low."
- Executive is cheap – "No ROI means no priority."
- Executive doesn't believe investment in security is worth it – "The loss involved will be so small compared to our revenues. It's easier to take a chance and write off any losses should they occur."
- Executive is overwhelmed by the size of the necessary investment required to add additional security measures – "We can't afford Fire Eye, IBM, HP, Palo Alto etc.. those tools are only affordable to the fortune 1000"
- Executive believes they are covered when they are not – "Our POS (or EMR) vendor is responsible for our security not us..."
- Executive doesn't believe any investment will have much of an impact – "Big companies have all the tools and they are still getting hacked."

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[ClarenceR927](#),
User Rank: Strategist
1/12/2017 | 9:10:58 AM

[Login](#)
 
100%0%



Isn't this what we were supposed to be doing all along?

Seriously, how far removed from the real world is IT/CISO management that this concept needs to be explained to them? This exact structure has been undersood and recommeneded for at least 25 years. The more important article would be one that examines the excuses, roadblocks and technical challenges that have prevented people from actually making it happen.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[DamnDesert](#),
User Rank: Apprentice
1/10/2017 | 10:47:06 PM

[Login](#)
 
50%50%

If only it were that simple

If it were just up to cybersecurity to get it done it would be so simple. I've spent 5 years trying to get the company I'm at to get such controls in place to government requirements SP-800-53 for a contract we have. In the end it takes executive buy in, available Capex/Opex budget, priority from other IT departments, and patience for needed downtime for many of the changes that need to take place. No small task, needed yes, getting people to understand it's a high priority is a whole other challenge.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[Subscribe to Newsletters](#)

[Live Events](#)

[Webinars](#)



Interop ITX - The Independent Conference for Tech Leaders

Attend the Leading Unified Comms & Collaboration Event

White Papers

- [Speed Up Incident Response & Discover Critical Attack Details](#)
- [\[IoT\] 4 Ways Predictive Maintenance Streamlines Manufacturing](#)
- [Gartner Research: Use SIEM for Targeted Attack Detection](#)
- [\[Data Center\] 5 Benefits of Having USB Ports on Your Rack PDUs](#)
- [\[Cybersecurity\] 5 Things Every Business Executive Should Know](#)

More White Papers



Video



[How To Find Hire The Best Threat Hunter](#)

All Videos

Cartoon



Backing Up the Internet of Things

[Post a Comment](#)

[Cartoon Archive](#)

Current Issue



Five Things Every Business Executive Should Know About Cybersecurity

Don't get lost in security's technical minutiae - a clearer picture of what's at stake can help align business imperatives with technology execution.

[Download This Issue!](#)

[Back Issues | Must Reads](#)

[Flash Poll](#)

What's missing from your incident response plan? (Pick all that apply.)

- ☐ Access to activity logs
- ☐ An up-to-date network diagram
- ☐ Blueprint for public disclosure

- ☐ Hostname-IP address maps
- ☐ IR fire drills before the event
- ☐ Plan for finding malicious files after the breach
- ☐ We don't have an incident response plan
- ☐ Other (Please explain in the comments)

Submit

All Polls

Reports

InformationWeek
DARKReading
reports

reports.informationweek.com

December 2016

Secure Application Development: New Best Practices

The transition from DevOps to SecDevOps is combining with the move toward cloud computing to create new challenges – and new opportunities – for the information security team.

Sponsored by CloudPassage



Secure Application Development - New Best Practices

The transition from DevOps to SecDevOps is combining with the move toward cloud computing to create new challenges - and new opportunities - for the information security team. Download this report, to learn about the new best practices for secure application development.

Download Now!

- Dark Reading Strategic Security Report: The Impact of Enterprise Data Breaches 0 comments
- The Top Cybersecurity Risks And How Enterprises Are Responding 0 comments



10 Cocktail Party Security Tips From The Experts

1 comments | [Read](#) | [Post a Comment](#)

What To Watch For With Ransomware: 2017 Edition

2

7 Ways To Fine-Tune Your Threat Intelligence Model

3

[More Slideshows](#)

Twitter Feed



divinereikitraining @juliefenn2012



The 7 Best Social Engineering Attacks Ever [darkreading.com/the-7-best-soc...](#) via [@DarkReading](#)



The 7 Best Social Engineering Attacks Ever
Seven reminders of why technology alone isn't enough to keep you secure.
[darkreading.com](#)



25s



Ercument B.Sumnulu @ErcumentSumnulu



Ransomware: How A Security Inconvenience Became The Industry's Most-Feared Vulnerability
[darkreading.com/endpoint/ranso...](#) via [@DarkReading](#)



Ransomware: How A Security Inconvenience Became The Industry's Most-Feared Vulnerability
There are all sorts of ways to curb ransomware, so why has it spread so successfully?
[darkreading.com](#)



1m



Enterprise Vulnerabilities From DHS/US-CERT's National Vulnerability Database

[CVE-2013-7445](#)

Published: 2015-10-15

The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated b...

[CVE-2015-4948](#)

Published: 2015-10-15

netstat in IBM AIX 5.3, 6.1, and 7.1 and VIOS 2.2.x, when a fibre channel adapter is used, allows local users to gain privileges via unspecified vectors.

[CVE-2015-5660](#)

Published: 2015-10-15

Cross-site request forgery (CSRF) vulnerability in eXtplorer before 2.1.8 allows remote attackers to hijack the authentication of arbitrary users for requests that execute PHP code.

[CVE-2015-6003](#)

Published: 2015-10-15

Directory traversal vulnerability in QNAP QTS before 4.1.4 build 0910 and 4.2.x before 4.2.0 RC2 build 0910, when AFP is enabled, allows remote attackers to read or write to arbitrary files by leveraging access to an OS X (1) user or (2) guest account.

[CVE-2015-6333](#)

Published: 2015-10-15

Cisco Application Policy Infrastructure Controller (APIC) 1.1j allows local users to gain privileges via vectors involving addition of an SSH key, aka Bug ID CSCuw46076.

Dark Reading Radio

Archived Dark Reading Radio

The Coolest Hacks of 2016

In past years, security researchers have discovered ways to hack cars, medical devices, automated teller machines, and many other targets. Dark Reading Executive Editor Kelly Jackson Higgins hosts researcher Samy Kamkar and Levi Gundert, vice president of threat intelligence at Recorded Future, to discuss some of 2016's most unusual and creative hacks by white hats, and what these new vulnerabilities might mean for the coming year.

[FULL SCHEDULE](#) | [ARCHIVED SHOWS](#)

[About Us](#)

[Twitter](#)

[Contact Us](#)

[Facebook](#)

[Customer Support](#)

[LinkedIn](#)

[Sitemap](#)

[Google+](#)

[Reprints](#)

[RSS](#)



Technology Group

Black Hat	Enterprise Connect	HDI	Network Computing
Content Marketing Institute	Fusion	ICMI	No Jitter
Content Marketing World	GDC	InformationWeek	VRDC
Dark Reading	Gamasutra	Interop ITX	

[Terms of Service](#) | [Privacy Statement](#)

COMMUNITIES SERVED

- Content Marketing
- Enterprise IT
- Enterprise Communications
- Game Development
- Information Security
- IT Services & Support

WORKING WITH US

- Advertising Contacts
- Event Calendar
- Tech Marketing
- Solutions
- Contact Us
- Licensing

Copyright © 2017 UBM, All rights reserved