August 5, 2011

Applying Zero Trust To The Extended Enterprise

Preparing Your Network For Any Device, Anywhere, Any Time

by John Kindervag
with Chenxi Wang, Ph.D., Stephanie Balaouras, and Lindsey Coit

EXECUTIVE SUMMARY

You are part of an extended enterprise — a new extended ecosystem of customers, clouds, service providers, partners, supply chains, and empowered users. The business expects you, the security professional, to somehow magically secure this ever-expanding universe despite budget restrictions and compliance pressures. This new reality will force security professionals to realign strategies in new and more efficient ways and discard many legacy world views. This is particularly true of network security. We can no longer control the perimeter, control the number of users that must access the network, or lock down the devices that connect to the network. We must take a fundamentally new approach to network and device security — we must take a data-centric approach, so that no matter where the data is, security travels with it.

THE EXTENDED ENTERPRISE POSES DRAMATIC NEW SECURITY CHALLENGES

Once upon a time, security and risk professionals had defined borders to protect — a limited and highly restricted user community — and a visible set of threats, such as worms and viruses. Today, our organization's functional network has extended well outside of our controllable borders. As we add new devices and connection options to our network, from smartphones to tablets, our potential attack surface has expanded well past the virus-infected laptop. And our users are beyond our control. Business partners, contractors, and user-owned devices make lockdown even harder. Known as the "extended enterprise," this new network is dynamic and organic.[1] It constantly shifts with the movement of users, the rise of new technologies, the inclusion of new partners and supply chains, and the advent of new attacks.

The infrastructure of the extended enterprise is in a state of continual flux. Devices and users come on and off the network unpredictably. IT-enabled business users can create new resources in mere moments thanks to virtual technologies, automation, and the abundance of cloud services. We must also prepare for the increasing sophistication and persistency of cyberattacks carried out by highly skilled, well-funded, and in some cases, state-sponsored, hackers.[2] Some of the key factors affecting security in the age of the extended enterprise include:

- **Mobility and device proliferation.** Many users now have two or three devices that must access corporate resources. The typical user has a corporate-issued laptop (and sometimes a desktop) as well as a smartphone and a tablet — all of which significantly expand the number of devices connected to the network. With an increasingly mobile workforce, device tracking and control

is not as simple as it was in the days when each user merely had a heavy workstation with an Ethernet cable plugged into the wall. This increase in device form factors and numbers leads to an inevitable increase in attack surfaces.

- **Greater dependency on business partners and service providers.** Before the advent of the Internet and collaborative technologies, large organizations built, in-house, all the technological capability and capacity that they needed. As networks became faster, it became easy to transfer large amounts of data quickly, and companies could outsource many of their technology needs to business partners and service providers. The extensive adoption of cloud and SaaS solutions is but an example. Outsourcing at this scale brings to light many security and compliance control questions, as the company must rely on the service partner to provide security controls.[3] As a recent Forrester report puts it: "The risks of cloud migration are largely captured in one word — 'security.' Half of the organizations that elect not to adopt cloud computing cite security as the reason."[4]

- **The loss of content control through Web 2.0 and social networking.** Content used to be difficult to create and disseminate. With the advent of Web 2.0 and social networking technologies, content creation and distribution can be as easy as the click of a button. Many of the tools necessary to create and share content are readily available and often free. Like it or not, your users are now empowered to use technology as they see fit. The content they see and share can be good or bad, malicious or safe, confidential or public. Policing and controlling content in a Web 2.0 world is a difficult proposition for the security professional.

YOU MUST TAKE A DATA-CENTRIC APPROACH TO SECURITY IN THE EXTENDED ENTERPRISE

Traditional security approaches have focused on protecting either the network itself or the user devices that access the network. Unfortunately, many currently deployed networks are notoriously hard to secure. This is because security was an afterthought and an overlay on the original network.[5] Security professionals still place most network security controls at the perimeter. But the traditional perimeter is no more. Public-facing websites expose a company's Internet presence to the entire world, while partner connectivity and extranets potentially open even more holes for an attacker to exploit. One global CIO recently told Forrester, "It's not fair. We have to protect against every vulnerability, but hackers just have to find one to exploit."

In an extended enterprise where your IT infrastructure changes frequently and assets (both external and those that you control) come together dynamically to deliver an enterprise function, one thing remains predictable — your data and the value it represents. Attackers rarely strike networks or users just for fun — they attack in order to steal data.[6] As a result, your strategy to protect your data needs to take on a data-centric view rather than focusing on infrastructure and device-level defenses.

Switch Your User Security Focus From The Device To Access And Behavior

Security professionals direct most of the user-focused security at ensuring that each endpoint is clean before they allow it on the network. This spotlight on pre-admission device control is the result of past fears that users with malware-infected machines would spread the malware across the network to other endpoints. Unfortunately, even users with clean machines account for a significant amount of cybercrime activity. To combat this, we must invert the model and not focus on who is on our networks but what they are doing on our networks. Therefore, we must focus on:

- **Providing more fine-grained access control.** We have recently speculated that network access control (NAC) functionality is important, but security professionals need access control that's much more role- and data-centric.[7] As this market evolves, vendors will embed NAC functionality into security software suites or into switching infrastructure.[8] The goal is to improve data security by restricting user access to data. The more restricted their access, the less likely users are to accidentally or maliciously leak data.

- **Monitor what users are doing on the network.** We've spun many cycles trying to let the good users on and keep the bad users off our networks. Unfortunately, it's impossible to determine good and bad intent by scanning a machine. Sure, we can get some insight into "clean" machines versus "infected" machines, but this is wasted effort. Malicious insiders take advantage of the old "trust but verify" model and steal important intellectual property (IP) with their "clean" machines. According to the 2011 Verizon Data Breach Investigations Report, ". . . insiders were at least three times more likely to steal IP than outsiders."[9] Having situational awareness and knowing what the traffic is doing is the first step to protecting your data and stopping users from doing bad things on your network.[10]

You Must Classify Your Data Before You Can Protect It

In the underground cybereconomy, certain data types such as credit card numbers or credit reports — which contain all the data necessary to steal an identity — have real dollar values that fluctuate up and down in a manner similar to the stock market. You must also worry about protecting intellectual property such as product road maps, designs, formulas, and sales strategies — information that is extremely valuable to competitors. You must also protect personally identifiable information (PII) and other regulated data. Forrester has generally defined "toxic data" as data that an enterprise is compelled to protect by legislation or by contract.[11] Understanding if your data has value to potential attackers or if you must protect it by regulation can help you more effectively plan controls. To protect your data you must:

- **Discover where all your data is located.** Data leaks and breaches often happen because users (both business and IT) have widely disseminated toxic data and security has lost track of its location. Before you can protect your data, you must inventory it. At the very least, you must inventory all your toxic data.

- **Classify your data according to value and "toxicity."** How is it possible to determine which data you should protect if you don't understand its value or toxicity? Data classification is the second fundamental step in creating a data-centric security organization. A data classification scheme must be simple and manageable, with a limit of three or four tiers. For example, "classified, internal and public" is a simple classification scheme. Anything more complex and you run the risk of users ignoring it or you fail to understand where to concentrate the deployment of specific security controls like data leak prevention (DLP) or encryption.

- **Consolidate your data, where possible, to make it easier to control.** A significant amount of toxic data is sitting on employee laptops and ad hoc databases throughout your enterprise. Once you've discovered and classified your data, a data consolidation project may be in order. Look at various data types — such as Social Security Numbers — and ask if all of the users who have that data stored in various places really should have access to it at all. Next, pull that data together and aggregate it into a more controllable environment while eliminating the ad hoc occurrences of the data. Finally, place controls around this consolidated data so that it doesn't proliferate in the future.

- **Encrypt or tokenize your data to eliminate its value to attackers.** Encrypting or tokenizing data is the future of data security. These technologies effectively "kill" data — making it useless to attackers.[12] Cybercriminals can't monetize tokenized or encrypted data. Plus, breached data that a security professional has tokenized or encrypted may not be subject to state or industry breach laws or regulations. For example, some states offer Safe Harbor if the breached data is encrypted. Many would agree, and there are theoretical evidences to back it up, that in the absence of the keys, encrypted data is not actually data at all. One precedent was set by California SB 1386, Section 2a, which clearly applies only to unencrypted data:

  > "Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[13]

USE ZERO TRUST PRINCIPLES TO CREATE A METHODOLOGY FOR DATA PROTECTION

The Zero Trust Model of information security simplifies how we conceptualize information security. It says that there are no longer "trusted" interfaces, applications, traffic, networks, or users. It takes the old model — "trust but verify" — and inverts it, since recent breaches have proven that when we trust, we don't verify.[14] By applying these principles to the extended enterprise, we can begin to create a robust plan for pervasively securing our data and consequently our users and networks. There are three simple ideas behind Zero Trust that we can adopt:

- **Ensure that all resources are accessed securely — regardless of location.** Clearly, there are many different types of users who need data access from an innumerable number of venues. Place is no longer important because of an ever-increasing mobile workforce. Whether they're inside or outside of the primary network, you must ensure that users will access data securely. To do this, security professionals will rely on more encrypted tunnels and real-time traffic inspection via network intrusion prevention systems (IPSes) or layer 7 firewalls.

- **Adopt a least-privilege strategy and strictly enforce access control.** When the company considers a user "trusted," it typically allows the user nearly free rein on a network. By adopting a posture of Zero Trust and applying granular data access control, a company limits the ability of unauthorized users to steal or reveal data that they don't need access to for their job function. In the future, expect security vendors to more closely intertwine NAC, identity and access management (IAM), and entitlement as they seek to create new and simpler methods of access control.

- **Inspect and log all traffic.** Data provided in the Verizon 2011 Data Breach Investigations Report shows that "good evidence of the breach usually exists in the victim's log files waiting to be used."[15] However, most companies don't know that they're in a breach state until a third party notifies them. To achieve the type of situational awareness necessary in the modern threat environment, security and risk professionals must inspect and log all traffic, both internal and external. This is done through a combination of threat mitigation controls such as firewalls and network IPSes, security information management (SIM) solutions, and network analysis and visibility (NAV) tools.[16] This combined approach will provide your organization with significant insight into the network traffic and the inherent potential threats that may be embedded in that traffic.

LOOK FOR OPPORTUNITIES TO SECURE INFRASTRUCTURE FOR THE EXTENDED ENTERPRISE

Every day, some type of change is happening on most networks. In fact, we're at the beginning of a global network refresh cycle. Drivers such as 10 GbE connectivity, virtualization, and IPv6 are causing network infrastructure professionals to re-evaluate their existing networks and often begin the network upgrade process. Zero Trust allows you to rethink network design in such a unique way that you can build security into your network's DNA.[17] One security professional inspired by Zero Trust recently said: "Zero-Trust helped us plug the holes and complete the architecture around a true data-and-user-centric operation."[18]

RECOMMENDATIONS

BUILDING SECURITY FOR THE EXTENDED ENTERPRISE REQUIRES ZERO TRUST

Each new trend in information technology — virtualization, VoIP, or cloud — seems to take the world of information security by surprise. Our brethren in other areas of the organization adopt new technologies, but we often remain stuck in the past and try to limit or inhibit that adoption. Well, the extended enterprise is coming and we can't stop it. Our old standby security methods will be ineffective with this new push. We won't be able to control users or devices, but we will certainly be able to control and protect our company's data if we so choose. Data-centric security requires new thinking, new paradigms, and new trust models. By adopting a posture of Zero Trust and coupling that with good data protection strategies we can go a long way toward mitigating the ever-changing threats against our data that we constantly face. More specifically, Forrester recommends that you:

- **Conduct a data discovery and classification project.** It's imperative that companies find, organize, and classify their data in this era of sophisticated cyberattacks, disappearing perimeters, and proliferating devices. Without these steps, data security is not possible.
- **Embrace encryption.** Encryption covers a multitude of sins. Unfortunately, many in the enterprise are afraid of encrypting data because they don't fully understand cryptography. Embrace encryption. There can be failures in many areas that open avenues of attack, but if you have encrypted data, it has no value to an attacker.
- **Deploy NAV tools to watch data flows and user behaviors.** The modern security professional must have situational awareness over the entire network in order to protect data from theft or misuse. Currently, most mature organizations have deployed firewalls, IPS, and SIM technologies to protect the perimeter, but the internal network remains wide open. One way to get situational awareness over the internal network is to deploy NAV tools so that you can proactively monitor the network for threats or malicious behavior.
- **Begin designing a Zero Trust network.** Many of our current security challenges are really network design issues. Our current networking design paradigms were created in an era before today's sophisticated security threats. Most network designers are infrastructure specialists with little security experience or awareness. In the future, you must embed security into the network fabric itself using the principles found in Zero Trust.

ENDNOTES

[1] The concept of an extended enterprise is defined in the forthcoming, "The Extended Enterprise: A Security Journey" report.

[2] The information security threat landscape is changing rapidly, and many security organizations are struggling to keep up with the changing nature, complexity, and scale of attacks. Not only is it important for security managers to keep up with this changing landscape and develop capabilities to handle this

new paradigm, but it is also essential to learn from past mistakes. Security managers must devise new ways to maximize the impact of their security controls, minimize risk, and efficiently deploy technology investments. For more information on changing threats, see the August 13, 2010, "The New Threat Landscape: Proceed With Caution" report.

[3] In an age when the consequences and potential costs of mistakes are rising fast for companies that handle confidential and private customer data, IT security professionals must develop better ways of evaluating the security and privacy practices of the cloud services. An effective assessment strategy must cover data protection, compliance, privacy, identity management, secure operations, and other related security and legal issues. The ultimate goal: Make the cloud service work like your own IT security department and find ways to secure and optimize your investments in the cloud. For a comprehensive look at security, privacy, and compliance issues with cloud outsourcing, see the May 8, 2009, "How Secure Is Your Cloud?" report.

[4] Concerns about security are the most prominent reasons that organizations cite for not adopting cloud services. Therefore, creating more comprehensive security capabilities is a prerequisite for getting organizations to adopt cloud-based services for more complex, business-sensitive, and demanding purposes. See the October 20, 2010, "Security And The Cloud" report.

[5] For a discussion on the flaws in current network designs from a security perspective, see the November 5, 2010, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture" report.

[6] Forrester has seen a "renaissance of high profile attacks perpetrated for political and ideological purposes." Source: Jonathan Penn, "Forget About Security's Impact On Business — What About Business' Impact On Security?" *Jonathan Penn's Blog For Vendor Strategy Professionals*, June 14, 2011 (http://blogs.forrester.com/jonathan_penn/11-06-14-forget_about_securitys_impact_on_business_what_about_business_impact_on_security_0).

[7] For a discussion on how fine-grained access control based on contextual information about an identity is a must-have for modern enterprises, see the June 27, 2011, "Your Data Protection Strategy Will Fail Without Strong Identity Context" report.

[8] See the June 15, 2011, "The Forrester Wave™: Network Access Control, Q2 2011" report.

[9] Source: Verizon 2011 Data Breach Investigations Report (DBIR) (http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf).

[10] For a discussion on a strategy to attain pervasive network intelligence and visibility, including continuous monitoring, pervasive data collection, and inspect and log all traffic, see the January 24, 2011, "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis and Visibility" report.

[11] Toxic data is "toxic" because it poisons the enterprise's air when spilled — in terms of press headlines, fines, and customer complaints. See the October 28, 2009, "Selecting Data Protection Technologies" report.

[12] For more information about the subject of tokenization, see the April 7, 2010, "Demystifying Tokenization And Transaction Encryption, Part 1: Get Ready To Place Some Bets" report.

[13] Source: California SB 1386 (http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html).

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

[15] Source: Verizon 2011 Data Breach Investigations Report (DBIR) (http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf).

[16] For an in-depth look at situational awareness and NAV, see the January 24, 2011, "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility" report.

[17] For more information about the Zero Trust network design principles, see the November 5, 2010, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture" report.

[18] Gianluca D'Antonio, CISO, FCC Group, quoted in *SC Magazine*. Source: Angela Moscaritolo, "Eliminating trust: The zero-trust model," *SC Magazine*, June 1, 2011 (http://www.scmagazineus.com/eliminating-trust-the-zero-trust-model/article/202672/).