

## *The Center is Everywhere*

*By Andreas Antonopoulos, Senior Vice President and Founding Partner, and John Burke, Principal Research Analyst*

### **Executive Summary**

*Changing work habits and data center technologies have destroyed the enterprise perimeter as traditionally conceived. End-node-centered security, both desktop- and server-centric, is one key part of defending the new enterprise. Network security addressing defense at every network port is another. Identity not related to network location can unify all security tools, providing the underpinning of policy-driven access control everywhere. The new center of enterprise IT security efforts everywhere – every device, connection, application, and user is the now at the center.*

---

### **The Issue: Perimeters Lost**

The very essence of “work” is changing. All across the world, but even more so in the U.S., society is changing the definitions of “work” and “office”. As communications and connectivity become more powerful and ever more widely available, work has become less and less a place and more an activity which takes place anywhere. In the last 4 years Nemertes Research has tracked the number of employees working away from their company headquarters. That number has gradually trended up, exceeding 90% in 2006. Today, branch office and mobile workers dominate, and knowledge workers are increasingly mobile, operating out of home offices, hotel rooms, airport lounges, coffee shops and taxis. As their work habits have changed through enabling communications technologies, they have in turn pushed adoption of those technologies by their companies: laptops, wireless Ethernet, smart phones, and web applications.

Large companies have gradually shifted more and more of their critical applications to the web. Through a web browser, the same application can be delivered to a desktop, a laptop, a phone, regardless of location, operating system

or (mostly) browser. This “webification” of applications has become a catalyst for further mobility and fluidity of the workforce.

But it is not just employees who have broken the barriers of an office and become mobile. Every business today is more integrated and interconnected to its partners, suppliers and customers. All these users also want—or require—access to applications from anywhere at anytime.

Just as trade and industry changed the landscape of Europe, trade in ideas and data is changing the landscape of the world. Walled medieval cities and their towers and moats became obsolete in a world of trade and commerce as trade and commerce became critical to the life of the cities. Similarly, a hardened enterprise network perimeter is a defense of the 90’s, hopelessly obsolete in a time of mobility, virtualization, and interconnectivity. As IT continues to grow in importance for the operations of all kinds and sizes of companies, the availability and reliability of core systems is ever more crucial. New applications and services can, increasingly, transform operations or customer interactions, but 67% of enterprises in Nemertes *Security and Information Protection* benchmark have rejected attractive and useful technologies because of security concerns around them. As companies extend their networks to support both information and physical supply chains, they have to poke holes through an increasingly porous security perimeter. At this time, with security more necessary than ever, it has become much more difficult to implement.

## **Systems-Centric Defense**

Perimeter-style defenses are not unnecessary, of course. They are simply not sufficient. With employees and contractors moving in and out of a perimeter and applications traversing the perimeter, the trusted internal network can no longer be trusted. A simplistic separation of “us” versus “them” and “inside” versus “outside” makes no sense. Instead, companies are increasingly treating the internal network as “wild”.

If the internal networks are untrusted then the next obvious place for security is within each network node. Each server, desktop, or laptop becomes a self-defending island in a sea of hostile packets. The systems-centric defense imbues each host with its own mini-perimeter. The host trusts only itself and treats all external communications as potentially suspect. The core of system-centric defense is a hardened operating system with a configuration that fulfills corporate policy. Each system that is deployed inside a company needs to be configured to resist attacks before it is ever connected to the network. The industry is now full of examples of systems being compromised within minutes of acquiring an IP address, even within presumably “trusted” networks.

System-centric defense of course goes beyond passive defense through configuration. Most operating systems today come pre-configured with at least rudimentary firewalls. Many companies install further protections such as anti-virus defenses, robust software firewalls and even host-based intrusion prevention systems.

In the traditional model we treated the corporate network like a big quarantine ward. The patients within had no immunities but they were protected

from the bugs outside. The problem with this model of course is maintaining the quarantine: if people keep walking in and out of the ward, eventually an outsider will sneeze and everyone dies. A more sensible approach is to help each patient develop their own immunity. They still need to avoid disease but they no longer have to live in a bubble. That is the essence of system-centric defense.

## **Network-Centric Defense**

Beyond system-centric defense, we also see the evolution of network-centric defense as a complementary strategy. While each system is given its own mini-perimeter or immune system, we also equip the network with additional defenses. Network-centric defense is more than just perimeter defense, however. Rather than looking just at the network ingress/egress routers, we treat every network port as a defense station.

Network-centric defense starts with admission of hosts to the network. This is the realm of Network Admission Control and goes beyond simple authentication. In Nemertes *Security and Information Protection* benchmark study, 60% of enterprises want to apply health checks upon admission to the network. In this scenario, before gaining full access to the network a host is first identified through a secure authentication mechanism. Then a series of policy and health verifications ensure that the hosts' defenses are operational and current and that no known problems exist. Only then is the host allowed to access any other network devices. Today, this form of network-centric defense is very rarely deployed—although 60% want it only about 14% currently do it—and it is more often found only in the context of a corporate VPN. A lack of solid interoperability standards for NAC and the high costs of internal deployments, have kept most companies from deploying such solutions across their networks.

Beyond admission, network-centric defense also involves the continuous behavioral monitoring of hosts on the network. A host is authenticated and then trusted, but its behavior is continuously examined – the security posture becomes “trust but verify”. Behavior analysis can be conducted with a variety of security devices: intrusion prevention, log monitoring, content inspection, anti-malware. For best results most companies invest in multiple technologies to cover a range of possible attacks. Think of that as “defense in breadth”. But instead of concentrating these defenses on the perimeter, looking outwards, companies need to deploy them in layers inside the network in multiple locations and multiple form-factors (hardware appliances, software, virtual appliances). Why is this different from perimeter-based defense? An in-depth network-centric defense is not looking only at threats originating outside the corporate network. Instead the defense is holistic, directed both inwards and outwards. The security mechanisms deployed in the company network are looking both for insider attacks and compromised systems or infected systems that have slipped past the perimeter defenses and are in the “inner sanctum”. In a medieval city, the walls kept bad elements outside so the guardians of the city could sit atop the walls pointing their weapons outwards. In a modern city we can't control all the ingress and egress points so we have distributed security: a police force that patrols the city looking for any threat that might arise. Similarly, modern interconnected

companies cannot maintain vigilance only towards external threats, but have to “patrol” their network with defenses layered in depth and breadth.

In addition to looking at behavior, most companies also segment their networks to provide compartmentalization of potential attacks. Using Virtual Local Area Networks, or VLANs, network administrators can restrict access to certain areas by controlling inter-VLAN traffic with firewalls. VLANs are cumbersome to manage and are likely to be superseded by other technologies, but the basic idea of compartmentalization will continue regardless of the underlying technology. A key disadvantage of current static segmentation technologies such as VLANs in the data center is that they work best in a fixed architecture with fixed server locations. With virtualization and dynamic virtual server migrations neither the architecture nor the servers remain fixed. Thus the need to look at other defenses to complement VLAN segmentation.

The network-centric defense is, of course, not restricted to servers. Desktops and laptops represent an even greater threat to the network because they involve the most unpredictable element in security: humans. If a server is prone to compromise upon its connection to the network, the risk for a desktop is at least tenfold because a user will initiate connections and visit websites which can inject malicious content into the operating system. Desktops therefore also need layered security, both system-centric and network-centric.

## **Identity-Centric Defense**

The fundamental unit of security in traditional security technologies is the IP address. It is the key component of an Access Control List tuple, it is used to define policies, access levels and (in combination with VLANs) segment the network into trust zones. The IP address is often seen as a unique system identifier, an identity token. This may have been true when desktops (workstations) weighed 30 pounds and connectivity was via an inch-thick coaxial cable. IP addresses served as a reasonable proxy for the user identity when they had a close one-to-one correspondence. But today, IP addresses are no longer adequate identifiers. Mobility, wireless systems, laptops, and smartphones (among other things) have created a network environment where IP addresses are constantly changing and the mapping of person to address is transitory. The foundational unit of security has become too fluid to be dependable. Instead, more fundamental forms of identity must be used as the foundation (root) of trust and policy. Hence we see strongly authenticated user identity gradually becoming the foundation for trust and policy decisions.

An identity-centric approach to security has three components. The first component is authentication. Strong authentication of user identity depends on a direct chain of trust to one or more authentication factors. An easy mnemonic for authentication factors is “something you have, something you know, something you are”. For example, a token is something you have, a password is something you know and a biometric is something you are. For authentication to be considered “strong” it must involve two or more authentication factors. In an identity-centric system, all users are considered untrusted until they have been strongly authenticated.

Once a user has been authenticated, they are “associated” with a set of authorizations based on policy. For example, a specific user may be associated with an authorization to access financial systems. Policies for users are most often based on role-based access to simplify management of the policies. A user may have multiple roles, both wide and narrow, associated with their identity. For example, a user may have a generic “company user” role and multiple specific roles like “financial auditor”, “customer service agent” etc. User-centric policies are mappings from users to roles to authorizations. The challenge with centralized identity-centric security system is that the identity and corresponding authorizations must be passed along with every user interaction to the various *policy enforcement points* which control access to systems, applications, services and even specific application components. Moreover, larger companies must share content with partners, suppliers and customers who come with their own identity tokens and trust levels. Hence the adoption of *federated identity* systems that allow the interoperability of distinct identity domains across a network.

## Conclusions

The erosion of a defensible network perimeter in the face of changing work habits and data center technologies has reshaped security thinking. End-node-centered security has taken on vast importance and both desktop- and server-centric tools are a key part of defending the enterprise. Network security has evolved to address every network port as a defensible position. Identity, not location, is growing to be the unifying thread for all security tools, providing the common currency required for robust, policy driven access control at all levels. In other words the new center of enterprise IT security efforts is now everywhere – every server and desktop, every network access point, every application and service, every user is the now at the center.

---

**About Nemertes Research:** Founded in 2002, Nemertes Research specializes in analyzing the business value of emerging technologies for IT executives, vendors, and venture capitalists. Recent and upcoming research includes Web services, security, IP telephony, collaboration technologies, and bandwidth optimization. For more information about the analyst, please contact Christine Zimmerman at [research@nemertes.com](mailto:research@nemertes.com).