Next-Generation Networks: Security for Today and Tomorrow

Securing today's threats on networks designed for yesterday's requirements leaves companies vulnerable.

The corporate computing environment is rapidly evolving in response to the consumerization of IT, mobility and cloud computing. These trends introduce new strategic business opportunities—as well as new risks and vulnerabilities. IT organizations must find a way to protect corporate assets while enabling the business to realize the value of these trends. This can be made more complicated than it needs to be when the IT organization is supporting a "good enough" network. This white paper looks at the implications of securing a low-capital-expenditure (CAPEX), good-enough-network against today's risks and how a next-generation network supports a more secure IT environment.

Yesterday's Network Security Model

Not too long ago, securing the IT environment was easier than it is today. Basic information such as users' locations, the applications they were running and the types of devices they were using were known variables. In addition, this information was fairly static, so security policies scaled reasonably well. Applications ran on dedicated servers in the data center. The IT organization controlled access to those applications and established boundaries to enforce security policies. Applications and endpoints were secured, and access to the network was restricted. The network's purpose was to connect users to IT resources in a client/server architecture, and—for the most part—the network experienced predictable traffic patterns.

Today, rapidly evolving computing trends are impacting network security in two major ways. First, they are changing the way the network is architected. The network edge has evolved as multiple diverse mobile devices connect to the corporate network from various locations. The applications themselves move as well—they are virtualized, and may move between servers or even data centers. At the same time, users are extending the corporate network by going to the cloud for collaborative applications like Dropbox or Google Docs. IT no longer knows which devices are connecting to the network or their location. The applications in use are no longer limited to what IT provides. Data isn't safely resting in the data center; it is traversing the country on smartphones and tablet PCs, and it is sitting beyond IT's reach, in the cloud.

A second trend impacting network security is the introduction of increasingly complex and sophisticated threats. Yesterday's networks were hit with broad-based attacks. Hackers would send, for example, 2 million spam emails that took advantage of a well-known risk or vulnerability, and count on a percentage of the recipients to open the email and succumb to the attack.

CUSTOM PUBLISHING FROM
CSO Custom Solutions Group

SPONSORED BY
CISCO

Any cost savings realized up front are quickly eroded, because good-enough networks lack integrated security. As a result, IT must address risks with multiple point solutions.

Now the attack model has turned around. Hackers no longer target a large number of individuals. They may not even go after a high-profile vulnerability. Instead, they carry out more complex, targeted attacks. Hackers may use social engineering to acquire information about the target and then exploit the trust that users have with an application or another user to install malware or steal data. These very targeted attacks are more likely than broad-based attacks to go undetected until long after the hacker has done some damage.

Securing the "Good-Enough" Network

Unfortunately, another development further complicates the IT organization's security efforts. Some analysts and vendors are encouraging IT organizations to view the network as a commodity; that is, any network will do, and IT organizations need only implement a good-enough network at the lowest acquisition cost. But any cost savings realized up front are quickly eroded, because these good-enough networks lack integrated security. As a result, IT must address risks with multiple point solutions—spending more time and effort deploying, configuring and managing the solutions. IT security can't keep up with, much less anticipate, security risks. Because the individual point solutions are not integrated, it can be difficult to enforce consistent security policies across the entire IT environment. From a defensive position, the more context IT has, the better equipped it is to stop a network attack. Having to correlate information from different systems to get that all-important context defeats the purpose.

A good-enough network with its many point solutions is an unstable network that creates a greater risk of downtime. Downtime can result from a security breach or from one of many systems breaking. When the network goes down, so does everything else, including revenue.

Modern Approach to Network Security

However, a good-enough network and its security implications aren't the only option. Innovations in network security have kept pace with rapidly evolving computing trends. A next-generation network takes into account tomorrow's technologies and is architected with integrated security capabilities for proactive protection against targeted, complex threats. It is this protection that enables the IT organization to proceed with confidence when pursuing strategic business opportunities like mobility and cloud computing.

A next-generation network delivers pervasive visibility and control with full context-awareness to provide security across the network, from headquarters to branch offices, for in-house employees and workers on wired, wireless or VPN devices. A networkwide policy architecture can create, distribute and monitor security rules based on a contextual language, such as who, what, where, when and how. Enforcement may include actions such as blocking access to data or devices, or initiating data encryption. For example, when an employee connects to the corporate network from a smartphone, the network identifies the device and the user, as well as the privileges granted them. The policy engine not only establishes policies for the device and user, but also shares these policies with all points on the network, and instantly updates information when a new device appears on the network.

Integrated, networkwide policies obviously facilitate the safe adoption of "bring your own device"[1] policies, but next-generation networks can also address security concerns related to cloud computing. With the flick of a switch across a widely distributed network, businesses can intelligently redirect Web traffic to enforce granular security and control policies.

[1] "Bring your own device" refers to a new trend where employees use personally owned devices like smartphones or tablets to access corporate resources.

With the implementation of a low-CAPEX network, IT organizations risk having to say "no" to new technologies or business ventures because the network is not capable of supporting them.

The Good-Enough vs. the Next-Generation Network

The next-generation network delivers much more beyond integrated security. A next-generation network is strategically developed to optimize for today's requirements and is architected to accommodate future technology disruptions while providing investment protection. In other words, a next-generation network is a dynamic network that supports trends around mobility, cloud computing and the changing threat landscape. It also transforms the network into a service-delivery mechanism that enables chief security officers to say "yes" to future strategic business efforts.

When calculating total cost of ownership (TCO), the CSO should be careful not to underestimate the business value to be gained from strategic opportunities. With the implementation of a low-CAPEX network, IT organizations risk having to say "no" to new technologies or business ventures because the network is not capable of supporting them. That means "no" to bring-your-own-device policies; "no" to expanding virtualization efforts to mission-critical business applications; "no" to cloud services; "no" to rich media. All of the cost savings, competitive advantage, productivity and agility benefits are lost because of a few dollars saved on the network. However, these same benefits can offset the total cost of a next-generation enterprise network.

Let's take a closer look and contrast how a low-cost or good-enough network differs from a next-generation, business-enabling network:

- **Purpose of the network:** A good-enough network has a single purpose: to connect a user to IT resources. This may have been acceptable in 2005 when your users sat at desktops that plugged into Ethernet ports. An enterprise next-generation network is a unified network consisting of wired, wireless and remote clients. It encompasses many devices, as well as building access and energy control. It can serve multiple purposes, including machine-to-machine connectivity, as may be required for new sensor networks or for data center backup applications.
- **Security:** In a good-enough network, security is bolted on. In other words, security consists of point products that don't integrate very well. A next-generation network integrates security capabilities from the premise to the cloud. Integration means less administrative overhead and fewer security gaps.
- **Application intelligence:** A good-enough network is application- and endpoint-ignorant. It operates on the notion that data is just data. A next-generation network is application- and endpoint-aware. It adjusts to the application being delivered and the endpoint device on which it appears.
- **Quality of Service:** Today's good-enough network is built on basic QoS standards, which can prove insufficient for video traffic and virtualized desktops. A next-generation network features media-aware controls to support voice and video integration.
- **Standards:** A good-enough network is standards based without concern for the future. A next-generation network not only supports current standards but drives innovations that lead to future standards.
- **Warranty:** Good-enough networks come with a form of limited support for maintenance and a warranty statement. Next-generation network providers offer a warranty, plus intelligent services with integrated management.
- **Acquisition cost:** Saving money on CAPEX can be more than offset by increases in OPEX if there are higher integration costs, more downtime or serious security breaches. While good-enough network vendors downplay these costs, next-generation network vendors promote a systems approach that not only reduces networking costs related to OPEX but also drives IT services improvements and new business opportunities, thereby increasing ROI.

Securing yesterday's network for the technologies of today is an uphill battle. To anticipate the risks and complex threats introduced by the consumerization of IT, mobility and cloud computing, IT needs a next-generation network on its side.

The Borderless Network Architecture

Cisco has positioned a framework for the next-generation network called the Borderless Network Architecture. This defines how the Cisco long-term vision is mapped out to deliver a new set of network services, to support the demands of the business and end users. These services enhance the ability of the organization to meet new and emerging requirements of users and IT. Intelligent network services are fundamental to driving down TCO and increasing IT's ability to deliver new business capabilities.

Cisco's goal is to build out systems and allow IT to spend less time at the bottom of the stack working on basic network integration, by providing a set of network services that enhance the ability of the network to meet the needs of the users and the business.

One key to the success of Cisco Borderless Networks is the Cisco SecureX Framework—a security system that spans from the endpoint to the cloud and provides policy and control at every hop in the network, as well as centralized management and integrated tools for preplanning, configuration, networkwide policy distribution and troubleshooting.

The Cisco SecureX Framework

Cisco SecureX blends the power of the Cisco network with context-aware security to protect today's organization no matter when, where or how people use the network. The Cisco SecureX Framework is built upon three foundational principles:

- **Context-aware policy** uses a simplified descriptive business language to define security policies based on five parameters: the person's identity, application in use, access device, location and time. These security policies help businesses provide more effective security and meet compliance objectives with greater operational efficiency and control.
- **Context-aware security enforcement** uses network and global intelligence to make enforcement decisions across the network and to deliver consistent, pervasive security anywhere in the organization. Flexible deployment options, such as integrated security services, stand-alone appliances or cloud-based security services drive protection closer to the user, reducing network load and increasing protection.
- **Network and global intelligence** provides deep insight into network activity and the global threat landscape for fast, accurate protection and policy enforcement:
  > Local intelligence from the Cisco network infrastructure takes context such as identity, device, posture, location and behavior to enforce access and data integrity policies.
  > Global intelligence from Cisco's global security footprint (Cisco Security Intelligence Operations–SIO) provides the full, up-to-date context and behavior of threats to enable real-time, accurate protection.

Cisco SecureX allows organizations to embrace mobility and cloud while protecting critical business assets. It delivers granular visibility and control, down to the user and device level, across the entire organization. For IT security organizations, this provides faster, more accurate protection from threats with end-to-end, always-on security and integrated global intelligence. The IT organization benefits with increased operational efficiency through simplified policies, integrated security options and automatic security enforcement.

Conclusion

Securing yesterday's network for the technologies of today is an uphill battle. In order to anticipate the risks and complex threats introduced by the consumerization of IT, mobility and cloud computing, IT needs a next-generation network on its side. Architected with pervasive, integrated security, a next-generation network makes it easier to enable the business while still maintaining the proper security posture needed for the mission-critical nature of today's IT systems. **Learn more at www.cisco.com/go/security.**