Your users have left the perimeter. Are you ready?

As roaming employees sidestep corporate VPNs, antivirus and other endpoint security solutions can't counter the resulting risks.

Executive Summary

Not long ago, even the most astute executives couldn't fully anticipate how quickly emerging technologies would transform their business operations — and even their business models. Laptops, smartphones, and other mobile devices; high-bandwidth wireless networks; and cloud-based computing services have proven to be among the most impactful of these advances, collectively untethering workers from office environments and fundamentally altering work behaviors. Employees today work anytime, anywhere while accessing applications and data that reside on company servers and in the cloud.

Despite this transformation, security tools and processes are still designed for more-controlled and static work environments; they fail to address some of the risks that accompany roaming workers and their evolving habits. Visibility is the foundation for security, yet security professionals are losing sight of their users once they leave the corporate network. The bottom line: Traditional controls such as firewalls, proxy servers, and anti-malware can identify and attempt to counter threats only after they hit the network perimeter or endpoints, opening the door for organizations to adopt a new approach to security.

In an ideal world, all communications to and from employees' corporate laptops would travel over secured virtual private networks (VPNs). The VPNs deliver traffic directly to the perimeter security systems for scrutiny and, if necessary, blocking and isolation.

In the real world, however, VPN usage can be a hit-or-miss proposition. One reason: Studies suggest that only a minority of organizations force their roaming workers to use VPNs. Equally important, a lot of corporate data now resides outside data centers in cloud-based services such as Office 365, Salesforce,and DocuSign.

The result, according to research firm and consultancy Gartner: "By 2018...25% of corporate data traffic will bypass perimeter security (up from 4% today) and flow directly from mobile devices to the cloud."1

Given this reality, organizations need a new, always-on security layer that provides protections that perimeter and endpoint security solutions can't deliver. To gain better insight into today's work practices and risks, IDG Research Services surveyed IT security decision-makers (ITSDMs) as well as end-users to gauge VPN usage. In addition to confirming that VPNs are regularly being bypassed, the survey revealed both agreements and discrepancies between IT security decision-makers and end-user perspectives when it came to VPN practices. It also identified several security capabilities that, if available, could prove extremely valuable in reducing the risk of off-network laptop usage.

Getting a handle on VPN practices

Not surprisingly, workers are indeed on the go. Nearly 60 percent of the IT security decision-makers said their laptop-toting employees use the devices away from the corporate physical network at least 50 percent of the time. End-users' self-reporting was similar, with 45 percent saying they did just that and 20 percent indicating that they roam 100 percent of the time.

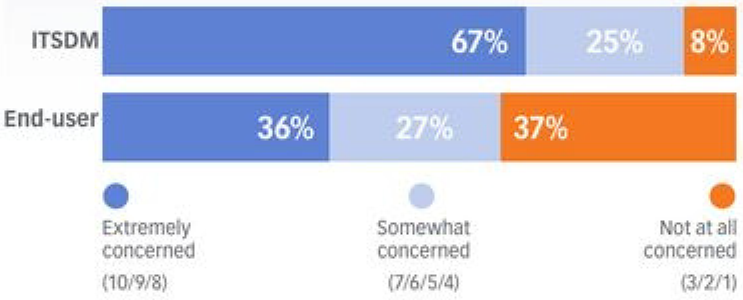
Most notably, 82 percent of the corporate laptop users admitted to sometimes bypassing their organizations' VPNs. Much of this off-network usage was for personal activities, but nearly 30 percent of the end users said they sometimes access company data without logging into their VPNs.

IT security decision-makers believe that the rates of non-VPN usage are even higher than the users reported, and these IT pros are well aware of the security risks this activity poses. When asked about the security of data stored on or communicated by offsite laptops, two-thirds of these decision-makers ranked their concern between 8 and 10 on a scale where10 was "extremely concerned" and 1 was "not concerned at all."

By contrast, as shown in Figure 1, only about one-third of the end-users ranked their level of concern in the 8-10 range, with an equal number saying that it fell to the bottom of the scale, with rankings in the 1–3 range.

FIGURE 1. LEVEL OF CONCERN ABOUT "OFF-NETWORK" LAPTOP USAGE

How concerned are you about the security of the data stored on, or passing to and from, your company-issued laptop when you're working away from your company's offices?



Off-network laptop usage is more than a theoretical risk. Indeed, 29 percent of the IT security decision-makers surveyed said one-quarter or more of their IT security issues can be traced to this particular practice. Predictably, the greater the percentage of off-network laptop users, the greater the negative security impact. At companies with 75 percent or more of off-network users, fully half of the IT security decision-makers said that one-quarter or more of their security issues are associated with this practice.

Reasons for avoiding VPNs

Given the risks of non-VPN communications and browsing, two obvious questions emerge. First, why don't organizations force corporate laptop users to log onto VPNs for internet access and other communications? Second, why do end-users, given the option, often go "off-network?".

Companies can configure corporate laptops to enforce VPN usage. However, only 16 percent of the end-users surveyed said they must log onto a VPN in order to access the internet with their work laptops. It's likely that many organizations simply don't want to impose security requirements that some employees may find onerous or an impediment to productivity. It may also be that a good number of organizations don't fully grasp all the risks if there is no visibility into malware threats.

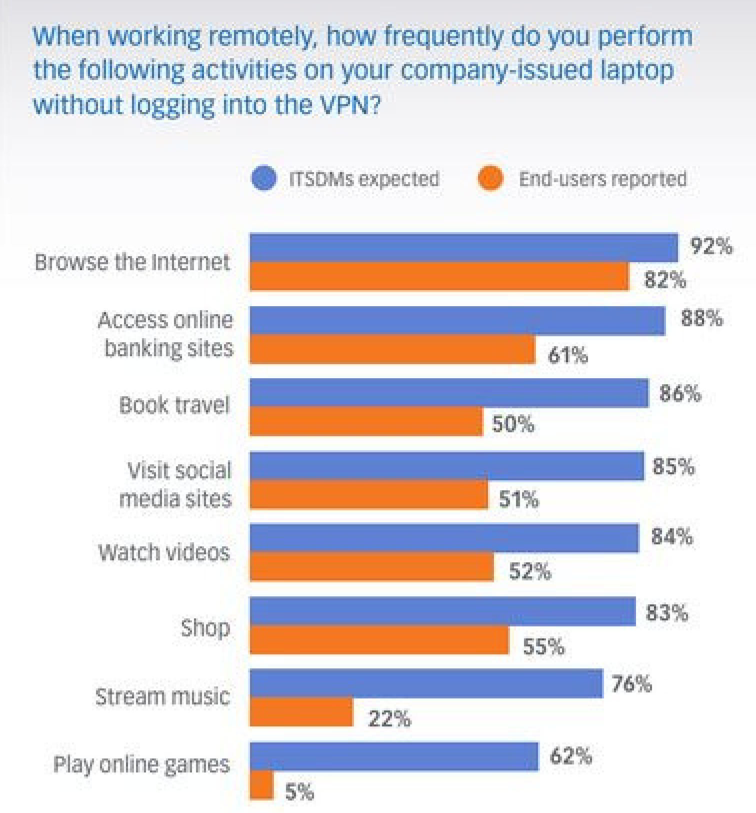
In terms of end-users, there is some evidence that VPNs are seen as annoyances rather than an important security measure. "I would rather not use the VPN, as it is slower," in the words of one end-user respondent.

Some end-users also avoid VPNs because they assume — often correctly — that their companies monitor networking activity when it occurs over the private networks. In fact, three-quarters of the IT security decision-makers said their organization does track VPN usage. Such concerns aside, the top explanation, cited by 58 percent of the end-users, was simply that "the VPN was not necessary to accomplish my task(s)." With increasing numbers of roaming users accessing cloud-based applications and data, it's easy to understand how a majority have little regard for VPNs.

So what are end-users doing when they access the internet without using a VPN? Here the perspectives of the IT security decision-makers and end-users were largely in line. Both groups, for example, identified browsing the internet as the top activity. As illustrated in Figure 2, however, there are some significant differences when it comes to IT security decision-makers' and end-users' perspectives about the frequency of various off-network activities.

For example, IT security decision-makers believe that end-users are performing several other risky activities at rates far higher than those the users admit to. This disparity is most notable in the areas of music streaming and game playing, with the IT security decision makers' frequency estimates more than 50 percent higher than the end-users'.

FIGURE 2. ESTIMATED FREQUENCY OF OFF-VPN NETWORK ACTIVITIES



Countering the risk of off-network laptop usage

Most companies may not be forcing the use of corporate VPNs, but the majority have deployed one or more security solutions in an attempt to protect those devices and the data they handle. By far the most common security measure is the installation of antivirus software and other endpoint security tools. More than 70 percent of the IT security decision makers said they use such laptop-based solutions. Others include everything from network-based tools to browser sandboxing. However, as noted earlier, the IT security decision-makers said a significant percentage of their security issues spring from off-network laptop usage. Clearly, then, their existing laptop security measures are falling short.

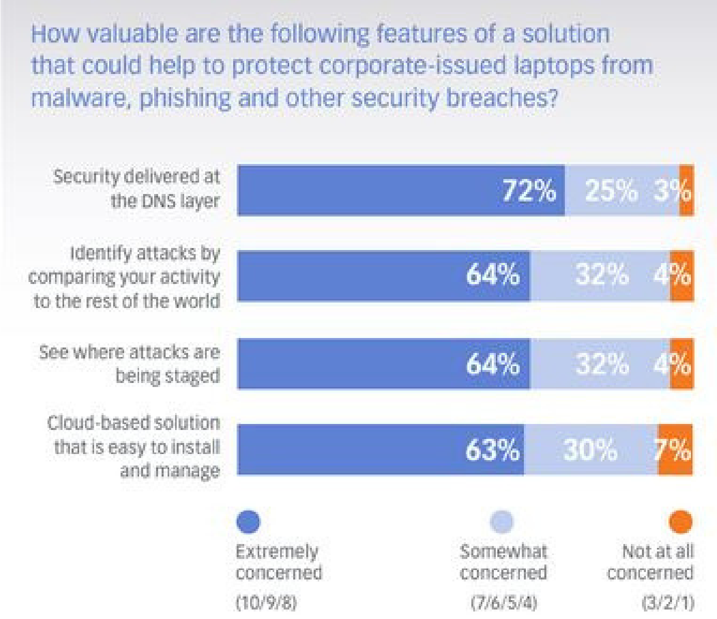
To help address these shortcomings, most IT security decision-makers agreed, several additional off-network security capabilities could prove extremely valuable, as shown in Figure 3.

The ability to implement DNS-layer security is valuable, because it can help organizations identify internet infrastructure and activities that are associated with attack staging and execution. For example, early phases of an attack often involve a redirect/link to a malicious web domain. Ideally, DNS-level protection would identify dangerous domains and traffic, blocking the download of a malicious file or preventing suspect IP connections from even being established.

Security at this layer can also foil the command-and-control call backs necessary to exfiltrate data from an organization's systems, by blocking the callbacks over any port or protocol. To accomplish these and other security tasks, a DNS-layer solution must be able to distinguish legitimate domains and actions from those that are known or suspected to be malicious. That includes the chance for broad and deep visibility into the internet to see where attacks are being staged.

The final "wish list" feature — to get these capabilities in a cloud-delivered service — reflects IT security decision makers' desire to avoid costly and complex on-premises deployments. Such deployments typically require long planning and deployment cycles and ongoing management overhead that can impose significant budget and time burdens — burdens that may be prohibitive. The bottom line: Organizations need to understand that their existing perimeter and endpoint-security controls (firewall, proxy, and antivirus) are not enough to protect a mobile workforce. Roaming users, cloud-based data, and off-VPN communications have changed the name of the security game. Only by adding a new layer of security that monitors threatening domains and activities across the internet can organizations confidently leverage the many benefits that come with modern technologies and flexible work practices.

FIGURE 3. VALUABLE SECURITY FEATURES FOR PROTECTING CORPORATE LAPTOPS



Delivering on the promise of DNS-layer security

Cisco Umbrella

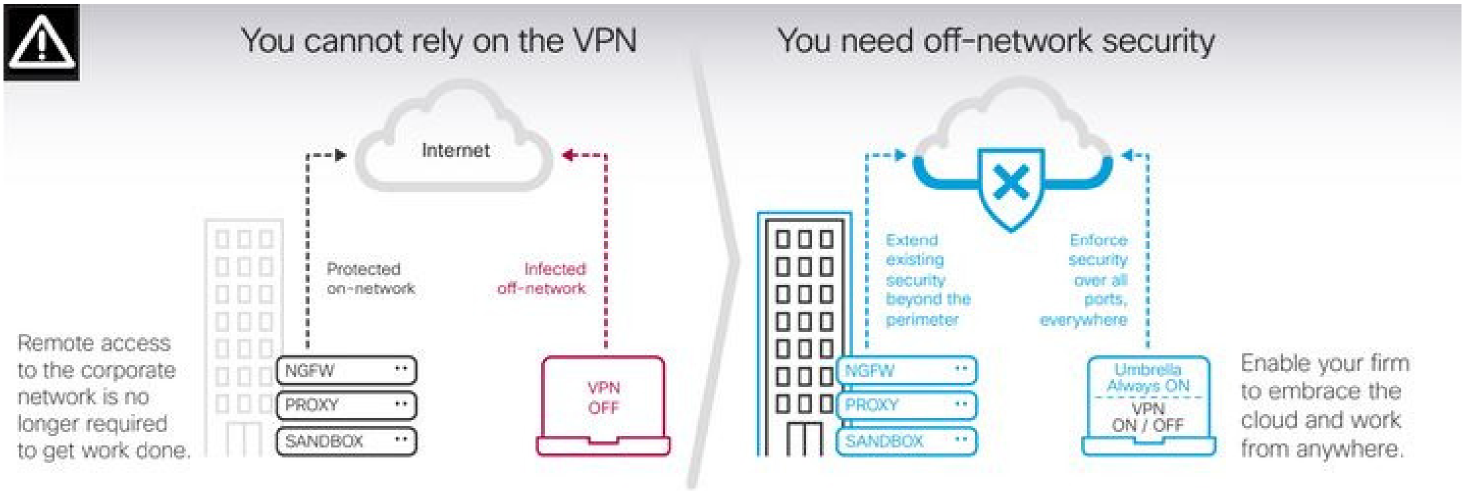
Cisco Umbrella fills the off-network security gap that exists in many organizations with remote and mobile workers. Umbrella enforces security at the DNS and IP layers, preventing malicious IP connections from being established or malware from being downloaded.

To accomplish these tasks, Umbrella leverages its customer base of more than 12,000 businesses and 65 million individual users. On any given day, the Cisco Umbrella network has visibility into about 80 billion requests and connections, tracking not just DNS domain names but also BGP routes, WHOIS records, IP geolocation, and other information. Each day, Umbrella discovers about three million new domain names and approximately 50,000 malicious locations or items. All told, Umbrella enforces about seven million malicious destinations at any given time. Umbrella provides a new layer of cloud-delivered protection in the network security stack, both on and off the corporate network. Umbrella prevents command-and-control callbacks, malware, and phishing over any port or protocol. And Umbrella provides DNS-layer network security for any device, regardless of location.

All the Umbrella identification and enforcement services reside in the cloud, running within the Cisco Umbrella global network of 25 data centers around the world. Internet requests and all other traffic from customers whose employees are working on corporate networks can be automatically directed to the Umbrella cloud service. And when roaming users fail to log onto their corporate VPNs, Cisco leverages a lightweight endpoint footprint that intercepts external DNS requests issued by the laptop and redirects them to Umbrella, a cloud security platform built into the foundation of the internet. The client software also adds a unique identifier so that Umbrella can identify which organization and which device each request comes from. As a result, Umbrella can apply the correct policy to each request and also create logs of individual laptop activity.

By intercepting and blocking dangerous requests and connections, Umbrella is typically able to reduce the number of security alerts that hit corporate perimeter security by a factor of 2 to 10. And, because it is offered as a cloud-delivered service, Umbrella requires no hardware to install or software to maintain. It's clear that corporate laptop users will continue to access the internet without using VPNs. It's also clear that this practice can negate the protections that perimeter security systems, antivirus clients, and other common security measures aim to provide. It is therefore critical that organizations not only understand the scope and potential consequences of off-network communications but also do everything possible to mitigate those risks.

Cisco Umbrella has established itself as an innovative and broadly adopted solution for providing off-network security protections.


You cannot rely on the VPN
Internet
Protected on-network
Infected off-network
Remote access to the corporate network is no longer required to get work done.
NGFW
PROXY
SANDBOX
VPN OFF
You need off-network security
Extend existing security beyond the perimeter
Enforce security over all ports, everywhere
NGFW
PROXY
SANDBOX
Umbrella Always ON
VPN ON / OFF
Enable your firm to embrace the cloud and work from anywhere.

Ready to try out this service?
Learn more about the Cisco Umbrella free trial at
resources.umbrella.com/ppov-free-trial-port53/