UMBRELLA

Mobility Whitepaper

7 Things You Need to Know to Secure Your Nomadic Workforce.

Why stopping 99% of threats across 50% of your users' devices just isn't enough.

Today, nomadic users are typically within range of a Wi-Fi hotspot 60% of the day. Over the next 5 years, Wi-Fi is expected to grow 4.5x. — ***[iPass, September 2012]***

322 business technology pros ranked using a VPN secure tunnel 1st out of 8 other solutions for securing data in transit. Beating by a wide margin secure HTTP, virtual desktop or secure email. — ***[InformationWeek, May 2012]***

The FBI recently warned of malware installed via hotel network connections. It followed a Bloomberg report claiming Chinese hackers stole private data from up to 760 firms by hacking into the iBahn broadband and entertainment service offered to guests of hotel chains such as Marriott International Inc. Forbes' reporter also recommends to users that all important data — including, but not limited to, emails, docs, IMs and web logins — is sent over secure HTTP or a VPN. — ***[Forbes, May 2012]***

210 Cloud Security Alliance members – most considered "experts in the field of information security" – were surveyed and 81% believe that unsecured Wi-Fi and rogue access points are already happening today. — ***[Cloud Security Alliance, Sept 2012]***

1

Face it: Your users are accessing company data over untrusted networks.

The ability for nomadic users to remain connected everywhere is approaching 100%. Yet, most users don't grasp that there's great risk associated with connecting to unsecured Wi-Fi networks. Many public hotspots have no security and can be easily compromised and fraudulent, computer-to-computer access points can be quickly setup to appear no less secure than other networks. In both environments, criminals can eavesdrop on communications or steal login credentials. Worse, many websites, Web protocols and non-Web apps that use file sharing or peer-to-peer protocols lack proper encryption to prevent data leaks during these increasingly frequent attacks.

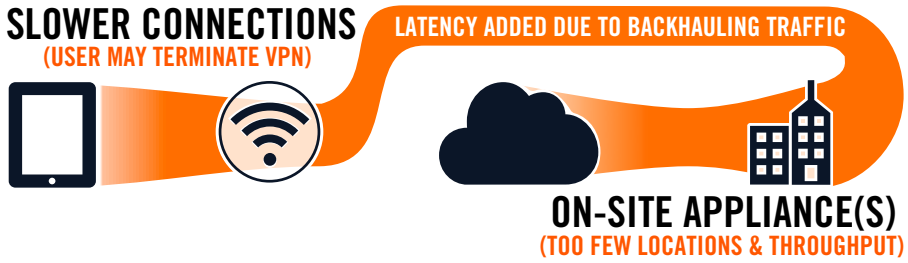
Current solutions may encrypt data stored on the device, but the protections don't extend to data communicated. Most solutions only encrypt app or protocol-specific communications, and are often complex for administrators to setup and nomadic workers to use.

In order to ensure private company data is protected when remote workers are accessing it, it's best to encrypt all communications, regardless of app, protocol or port. Only one solution achieves this: VPNs (Virtual Private Networks). Most VPN connections are simple to setup and transparent to the end user, but do your homework. Many solutions aren't compatible with mobile devices or require backhauling traffic that impacts performance.

2

Nomadic users won't sacrifice performance for security.

Most security vendors' VPN solutions require backhauling traffic from all devices to a security appliance that's installed behind the enterprise network perimeter. While effective in adding security, this approach also adds latency for the end user. Unfortunately, it isn't feasible for network admins to install appliances at every site on the globe in order to ensure the end-user experience is optimal.



The average mobile connection speed was 189 kbps in 2011. It will surpass 1 Mbps by 2014 and 2.9 Mbps by 2016.
*— **[Cisco, February 2012]***

Nomadic users are impatient with security that decreases Internet connection speeds, device battery life or usability. They're quick to disable or work around any perceived roadblocks. And traditional security solutions lack the sophistication to give admins visibility into user engagement, or worse, disengagement.

In conjunction with educating users on the importance of keeping security solutions in tact, network admins can do their part to optimize the end-user experience. A cloud-based solution is, by design, nearly infinitely scalable. Too, an effective Secure Cloud Gateway will leverage a globally-distributed network of always-on (or Anycast) data centers, ensuring very low latency. Ideally, a lightweight combination of DNS traffic routing and selective proxying should be used instead of only proxying Web traffic.

Today, 150 million user-owned smartphones and tablets are used in the enterprise. Or 23% of all such devices. And by 2014, it's expected to reach 350 million. —
[Juniper Research, Sept 2012]

3 Thanks to cloud computing, users access data anytime, anywhere — including outside your secure network.

The rise of cloud computing has put users squarely in the power seat. They can access the data and apps they need for work from smartphones, tablets and laptops. They no longer have any need to connect back to the private enterprise network. In the process, they've kicked out the pesky middleman — enterprise-grade security. Threats are becoming more advanced and persistent while at the same time it's becoming more essential for productivity that users be able to access Salesforce, Basecamp, Google Drive, Dropbox and other cloud-based apps.

In order to regain complete control, some admins may attempt to use single sign-on authentication or DLP solutions to enforce access and availability. Annoyed by the barrier it presents to their productivity, users often find a way to circumvent such methods.

Even with losing some control by embracing cloud computing, admins can still completely protect their data. Just like the ubiquitous connectivity nomadic users enjoy today, admins can provide users ubiquitous security by embracing a Secure Cloud Gateway, powered by a global network, and managed via a cloud-hosted console for centralized visibility and control.

150 North America Enterprise CIOs were asked about data leakage on the public cloud. Over 50% noted that they were "extremely worried. The top two causes for data leaks onto public clouds were BYOD and personal decision-making by employees. And top two biggest obstacles to stopping data from leaking onto public clouds is the perceived notion that there are no obvious options to protect data behind the corporate firewall. And the political and cultural dimensions where IT (the department) is unable to mandate policy for the business use of IT (the technology). —
[Mezeo Software, July 2012]

4 The BYOD nightmare: With no incentive to protect their personal devices, users make security a challenge.

BYOD presents a series of challenges to the network admin, not the least of which is Internet security. In addition to setting (and adhering to) guidelines for device management, IT admins must also negotiate boundaries between enabling employees to do their work and infringing upon their personal device sovereignty. Admins are further prevented from easily enabling security because employees

Today, the average person has 1.8 devices that connect to the Internet. By 2015, its expected to be 3.47, and by 2020, 6.58 devices per person. — ***[Cisco, May 2012]***

may not bring all the devices they use for work into the office for provisioning. So how can IT teams compel users to provision security on every device? And how can IT know whether users actually did?

Users' desire to maintain autonomy and IT managers' desire to maintain security sometimes conflict when it means partially locking the user out of their own devices. For example, they often try to restrict personal apps or force alternative, less compatible secure browser apps. But as the use of cloud computing increases, the effectiveness of this heavy-handed tactic is decreasing.

Users must be incentivized to install security on their devices, and the best way to do this is by making it easy and transparent. If the security solution adds value for the end user, and isn't disruptive to their productivity, they'll be more likely to install it. Too, the solution should give the network admin visibility into how and when it's being used. Keeping things simple is key. An IT-traceable process, for which user only needs to click 'OK' a few times is an admin's best bet. A solution should be selected that allows for notifications when the end user shuts it off.

36% of nomadic users admit to using workarounds to access corporate data on their smartphones and tablets. Those that do bypass their IT departments cited slow response times and strict policies as motivations. — ***[iPass, September 2012]***

5 Whether it's a user or IT-owned device, location matters when it comes to enforcing acceptable use policies.

The majority of 278 business technology pros responsible for personal mobile device use on their organization's networks enforced no restrictions or basic user agreements. — ***[InformationWeek, May 2012]***

In many ways the work-everywhere era also gives way to the work-anytime era. Users are checking email, accessing data, writing code and finalizing projects and presentations at all times of day, from wherever they work. But there's a flip side to this. Nomadic workers are also accessing the same devices they use for work for personal use. And while IT admins want to ensure ubiquitous security protection, enforcing acceptable use policies for accessing inappropriate or bandwidth-heavy content may not be warranted outside of the office.

Some solutions attempt to virtually split work and personal use environments on the device, but it is often complex for IT to setup, and difficult to compel users to allow it on their own devices. It also still doesn't prohibit the user from accessing the personal use environment while at work locations.

"Nearly 74 percent of workers globally would prefer an unconventional workday—being online and connected at any time, from any place they choose, throughout the day. Over two-thirds of survey respondents believe the ability to work remotely is either a necessity (62 percent) or a right (7 percent)."
. — ***[iPass, May 2012]***

A better solution is location-aware policy enforcement. This solution recognizes when devices are not behind network perimeters and turns off all or most content filtering, while still keeping security protections on. Most organizations find this balance between network security and user freedom to be an appealing and fair compromise.

946 security professionals at organizations with over 100 users were asked what their biggest IT security challenges were. First, was managing the complexity of security. Second, was enforcing security policies. ***[InformationWeek, May 2012]***

946 security professionals at organizations with over 100 users were asked if mobile devices pose a threat to your organization's security. 69% say it does, and 21% say it will. — ***[InformationWeek, May 2012]***

The majority of 322 business technology pros believe the primary responsibility for mobile security policy is a joint effort between security teams and business units. — ***[InformationWeek, May 2012]***

6 Workers use the same login credentials for both personal and company accounts, amplifying risk.

The number of accounts and passwords users must remember is overwhelming. Workers often seek to simplify their online presence by using the same password across all accounts. Through this process, they abandon security best practices. This poses a great threat to corporate security if users fall victim to clever phishing and spear phishing scams. User login credentials can also be stolen via botnet controllers or untrusted networks and distributed through criminal marketplaces. Cyber criminals are smart enough to try the same credentials to access cloud-hosted customer, accounting, HR, IT, project and other company data (e.g. salesforce.com, quickbooksonline.com, zendesk.com, basecamp.com, drive.google.com), or even data hosted internally on publicly accessible Intranets.

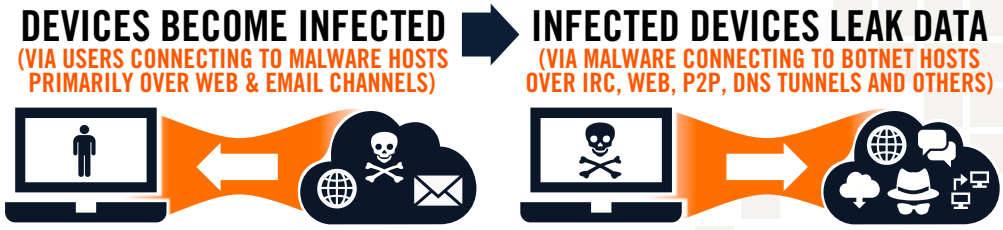
Some solutions attempt to consolidate enterprise accounts via secure single-sign on services with two-factor authentication. However, this adds complexity for IT teams to on-board or off-board new or past employees, and it adds complexity for users to access their accounts. End user education regarding the use of strong, secure passwords or bad Web links in emails is valuable. Yet, changing user behavior can take time.

A solution that counters these risks, while improving the performance and reliability of their devices' Internet connections, is a win-win. If every user device could not connect to phishing sites or botnet controllers and could encrypt all data over untrusted networks, credential theft risks would be countered.

7 Advanced threats aren't limited to email and websites, but Secure Web and Email Gateways are.

Nearly all IT teams have deployed Secure Email Gateways to prevent unwanted or phishing messages. Most IT teams have deployed Web Proxies (aka. Secure Web Gateways) or Firewall Filters (aka. Unified Threat Management) to prevent new infections via compromised or malicious sites. Yet data leaks are still making news headlines every day. One key cause of these data leaks is that hackers have figured out how to circumvent traditional security solutions by leveraging non Web and email protocols (e.g. P2P, IRC, DNS tunnels) and ports other than 25, 80 or 443 to leak data.

Network traffic assessments were conducted in 2,036 organizations worldwide between November 2011 and May 2012 by a firewall vendor. The vendor categorized 1,280 applications. Summarizing the assessments, 32% of applications did not use Web traffic ports (80 or 443) at all, and 26% were able to use dynamic or other non-Web ports to communicate over. — ***[Palo Alto Networks, June 2012]***



Some legacy security companies encourage IT teams to increase defense-in-depth strategies by layering on more protections to prevent infection. But we're not just living in a world of growing depth; we're living in a world of growing breadth. Stopping 99% or more of threats across only 50% of the attack surface is not an effective strategy.

A better solution is to use a Secure Cloud Gateway that enforces protection and policies regardless of application, protocol or port. Also, a solution that enables distributed enterprise networks, roaming laptops and mobile devices to connect through this Secure Cloud Gateway anywhere, anytime.

Sources Cited:

[iPass] http://bit.ly/Mobile-Workforce-Q3-Report and http://bit.ly/Mobile-Workforce-Q2-Report

[InformationWeek] http://bit.ly/2012-Mobile-Security-Report and http://bit.ly/Strategic-Security-Survey

[Forbes] http://bit.ly/FBI-Hotel-Networks

[Cisco] http://bit.ly/BYOD-User-Driven-Movement and http://bit.ly/Mobile-Data-Traffic-Forecast

[Juniper Research] http://bit.ly/Mobile-Incidents-Increase

[Mezeo Software] http://bit.ly/CIO-Mobility-Security-Survey

[Palo Alto Networks] http://bit.ly/App-Use-Risk-Report

Umbrella is brought to you by OpenDNS.

Trusted by millions around the world.

The easiest way to prevent malware and phishing attacks, contain botnets, and make your Internet faster and more reliable.

OpenDNS

OpenDNS, Inc. • www.umbrella.com • 1.877.811.2367

WP-7-Things-Secure-Nomadic-Workforce-v1.1