SELF-ASSESSMENT QUESTIONNAIRE
SECURITY OF REMOTE WORK SET-UP

SECURING YOUR REMOTE WORK ENVIRONMENT

IT organizations are under high pressure to enable remote work to meet the COVID-19 response mandates. In addition to delivering the functionality and capacity, it is important to ensure these solutions are secure, as the exposure to remote workers will be vastly increased.

The questionnaire below will help you to think about how to deliver remote access securely.

ILLUMANT CONTACT INFORMATION:

650-961-5911
info@illumant.com

ARE YOU READY TO DELIVER REMOTE WORK?

The first question ***is***:

Are you ready to deliver sufficient remote access? VPN? Remote desktop management?
If you don't have sufficient remote access capacity, it may be time to provision it. Note that if you do not have sufficient capacity, you maybe vulnerable to organic denial-of-service (ODOS) – too many users at once. And if you don't have remote administration capabilities, achieving your security (and operational) objectives will be hampered.

SECURITY SELF-ASSESSMENT

Once you have, or plan to have, remote access, consider the following questions to help you think about how best to secure your remote-work environment.

1. **CRITICAL: Password Complexity – Do all users have complex passwords (12+ characters, upper and lower case, number and symbol, not related to common passphrases)?**

   Password guessing is a common attack vector against VPN access. High-complexity passwords are often harder to guess unless they follow common patters, or use variants of dictionary words. Tools exist that can check for guessable complex passwords.

2. **CRITICAL: Brute-force Protection – Do you have measures in place to limit authentication attempts?**

   Brute-forcing is a common technique to gain access to accounts by trying sequences of logins and passwords – often using automated tools. Consider rate limiting attempts by IP and by user, and locking out accounts after a set number of tries. (But also remember, resetting locked accounts can be labor intensive. Consider secure self-service password reset and/or automatic account reinstatement after a longer delays.)

3. **CRITICAL: Endpoint protection – Do you have strong endpoint protection solutions? Are they installed on all user endpoints? Are they up to date?**

   Strong endpoint protection can help against malware delivered through phishing, downloads, and other delivery mechanisms, e.g. USBs. Note that out-of-date AV can present serious vulnerabilities by themselves. This is parti

4. **CRITICAL Two-factor Authentication – Do you have 2FA on VPN endpoints, email inboxes, and/or any other publicly accessible infrastructure?**

   2-factor Authentication (2FA) is a more efficient way to protect against brute-forcing, password guessing, and other access control security issues (e.g. stolen passwords). You can go a long way to improve security without it, but it is also a modern-day must for strong security.

5. **CRITICAL: Physical Security – Do you have physical security to protect offices while users are remote?**

   Unattended and insecure facilities and offices are more prone to physical intrusion. Once on premises, besides access to sensitive paper documents, an attacker can have access to network ports and unattended systems, which can be used to propagate attacks. This is particularly important if physically connecting to a network is sufficient for network access (see below).

6. **CRITICAL: BYOD – Do you allow personally owned and controlled computers/devices to connect to your network? If so, how do you ensure they are secure?**

   Home computers and personal devices are often not secured to your corporate standards. If you will allow home computers, you will need to take control of them with strong endpoint protection and MDM solutions. Consider virtual desktops with built-in security measures to mitigate the risk of insecure personal devices.

7. **HIGH: Network Access Control – Do you have network access control to limit access to Ethernet ports?**

   Network Access Control (NAC) provides a mechanism to prevent systems that do not have a valid certificate from gaining access to organizational networks. This prevents and attacker from plugging in a system into a physical network and launching attacks. There are variants that compare devices to a known table of MAC addresses, although better than nothing this is weak, because MAC addresses can be spoofed. A better option is to use installed certificates. Note: NAC is particularly important if offices are left unattended.

8. **HIGH: Updates – Do you update workstations regularly?**

   Workstations are at higher risk of compromise when new updates are not installed regularly.

9. **HIGH: No Local-Admin Privileges for Users – Do users have local administrator rights on their workstations?**

   A user with local administrator rights is more likely to install malware by accident, or install vulnerable software, which in turn attackers could use to turn off endpoint protection and hijack VPN connections to pivot to an internal LAN. Of course, if you don't have reasonable remote system administration in place, it will be hard to support users administrative needs.

10. **HIGH: Social Engineering Awareness – Do you have ongoing cyber security awareness training for your employees?**

    COVID-19 phishing emails are on the rise, and it is more important than ever to make sure your employees know how to identify phishing emails.

11. **HIGH: Inactivity Timeouts – Do you have inactivity timeouts on laptop/desktops, VPN, and applications?**

    With employees working remotely, physical security is less controlled, which puts emphasis on logical controls. Inactivity timeouts give some protection against workers leaving their desktops or laptops unattended.

12. **MEDIUM: Segmentation – Do you have role-based or user-based segmentation network and application access for VPN users?**

    Segmentation of access for VPN users can help to limit the potential threat of hijacked VPN access.

13. **MEDIUM: Wireless Security – Do you have robust wireless security?**

    If wireless access is not needed while workers are remote, it is better to turn it off. One less attack surface to worry about.

14. **MEDIUM: Trusted WiFi – Are your users connecting to critical devices from an untrusted WiFi?**

    Connecting to public or untrusted networks opens up the possibility for your users falling victims of Man-In-The-Middle attacks. Make sure you have trusted certificates on your VPNs and any remote access systems, and ensure that users are trained not to connect if they are warned about insecure certificates.

15. **MEDIUM: Active Monitoring – Do you have proper monitoring in place for all workstations, critical servers, and network traffic between them? SIEM, IDS, IPS, etc.**

    Paying extra attention to remote employee sessions is critical to ensuring no accounts have been compromised.

"NO" answers to any of the critical questions above should be addressed immediately. The highs deserve attention as soon as criticals are addressed, to the extent resources allow. The mediums are sound practices that can help reduce overall vulnerability.

It is essential to have a remote work option for the restrictions we are facing, but security must not be ignored.

If you would like to talk with us about any of these concerns … Email us at **info@illumant.com**, or give us a call on **650-961-5911**.

illumant

> *"We were very pleased with Illumant's management of our security project and the outcomes. Outstanding team to work with and HIGHLY skilled and knowledgeable. Would use them again in an instant."*
>
> *– Marta Williams, Joint Tech Team Lead, Central Health, Austin, Texas*

DIFFERENTIATED THROUGH EXPERTISE, VETTED BY EXPERIENCE:

We're one of the best – We are not just making this up. Our clients often tell us that we're the best pen-testing firm they've worked with. And we have some great clients.

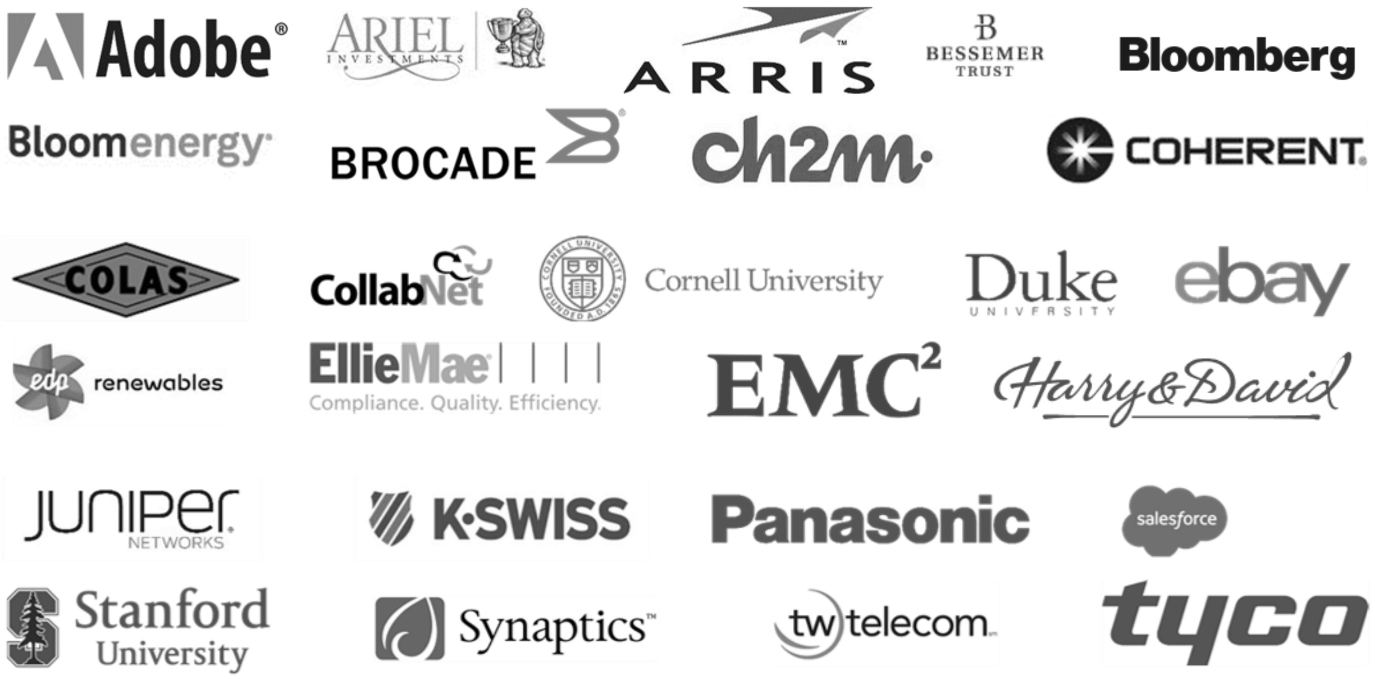
Hall of fame bug hunters – Became 1st ranked on Alibaba's Bug Bounty Hall of Fame for 2018 after only a month: Alibaba Bug Bounty Hall of Fame 2018 (or go to www.illumant.com/blog/ and find Alibaba entry).

Awesome deliverables – We take a lot of pride in our reporting. Our reports are super informative and look great – and following our recommendations improves your security.

Zero-days – We don't just find the vulnerabilities that everyone already knows about, we find new and undiscovered vulnerabilities as well – meaning with us you are ahead of the hackers. Check out our latest, here: www.owndigo.com.

Friendly, expert hackers – We have some of the top hacking talent around, with the best skills and certifications, as well (OSCE, OSCP, GPEN, etc.) But we're not just great at hacking, our people our great at presenting and discussing, too.

Great clients – here are a few:



For more information go to **www.illumant.com**, email us at **info@illumant.com**, or give us a call on **650-961-5911**.

illumant

Illumant | Security Assessments and Compliance
431 Florence Street, Suite 210, Palo Alto, CA 94301
Tel. 650.961.5911 | Fax. 650.961.5912
www.illumant.com
info@illumant.com