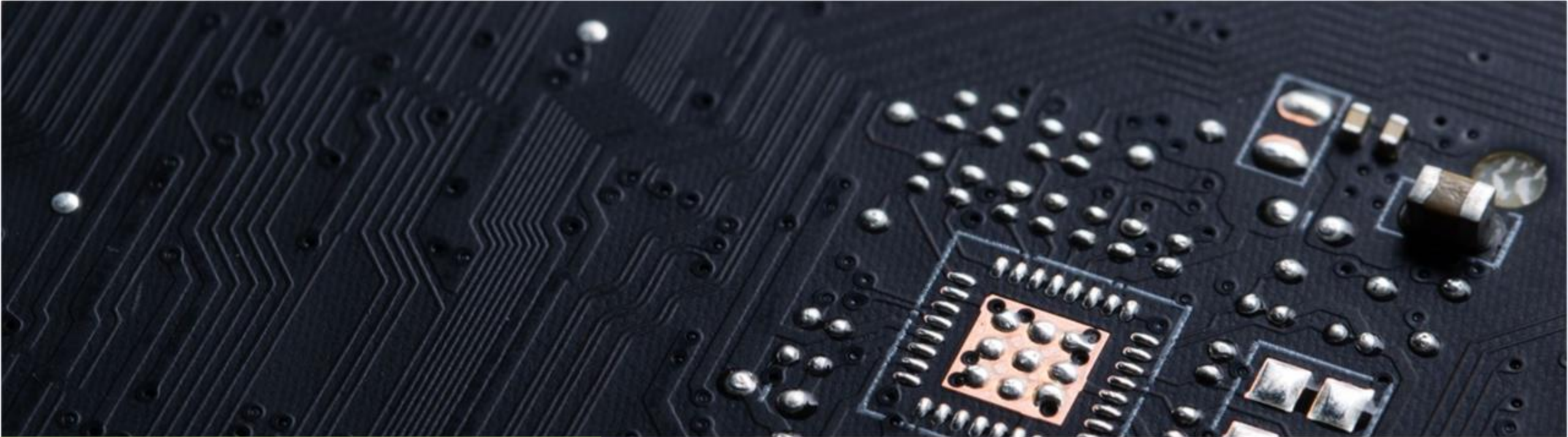




Quest Technology Management

Cybersecurity Checkup Program

Presenter:

Date:



Keeping Hackers at Bay with Critical Cybersecurity Checkups

It is imperative to take a proactive stance in protecting yourself by conducting more frequent checkups and making this an essential part of your overall cybersecurity plan.

- Our Cybersecurity Checkup Program that is designed to review configuration and adjustments to your critical security systems and flows.
- These checkups allow for experts to do a review of your configuration and provide recommendations for improving your security operations.
- Our Cybersecurity Checkup Program includes a series of **7 individual Cybersecurity Checkups** that have been developed to help in each critical flow that threat actors consistently attack.
- Checkups can be ordered individually or bundled for increased cybersecurity protection to provide maximum flexibility to meet the specific needs of your organization.

Cybersecurity Checkup Overview

Maintain your organization's surveillance and protection with these 7 checkups.

1 Email Security Flow

- The importance of securing your email has never been more important than now and should be a high priority process.
- With the changes in rules, ratings, and attacks, checking your email flow, and email anti-malware settings once every six months will ensure you are keeping up with the latest configurations and processes to minimize email attacks.
- Quest's Email Security Flow Checkup will also let you know your email protection rating with your tools and email systems such as Microsoft 0365.

2 Patching

- Gaps in patching have been a threat bad actors have been easily exploiting for years; however, keeping up with patching has been incredibly difficult to complete for most organizations.
- The growth of threats with every application and operating systems have been exponential.
- Having a Patch Management Checkup once every six months will allow your team to review their process, effectiveness, and help close any gaps before it is too late.

Cybersecurity Checkup Overview

Maintain your organization's surveillance and protection with these 7 checkups.

3 Endpoint Protection

- Endpoint protection is a checkup that allows Quest security experts to see into the effectiveness of your desktop and server antivirus tools.
- Our Endpoint Protection Checkup allows you to review your policy that could impact the tool from being effective and review options to improve your security posture.
- It is critical for our organization to completely understand what is being blocked versus monitored and how the tool you've implemented will report a threat.

4 Backups

- System backups have been a common IT practice for many years; however, these days it is imperative to have a highly proactive backup process with the understanding of its effectiveness against ransomware.
- These days, organizations not only need to have an off-site copy, but they also need an immutable copy. This is extremely critical — effective backup systems help protect against ransomware.
- Quest's Backup Checkup will allow your team to have a second set of eyes to review your current backup process and provide guidance.

Cybersecurity Checkup Overview

Maintain your organization's surveillance and protection with these 7 checkups.

5 [VPN, MFA, SSO](#)

- Having secure remote access is essential.
- For all organizations. Remote access, BYOD, work from home, and third-party access are services all companies provide to their business users.
- But with every access comes another vulnerability:
 - Because these services are constantly changing within your organization, a review of your process and systems every six months is vital.
 - Quest's Remote Access Checkup provides your organization a second set of eyes as new requirements come into your company, a check for security threats as well as provided recommendations.

6 [DNS Protection/URL Filtering](#)

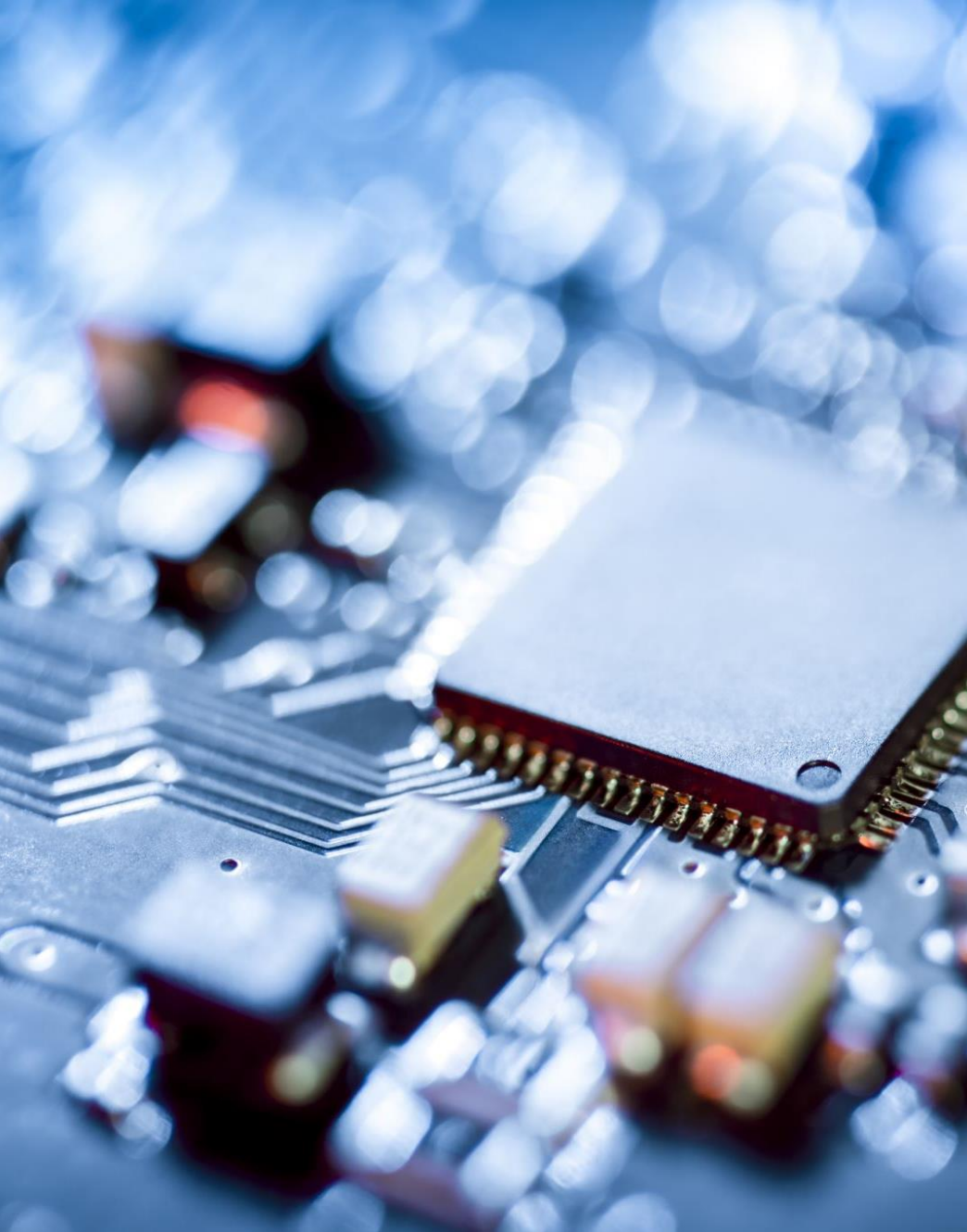
- Effective DNS/URL protection provides organizations with visibility into where people are going to the Internet — this includes what is leaving your company.
- Threat actors constantly focus on bypassing these systems; unfortunately, many organizations do not have this protection set up correctly, creating hidden vulnerabilities.
- Quest's DNS/URL Checkup provides a review to where your users are going, new threat vectors they may experience, and feedback to prevent new threat vectors.

Cybersecurity Checkup Overview

Maintain your organization's surveillance and protection with these 7 checkups.

7 Firewall/IPS

- Your firewall is your gateway to the Internet, and since platforms are constantly being updated along with feature enhancements, this needs to be consistently checked. This includes traffic coming in and out of your network.
- Additionally, the IPS also provides visibility to the in and out bound traffic and needs to be reviewed on a regular basis, as well for logging and blocks.
- Quest's Firewall/IPS (Intrusion Prevention System) Checkup is a fundamental security component for every organization.
 - We recommend this checkup to be performed every six months, if not every quarter.



How Does the Quest Cybersecurity Checkup Program Work?

1. Select your checkup(s).
2. Quest will send you a scope of work and pricing for the plan you've chosen.
3. After your approval, a Quest Security expert will schedule a call to discuss your systems and gather configuration information.
4. A Quest Security expert will analyze your configurations.
5. Quest will provide improvement recommendations within the next 3-7 business days.



Thank you!

Would you like to learn more about Quest's capabilities?



Phone

+1-800-326-4220



E-mail

Contact@questsys.com



Quest

<https://questsys.com/>

Contact us

<https://questsys.com/contact-us/>

