Email Security Assessment

To limit the spread of illness, organizations around the world are required to support your users remotely. That now means your users are accessing sensitive from unknown networks and devices making applying a security policy almost impossible. We are seeing a major increase in targeted phishing emails with the goal of stealing your users credentials.

The unprecedented—and unplanned—move to a 100% remote workforce relies heavily on cloud-based platforms such as Google G Suite and Microsoft Office 365 (O365) for both communication and collaboration. Unfortunately, this disruption in normal work habits and location brings with it inherent risk, as distributed employees rely more heavily on email for communications, and critical business processes break due to these changes.

It's imperative your email security is ready to identify and stop this, but do you know if it will? Integration Partners is offering to perform a complimentary email security check up to ensure your email security technology will identify and stop phishing and credential threat attempts.

FAQs

Q: Will this impact my current email security technology?
A: No, this assessment runs in parallel to your current technology and will not impact any currently installed technology.

Q: How long will this take?
A: We typically perform this assessment for 2 weeks with regular progress check-ins however, this can be extended to 60 days given the current health situation.

Q: Does it matter if I am using Microsoft Exchange or Gmail?
A: No, our assessment can work with both.

Q: How long does this take to set up?
A: Typically 30-minutes via a remote screen share session.

Q: What will I receive at the conclusion?
A: A comprehensive report will be made available showing any/all threats received and whether your current security technology took appropriate action or not.

Q: What do I need to do to sign up for this?
A: Your Integration Partner's Account Executive can assist you with setting this up.

External Vulnerability Assessment

With your users moving to a 100% remote work format, more of your applications and corporate access will be made publicly available and may not have properly checked for vulnerabilities. Consequently, Integration Partners is offering to perform a complimentary vulnerability assessment for up to **5 recently released (as of March 1st, 2020)** external IP Address and/or applications.

Integration Partners perform numerous security services and we are offering this to ensure your applications are not open to attacks from hackers who are taking full advantage of this current health situation and we are determined to help you with defending against these attempts.

FAQs

Q: What does 'recently released' mean?
A: It means any external IP Address or application that was made public since March 1st, 2020.

Q: Can this scan be performed at certain times?
A: Yes, you can choose when this scan is performed.

Q: What will I receive at the conclusion?
A: You will receive a full result report that includes the level of security and any discovered vulnerabilities which will be reviewed by a security expert to ensure all your questions are answered.

Managed Security Monitoring

With the increase in remote workers, logins and account access attempts are initiated from network, systems and devices that your environment has not previously allowed. Consequently, ensuring you're aware of unauthenticated users accessing your critical data is now more imperative than ever. Integration Partners is here to help.

We are offering to monitor your user login activity for **free for up to 30 days**. We are also offering to perform 30 days of free monitoring of your Microsoft O365, Active Directory and Email activity to help you focus on delivering immediate needs to your users.

FAQs

Q: Is there a user limit?
A: No.

Q: How quickly can this be deployed?
A: Typically, within five days of receiving a signed agreement depending on the size of the organization.

Q: Is this 24/7?
A: Yes.

Microsoft Security Workshop

As organizations rapidly expand and evolve their digital estates due to distributed environmental demands, having an integrated approach to security is more important than ever.

Designed for today's security leaders, the Microsoft Security Workshop focuses on learning your organization's unique needs and develops a strategic plan based on approaches recommended by Integration Partners experts.

This engagement includes a Threat Check that will allow you to gain visibility into threats in your cloud environment across email, identity, and data.

FAQs

Q: Is there any possibility of production impact to systems during the workshop?
A: No. Save for the application of trial licensing from Microsoft, there are no required changes to production tenants or endpoints.

Q: How quickly is the workshop conducted?
A: The initial discovery session and Threat Check setup will take less than a day. Following several weeks of data collection, the team will reconvene to discuss the results of the Threat Check.

Q: What will I receive at the conclusion?
A: A report which contains the Threat Check results – designed to better understand, prioritize, and mitigate potential vectors of cyberattacks against your organization. Additionally, Integration Partners will provide customized recommendations with respect to strategy, initiatives, and tactical configuration steps.

Cloud Risk Assessment

Integration Partners CRA offers security administrators and Dev Ops teams the ability to evaluate their cloud configuration security posture, detect potential threats originating from misconfiguration of cloud resources, analyze traffic across cloud resources (in and out of the cloud), and evaluate cloud configuration against best practices. It enables the ability to manage risk throughout multi-cloud infrastructures, provides regulatory compliance reporting, and integrates remediation into the cloud infrastructure lifecycle automation framework.

FAQs

Q: What is needed to start this process?
A: Admin level access to your cloud domains.

Q: How long does this review take?
A: Typically 2 weeks however this can be extended.

Q: What will I receive at the conclusion?
A: You will receive a thorough report documenting the findings including an executive summary. Sample reports are available.