Integrity360
your security in mind

Covid-19 Resources

Overview

With the advancement of Covid-19 in recent weeks, cyber security teams have been introduced to an additional challenge of mobilising entire workforces securely, in a very short space of time.

On top of that, they also have to deal with heightened threats which have appeared in the form of new Covid-19 malware, phishing campaigns and DDoS attacks, as well as continuing their existing cyber security enhancement projects and BAU activities.

We understand that this is difficult to juggle for any business and we aim to support our clients in any way possible during this time with advisory webinars, resources and services.

We are assisting many of our clients with a number of core services during this unprecedented time and we invite you to get in touch if you require assistance of any kind in keeping your business secure.

Above all else, we are offering guidance and advice in whatever way we can so please feel free to reach out on any areas of concern and our team can advise accordingly.

The Top 5 Global Threats

1.

Phishing

Threat actors are using the current Covid-19 pandemic as an opportunity to encourage people to click on malicious links and open malicious attachments. There has been a significant increase globally in the number of Covid-19 related phishing emails being sent with many of Integrity360's customers experiencing these phishing attempts. Concerningly, the click rates reported globally on these phishing emails is very high with users.

2.

Malware

Threat actors are benefiting from the curiosity of people investigating the current Covid-19 pandemic, therefore there is a significant increase in the number of domains being created using wording related to the pandemic. These domains are showing legitimate information relating to Covid-19, however they are being used to host malicious software. This risk is raised significantly as users are actively searching for this topic, therefore the links are often not being delivered via email. This makes them more difficult to detect and prevent.

3.

DDoS

With workforces now working remotely, corporate resources are under significantly increased pressure. Customers are reporting slow networks, high bandwidth, and networks teams are monitoring closely to ensure services remain available. With many businesses preparing to close due to the global pandemic, threat actors are turning their focus to interrupt service availability of critical national infrastructure.

4.

Third Party Vendors

With organisations extending remote working capabilities, third party vendors have been given increased access to corporate networks remotely. This is necessary to ensure ongoing daily operations are maintained however this introduces enhanced risk of data leakage including credential harvesting on less secure personal computers.

5.

Access Control

Within the current economic climate, adapting to the remote working scenario and backup support teams being deployed, the access management process is critical to security. With employees requesting increased levels of access which may be required in the event of certain employees being unavailable, managing these new requests and ensuring access is only extended as required is key to minimising the risk of data leakage and service incidents due to mistaken configuration changes.

Technology and Infrastructure Services

VPN Health Check

Many businesses have been forced to rapidly implement remote access solutions. These platforms often contain latent risk from misconfiguration and misalignment with industry best practice. Our VPN Health Check includes:

- High-Level topology and infrastructure review
- Endpoint deployment review
- Rule-base review and analysis
- Platform hardware, software and licensing review and validation

Remote Access Technical Design

In-depth assessment of your remote access infrastructure and recommendations report as to what is needed to meet specific requirements in your new environment. Considerations of the review include:

- Security of existing infrastructure
- Scalability of existing infrastructure
- Resilience of existing infrastructure
- Recommended solution, if needed to meet the emerging client needs

Benefits:

- Validate that external resources/assets are not presenting ‘easy targets’ to malicious actors.
- Provide the business with assurance that new services have had a certain level of security rigor applied in their provision.
- Gain visibility and gather insights to improve your platforms and services

Home Working Testing Services

External Network Penetration Test

Network penetration tests examine and identify security vulnerabilities in systems at the network and unauthenticated application layers. This test includes manual issue verification and exploitation to take advantage of the vulnerabilities identified to see them through to their logical conclusion, penetrating defences and uncovering further vulnerabilities.

VPN Configuration Review

A VPN configuration review is a full review of a VPN's configuration and security posture from an authenticated perspective.

Laptop Build Review

Laptop build reviews are comprised of three primary elements including a stolen laptop test, locked down user breakout test and a full review of a laptop's configuration and security posture from an authenticated perspective

Benefits:

- Validate that external resources/assets are not presenting 'easy targets' to malicious actors.
- Gain real-world insight into the existing vulnerabilities in your networks

Cyber Security Awareness & Training

Phishing Simulation (Covid-19 Specific)

A phishing exercise is an exercise designed to measure the number of staff members that are susceptible to well-constructed emails requesting certain actions like clicking on links, opening attachments and entering user credentials.

Carrying out a once off or recurring phishing campaigns related to Covid-19 content gives businesses a metrics of employee's awareness and exposure to phishing related attacks.

User Awareness Training

Tailored user-awareness training plans to cover working from home content as well as phishing awareness using industry leading programmes.

Benefits:

- Provide added protection to workforce who are working remotely
- Maintain communication and education for remote workforce
- Educate users to cyber risks at home (which are not just confined to the office)
- Raise awareness of Covid-19 specific phishing attacks while demonstrate responsiveness to reported/known threats

Support Augmentation Services

SOC Response Team

Integrity360 has access to a number of skilled resources who would be able to help our clients in cases of emergency staff cover requirements. These resources can provide remote assistance for security infrastructure, virtualised environments, Windows and Linux administration, among other niche areas.

Technical Support Services (TSS)

TSS offers access to skilled resources on an SLA basis to assist with advanced troubleshooting and service restoration of cyber security technologies in response to high-severity incidents.

Vendor technologies supported include Check Point, Fortinet, F5, Cisco, Forcepoint and others upon request.

Benefits:

- Access to skilled resources on a draw-down basis to assist in a ‘pinch’
- Contingency planning as part of BCP measures in the event of illness or unavailability of critical resources

Governance and Controls Services

Remote Access Review

A remote access review assesses your current environment including:

- Supporting/enabling policies (WFH, information security, etc)
- Supporting processes (Authentication and Auditing)
- Supporting technologies
- Regulatory implications

Active Directory Audit

Access control is of increased importance given the heighten insider threat that the evolving situation poses. An Active Directory (AD) audit provides high-level reporting and recommendations covering:

- Admin and privileged accounts
- Accounts with Mailbox Rights on senior stakeholders
- Stale accounts (not accessed in last 14 days)
- All user and group memberships

Benefits:

- Validate that your approach to Secure Remote Working is in line with industry standards, recommended best-practice and with your remote working policy
- Ensure that appropriate security considerations have been taken
- Review whether any short-term changes which have been implemented affect the organisation's regulatory position or conflict with compliance requirements
- Validate that Role-Based Access Control (RBAC) processes are current and relevant

Remote Access Solutions

Integrity360 partners with some of the world's leading cyber security vendors. Many of these providers have offered advice to businesses on how best to protect their mobile workforce during this unprecedented time.

We've compiled a number of solution offerings from these industry leading providers that can solve challenges of remote working in a secure environment.

We remind our clients to continue to follow your existing security guidelines during this time and ensure that no solutions or changes are implemented without adequate considerations to their impact on your environment.

Our specialist team are available to discuss your requirements or concerns you have with your current infrastructure. If you require assistance or advice please just get in touch.

Check Point SOFTWARE TECHNOLOGIES LTD

RSA

f5

CISCO

FORTINET

FORCEPOINT

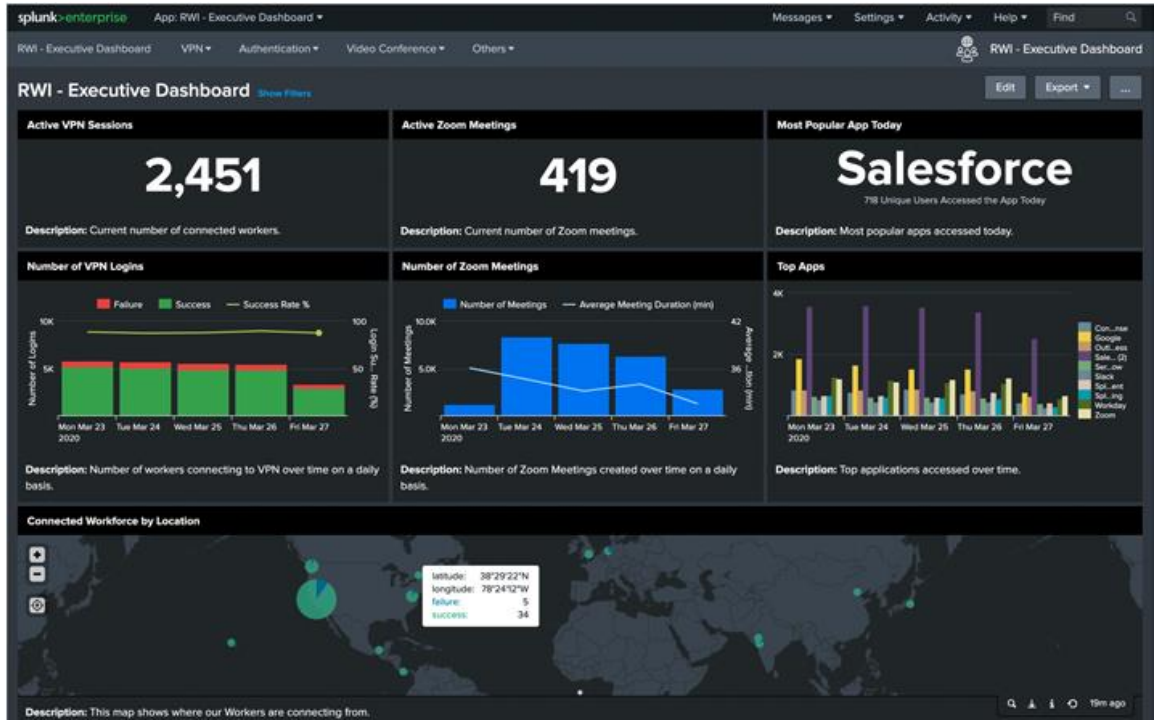
splunk>

Microsoft

Remote Access Solutions

Remote Work Insights (RWI) empowers IT and Security teams to manage applications, monitor business performance and secure networks from remote locations.

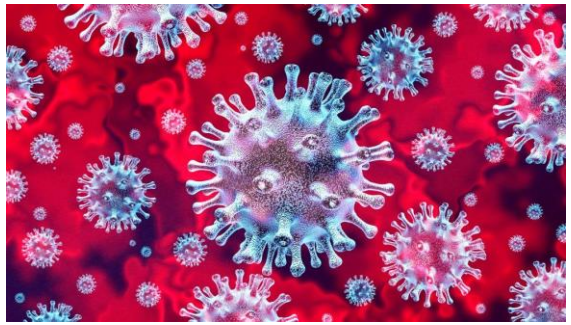
RWI provides real-time visibility across multiple disparate systems, such as VPN, Authentication, Zoom, and Microsoft 365, alongside executive level dashboards to boost productivity and ensure high performance of your critical business activities. Remote Work Insights includes apps and add-ons, best practices, dashboards and more. Getting started with this feature is quick and we have a team of specialised Splunk consultants at the ready to provide assistance and support if needed.



[Learn how Splunk's CTO uses Remote Work Insights]

splunk>

Related blogs



Blog: Coronavirus Malware and Phishing campaigns

The latest Global Threat trends show cyber-criminals exploiting interest in the global Coronavirus pandemic. The aim of these cyber-criminals is to spread malicious activity, with several spam campaigns relating to the outbreak of the virus. Read more

Blog: 9 physical cyber security tips for transitioning to remote working

There's a good chance that with no one in the office, hackers will see this time as an opportunity to steal information and data while no one is the wiser. Or, with everyone working from home, employees could forget that cyber security policies apply everywhere – including from the living room. Physical cyber security expert, Neil Gibb has a few tips to help organisations keep their records and servers safe from cybercriminals during the months ahead. Read more

Related blogs

Blog: Industry Leading Remote Access Solutions

While the effects of the Coronavirus develop, businesses across the world are turning to remote working to ensure the safety of their employees as well as the continuity of their services. We've compiled a number of solution offerings from industry leading providers that can solve challenges of remote working in a secure environment. Read more

What will the new normal for information security look like?

The current pandemic situation and restrictions may create an opportunity to transition your data protection and security approach to be ready for a new norm. Ciaran Johnson reviews what this new normal for information security could look like. Read more

Related blogs

Blog: 7 Top Tips for effectively enabling secure remote working

The advancement of Covid-19 in recent weeks is challenging all organisations to mobilise their entire workforces, not just a select few departments. With this challenge in mind, Michael Cowley, outlines his ‘magnificent 7’ must-dos for enabling secure remote working in your business, assuming it is not something that has previously been a business focus. Whilst not exhaustive, it is offered as a check-list to ensure that the foundational elements have been considered. Read more

Integrity360 On Demand Webinars

7 Tips for enabling secure remote working – ON DEMAND

Michael Cowley, Design & Consulting Lead discusses the 7 'must-dos' for enabling secure remote working in your business, assuming that it is not something that has previously been a business focus. Whilst not exhaustive, these 7 tips are offered as a check-list to ensure that the foundational elements have been considered. **Watch on Demand**

Technical considerations for implementing secure remote working – ON DEMAND

Our panel of cyber security specialists will be on hand to answer any questions or concerns you have around securing your remote workforce. We'll also share queries that other businesses like yours are having and advice on the best approaches to take. **Watch on Demand**

Protecting your workforce and your information – ON DEMAND

During this webinar we share tips and actions that will help your business stay secure while still operating effectively, including:

- Advice on what your business can do to protect your information and assets as the workforce continues to work outside of your office
- Guidance on what your employees can do to protect themselves and your business information while working remotely
- Advice on dealing with the operational impact of key IT staff being absent

Watch on demand

Useful Resources

Ask The Specialists – Integrity360 Covid-19 Q&A
We welcome you to submit your questions in the form below about challenges your face in managing your business' cyber security requirements during this evolving situation. Our panel of Integrity360 specialists will respond directly to you with guidance and suggestions. We'll also share any relevant information on this Q&A page to help you and others. Submit a Question

Home working: preparing your organisation and staff
The National Cyber Security Centre outline how to make sure your organisation is prepared for an increase in home working, and advice on spotting coronavirus (Covid-19) scam emails. Read more

The National Cyber Security Centre (NCSC) – Ireland
The NCSC-IE and trusted partners have observed an increase in phishing and malware campaigns exploiting the Covid-19 pandemic. The have outlined these threats in their latest advisory. Read more

SANS Security Awareness Working-from-home Deployment Kit
Everything you need to know to create secure work-from-home environments during the Covid-19 pandemic and beyond. Read more

Integrity360
your security in mind

Further Information

If you'd like further advice or guidance please get in touch or speak with your account manager who can arrange an advisory session with one of our specialist teams. info@integrity360.com | www.integrity360.com