

SECURITY FIRST

Cyber Security Conference 2023

LONDON

March 22nd, 2023

IET London: Savoy Place

<https://bit.ly/Sec1stLDN>



Integrity360
your security in mind

Foreword

Welcome to Integrity360's cyber security conference "Security First". Firstly, I would like to thank you for taking time out of your schedules to attend our annual conference.

As IT professionals and cyber security experts, you encounter various challenges that are becoming increasingly intricate as the digital world evolves rapidly with significant challenges defending against increasingly sophisticated criminals and attackers who are constantly coming up with new ways to potential attacks at your organisations.

At Integrity360, we are dedicated to embracing the ethos of a Security First mindset to operate IT environments safely, reliably, and continuously.

Our objective for hosting these specialist conferences is to bring together IT and cyber security professionals like you to gain insights into the latest trends, services, technologies, and strategies. We hope to equip you with actionable insights to enhance and support your own strategy, processes, and systems to foster a better security posture.

We encourage you to attend our keynote sessions, ask questions to our panellists, and network with your peers and industry colleagues throughout the day. We believe in the value of sharing knowledge and experiences to stay ahead of the curve when it comes to cyber security.

We understand that your work is challenging, and we are committed to supporting you in every way possible. As a team that speaks to IT and cyber security professionals from various industries, we comprehend the unique challenges that you face.



Ian Brown
Executive Chairman, Integrity360

”

It takes 20 years to build a reputation and a few minutes of a cyber incident to ruin it

“Failing to prepare is preparing to fail” – Benjamin Franklin

Agenda

09:30 Registration & Breakfast Bites

10:00 - 10:30 – Demo Labs

Riverside Room

10:00 - 10:15 A - Splunk B - Cynet

10:15 - 10:30 A - Trellix B - Splunk

10:30: Welcome by Host, Kate Russel

Turing Lecture Theatre

10:35: What you can't see - you can't control

Matt Tomlinson, Director UK, Integrity360

10:45: Gaining visibility in an always-on world

Richard Ford, CTO, Integrity360

11:30: Demystifying Cloud Security: Clearing the fog of understanding

Brian Martin, Director of Product Management, Integrity360

12:00: Securing Your Organisation with Effective Threat Monitoring & Detection

Alexandra Marsden, Director of Analyst Operations, Darktrace

Ellis Reed, Solution Architect, Integrity360

Ellis Fincham, EMEA Practice Lead - Threat & XDR, Rapid7

Matthew Middleton-Leal, Managing Director EMEA North, Qualys

12:40 - 13:10 Demo Lab

12:40 - 12:55 A - Mimecast B - Trellix

Riverside Room

12:55 - 13:10 A - Cynet B - Mimecast

13:00 – 13:45 – Lunch

13:45: Modern Day Exposure Management

Turing Lecture Theatre

Nick Brownrigg, Director of Solution Architecture at Integrity360

14:20: How to stop Business Email Compromise from crushing your business.

Matt Griffith, SE Manager, UK & I Channel at Check Point

14:50: Data Security starts here: A practical guide to protecting your data

Ahmed Aburahal, Technical Product Manager

Steven Nesbitt Enablement Manager – Europe, Varonis

15:25 - 15:50 - Coffee Break

15:50: The Ransomware Epidemic: Ransomware insights with Integrity360's IR team and experts from Skyhigh and XM Cyber

Patrick Wragg, Head of Incident Response, Integrity360

Matthew Quinn, Technical Director for Northern Europe, XM Cyber

Boubker El Mouttahid, Global Technical Director, Skyhigh

Richard Breavington, Partner Head of Cyber & Tech Insurance, RPC

16:35: **KEYNOTE SPEAKER** Hackers Inc. – an inside view of organised cybercrime, and where it goes next

Geoff White, Author, Cybercrime Investigate Journalist & Former Channel 4 News Tech Correspondent

Sponsors



Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data: sensitive files and emails; confidential customer, patient and employee data; financial records; strategic and product plans; and other intellectual property. The Varonis Data Security Platform detects cyberthreats from both internal and external actors by analysing data, account activity and user behaviour; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation. Varonis started operations in 2005 and has customers in major leading firms from various industries.

[VARONIS.COM](https://www.varonis.com)



Check Point is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from 5th generation cyber-attacks with an industry-leading catch rate of malware, ransomware and other types of attacks. Check Point offers multilevel Security Architecture, "Infinity" Total Protection with Gen V advanced threat prevention, which defends enterprises' cloud, network and mobile device held information. Check Point provides the most comprehensive and intuitive one point of control security management system.

[CHECKPOINT.COM](https://www.checkpoint.com)

DARKTRACE

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,100 organizations globally from advanced cyber-threats.

[DARKTRACE.COM](https://www.darktrace.com)

RAPID7

Rapid7 simplifies cybersecurity. With powerful automation and integrated threat intelligence from our industry-leading researchers and SOC analysts, our Insight Platform gives security teams the visibility they need to secure their environment no matter the size or complexity. Don't just protect your business, drive it forward.

[RAPID7.COM](https://www.rapid7.com)

Sponsors



At its heart, security is a data protection problem. Our mission at Skyhigh Security is simple: to protect our customers, their employees, and most important, their data—regardless of where it's located— in a rapidly shifting, hybrid work environment. Thanks to innovations in technology, and changing work patterns wrought by the recent pandemic, hybrid work is now not only commonplace but essential for organisations to succeed. Business critical data is scattered across multiple platforms— from legacy PCs, data centers and websites to cloud applications/infrastructure and remote devices. The urgent need for security to protect users' data wherever they are has galvanized the emergence of Security Service Edge (SSE), making it our singular focus.

[SKYHIGHSECURITY.COM](https://skyhighsecurity.com)



Qualys, Inc. is a pioneer and leading provider of disruptive cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide. The Qualys Cloud Platform and its integrated security solutions continuously deliver critical security intelligence to businesses across their global IT assets.

[QUALYS.COM](https://qualys.com)



Splunk helps make organizations more resilient. Leading organizations use our unified security and observability platform to keep their digital systems secure and reliable. Organizations trust Splunk to prevent security, infrastructure, and application issues from becoming major incidents, absorb shocks from digital disruptions and accelerate digital transformation. Splunk helps SecOps, ITOps and DevOps teams deliver these outcomes with comprehensive visibility, rapid detection and investigation, and optimized response, all at the scale necessary for the world's largest digitized organizations.

[SPLUNK.COM](https://splunk.com)



Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers. More at <https://trellix.com>.

[TRELLIX.COM](https://trellix.com)

Sponsors



Cynet's end-to-end, natively automated XDR platform, backed by a 24/7 MDR service was purpose-built to enable lean IT security teams to achieve comprehensive and effective protection regardless of their resources, team size or skills.

[CYPNET.COM](https://cynet.com)



Since 2003, Mimecast has stopped bad things from happening to good organisations by enabling them to work protected. We empower over 40,000 customers to mitigate risk and manage complexities across a threat landscape driven by malicious cyberattacks, human error, and technology fallibility. Our advanced solutions provide proactive threat detection, brand protection, awareness training, and data retention capabilities evolving workplaces need today. Mimecast transforms email and collaboration security into the eyes and ears of organisations worldwide.

[MIMECAST.COM](https://mimecast.com)



XM Cyber is a hybrid cloud security company that's changing the way innovative organizations approach cyber risk. Its attack path management platform continuously uncovers hidden attack paths to businesses' critical assets, enabling security teams to cut them off at key junctures and eradicate risk with a fraction of the effort.

[XMCYBER.COM](https://xmcyber.com)



The Armis Platform is the industry's most comprehensive asset intelligence platform providing unified asset visibility and superior security for organizations that need to protect against unseen operational and cyber risks, increase efficiencies, optimize use of resources, and safely innovate with new technologies to grow the business.

[ARMIS.COM](https://armis.com)



Security risks due to misconfigurations are a major pain-point for all organizations. Gytpol is a Security Configuration Management platform that provides continuous monitoring and automatic remediation with zero impact of security risks caused by misconfigurations and non-compliance on endpoint devices. It's fast, accurate & secure. Gytpol stops breaches, reduces risks and saves organizations, significant time and cost.

[GYPTOL.COM](https://gytpol.com)

Integrity360

your security in mind

Your Trusted Cyber Security Partner:

Empowering organisations to achieve great things, securely



Cyber Security Solutions



Cyber Risk & Assurance



Cyber Security Testing



Incident Response



Managed Security Services



Managed Detection & Response



integrity360.com



We protect data.

Is your data safe?

At Varonis, protecting your file and email systems from cyberattacks and insider threats is our primary focus. We're fighting a different battle — so your data is protected first. Not last.

Learn more at www.varonis.com.



Reduce your ransomware blast radius with data-centric security

- ✓ Dramatically reduce your attack surface by automatically identifying and removing excessive access to data
- ✓ Detect early signs of ransomware attacks with behavior-based threat models for each phase of the kill chain
- ✓ Automatically stop attacks in their tracks and limit damage
- ✓ Call on Varonis' world-class Incident Response & Forensics teams to help with any incident



Get your **free risk assessment** at
varonis.com/risk

YOU DESERVE THE BEST SECURITY

Only the best security can protect you from today's complex cyber threats. Large scale, multi-vector attacks now threaten the fabric of organizations around the globe.

Check Point fully protects you against these Gen V attacks. Our transformative product innovations protect better than all other options.

In a world where threats are ever growing, you deserve the best security. Check Point.



www.checkpoint.com

CYBER SECURITY ISN'T A PRODUCT. IT'S A STATE OF BEING.

We believe that cyber security should cover you from all angles, all the time. It's why Darktrace detects threats, responds to them, and helps proactively prevent them. And it's all powered by our industry-first Cyber AI Loop — which uses Self-Learning AI to constantly optimize your state of security.

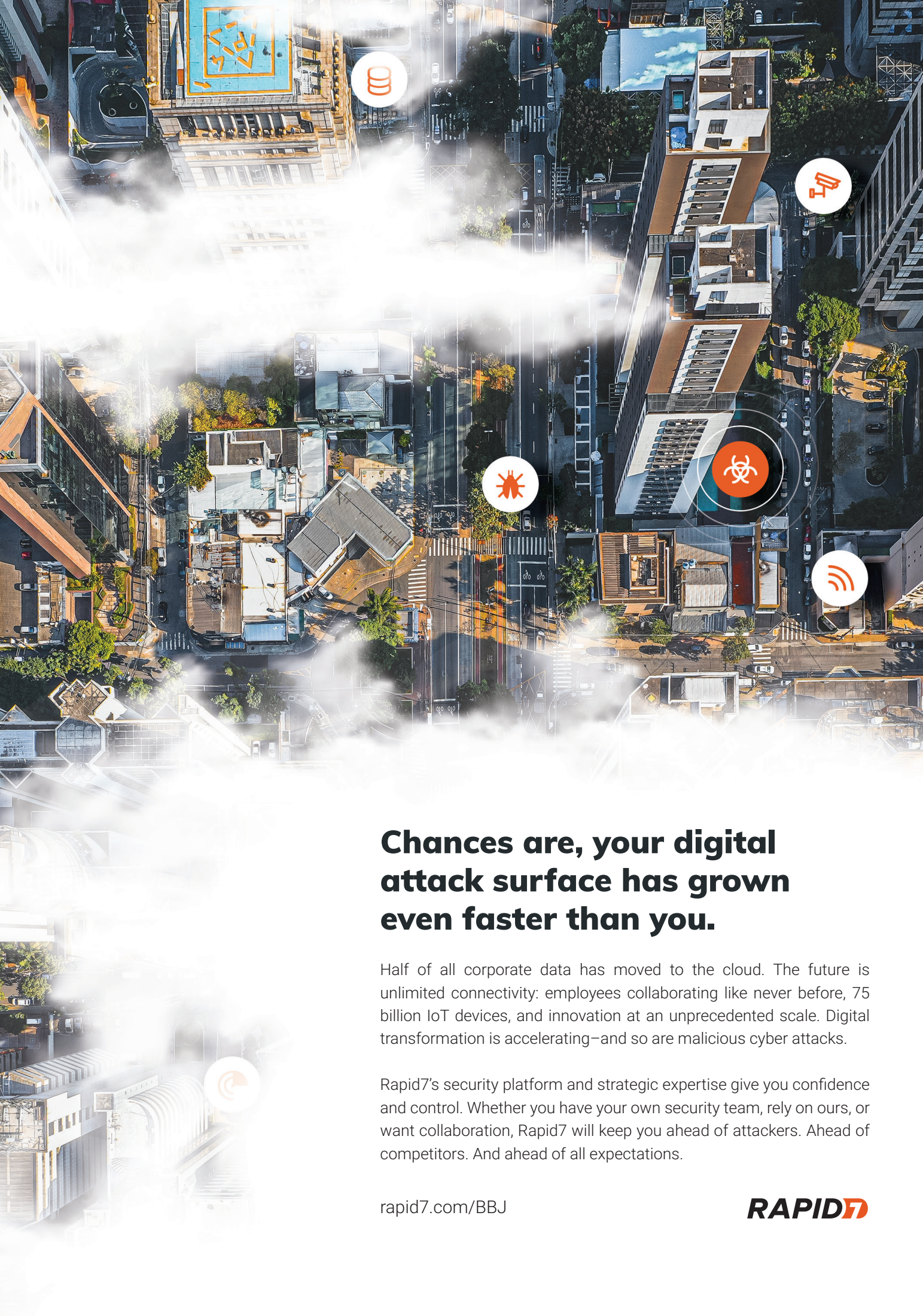


DARKTRACE

Evolved threats call for evolved thinking

[Darktrace.com](https://darktrace.com)

© 2022 Darktrace Holdings Limited. All rights reserved. The Darktrace name, logo, and other trademarks used herein are trademarks of Darktrace Holdings Limited.



Chances are, your digital attack surface has grown even faster than you.

Half of all corporate data has moved to the cloud. The future is unlimited connectivity: employees collaborating like never before, 75 billion IoT devices, and innovation at an unprecedented scale. Digital transformation is accelerating—and so are malicious cyber attacks.

Rapid7's security platform and strategic expertise give you confidence and control. Whether you have your own security team, rely on ours, or want collaboration, Rapid7 will keep you ahead of attackers. Ahead of competitors. And ahead of all expectations.

rapid7.com/BBJ

RAPID7



Close Today's Exposures. Prevent Tomorrow's Attacks.

XM Cyber - See All Ways

Vulnerability management has long been a security program cornerstone, with the goal of trying to address issues as they are disclosed. But addressing vulnerabilities is only part of the problem; There's a world of other exposures, that when combined, create attack paths straight to your most critical assets.

And while exposure management solutions attempt to address issues beyond CVEs and vulnerabilities, most solutions fail to provide the visibility needed to prioritize effectively. Security teams are struggling to handle volumes of security issues and understand what exposures put critical assets at risk.

The XM Cyber Exposure Management Platform is transforming the way organizations find and fix security exposures across the hybrid cloud. With XM Cyber, you can see how attackers leverage and combine misconfigurations, vulnerabilities, identity exposures, and more, across your AWS, Azure, GCP and on-prem environments to compromise your critical assets.

Now you can see all the ways attackers might go, and all the best ways to stop them, with a fraction of the effort.

Instead of addressing volumes of issues as independent entities, XM Cyber combines them together into an attack graph, which proactively exposes hidden attack paths and security control gaps across your cloud and on-prem networks. By mapping all possible attack paths onto an attack graph, you gain context of risk towards critical assets. And by understanding context, issues can be accurately prioritized, to focus on remediating the exposures where attack paths converge. **This allows for productive remediation that reduces risk in the most time and cost-efficient manner.**

With The XM Cyber Exposure Management Platform, you can:

Answer Critical Questions

Gain complete visibility of what's putting the business at risk and the insights needed to take precise and decisive preventative actions

Prioritize Game-Over Issues

Using advanced attack graph analysis, pinpoint the exposures that need to be remediated to proactively keep the business secure

Continuously Reduce Risk

24/7 monitoring of your environment for new exposures that emerge as a result of the dynamic environment, with accurate remediation of the exposures that matter

Preventing exposures from impacting an organization is challenging; but with the right approach, it becomes scalable, no matter how large or complex the network, and regardless of what types of new exposures emerge. Want to learn more about The XM Cyber Exposure Management platform? **Speak with us at the Security First events or visit www.xmcyber.com.**

Extend Your Data Protection to the Cloud and Beyond

By Lalan Mishra - Senior Cloud Engineer, Skyhigh Security

With the new norm of the 'work from anywhere' hybrid workforce comes the collective hurdle: how are organizations expected to evolve at a record pace and ensure the security of their sensitive data at the same time?

It's evident that with the introduction of elastic cloud computing the public cloud adoption has been increasing exponentially, which means more data is being shipped and stored on the cloud services providers platform. This could be a potential advantage for the bad actors, who are always looking for weaknesses or vulnerability in the system.

With the explosive growth of cloud service, more and more organizations are onboarding software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) solutions based on business requirements and an ever-growing demand to meet the market potential.

SaaS solution providers, such as Microsoft 365, Google Suite, and other known collaboration providers such as Box, Zoom, Teams, and Webex are stepping in to meet the work-from-home user workforce requirements and keep business units connected, irrespective of location. This allows employees to be available from anywhere, at their convenience.

The harsh reality is that organizations are still catching up on how best to provide data visibility and protection in the cloud and beyond. This disconnect can happen daily in many ways, such as where remnants of data may be left on a work device or similarly where data is downloaded from cloud services but kept locally. And so, the challenge continues.

Skyhigh Security aims to bridge the gap with a data protection platform that enables users with corporate devices to extend their data protection to the cloud, web and private apps. Should you wish to expand your current data protection from your device to a cloud platform, Skyhigh Security's unique cloud DLP plays a vital role in protecting this data on the cloud platform.

Whether your enterprise data is stored with Microsoft, Google, Amazon or other, regardless of the location.

Why should you consider a Skyhigh Security Combination for your cloud data protection? Skyhigh Security is the industry-leading comprehensive, cloud-native SSE security platform that converges a set of security solutions, providing complete visibility and control over your data from a unified console, no matter where it resides.



Unlock the Value of Qualys VMDR to Drive a Risk-Based VM Program

Using a risk-based approach to remediating vulnerabilities is revolutionizing the way organizations traditionally approach vulnerability management with an all-or-nothing strategy of remediation. Prioritizing the remediation of vulnerabilities that are most likely to be exploited on critical systems will greatly improve risk posture and reduce remediation fatigue.

Qualys VMDR with Qualys TruRisk™ helps organizations quantify cyber risk so that they can accurately measure it, take steps to reduce exposure, track risk reduction trends over time, and better measure the effectiveness of their cyber security program. The chart below illustrates at a high level how teams can use VMDR to operationalize their risk-based vulnerability management program against the five pillars of RBVM.

PILLAR	OBJECTIVE	QUALYS VMDR APPROACH
Identify	Inventory Assets and Services Exposed to the Public Internet	Automate attack surface discovery using the Qualys Internet Scanners and Qualys Cybersecurity Asset Management (CSAM) with External Attack Surface Management (EASM) ² to discover blind spots for internet-connected assets
	Inventory Internal On-Premises Assets	Automate asset discovery with Qualys VMDR by deploying Qualys scanner appliances, agents, passive sensors, and more
	Inventory Public Cloud Workloads	Configure Qualys Cloud connectors to inventory virtual workloads on Public Cloud accounts
Context	Assign Criticality to Assets	Assign criticality to assets using Qualys TruRisk™ or directly import and assign business criticality to assets using Global AssetView or CSAM from a CMDB such as ServiceNow ³
Assess	Continuous Vulnerability Scanning	Perform regular vulnerability scanning of the environment using Qualys VMDR. Realtime vulnerability scanning every 4 hours or less with Qualys agents
	System Configuration Auditing and Security Hardening	Perform regular configuration audits using Qualys Secure Configuration Assessment (SCA)
Remediate	Prioritize Vulnerability Remediation	Pinpoint vulnerabilities that pose the most risk to the organization by using Qualys TruRisk™ Qualys Detection Scores on critical assets. Automate remediation using Qualys Patch Management and dispatch tickets to remediation teams with Qualys VMDR for IT Service Management (ITSM) integration ⁴
Monitor	Use Metrics to Evaluate Program Efficacy	Monitor asset posture in real time using Qualys dashboards that aggregate risk data with near real-time visibility

Get More Security

Qualys helps organizations cost-effectively reduce risk faster

Consolidate your point products on to a single cloud platform to deliver a unified IT, Security and Compliance solution—Get More Done

Try it today for free

qualys.com/free-trial





The State of Email Security 2023

DOWNLOAD YOUR REPORT



An increase in email has led to more email-based threats, and three out of four (74%) SOES respondents say threats have risen over the past 12 months:

- ▶ Corporate reliance on email continues to grow at a rate outstripping the surge in email that took place at the outset of the COVID-19 pandemic — with 82% of companies reporting a higher volume of email in 2022, compared with 79% in 2021 and 81% in 2020.
- ▶ Respondents singled out the increasingly sophisticated nature of the attacks they face as their biggest challenge (59%).
- ▶ 76% expect an email-borne attack will have serious consequences for their organization in the coming year.

www.mimecast.com/state-of-email-security/

Integrity360

your security in mind

**Don't get lost in
the maze of hype.**

MDR isn't perfect
but it's close



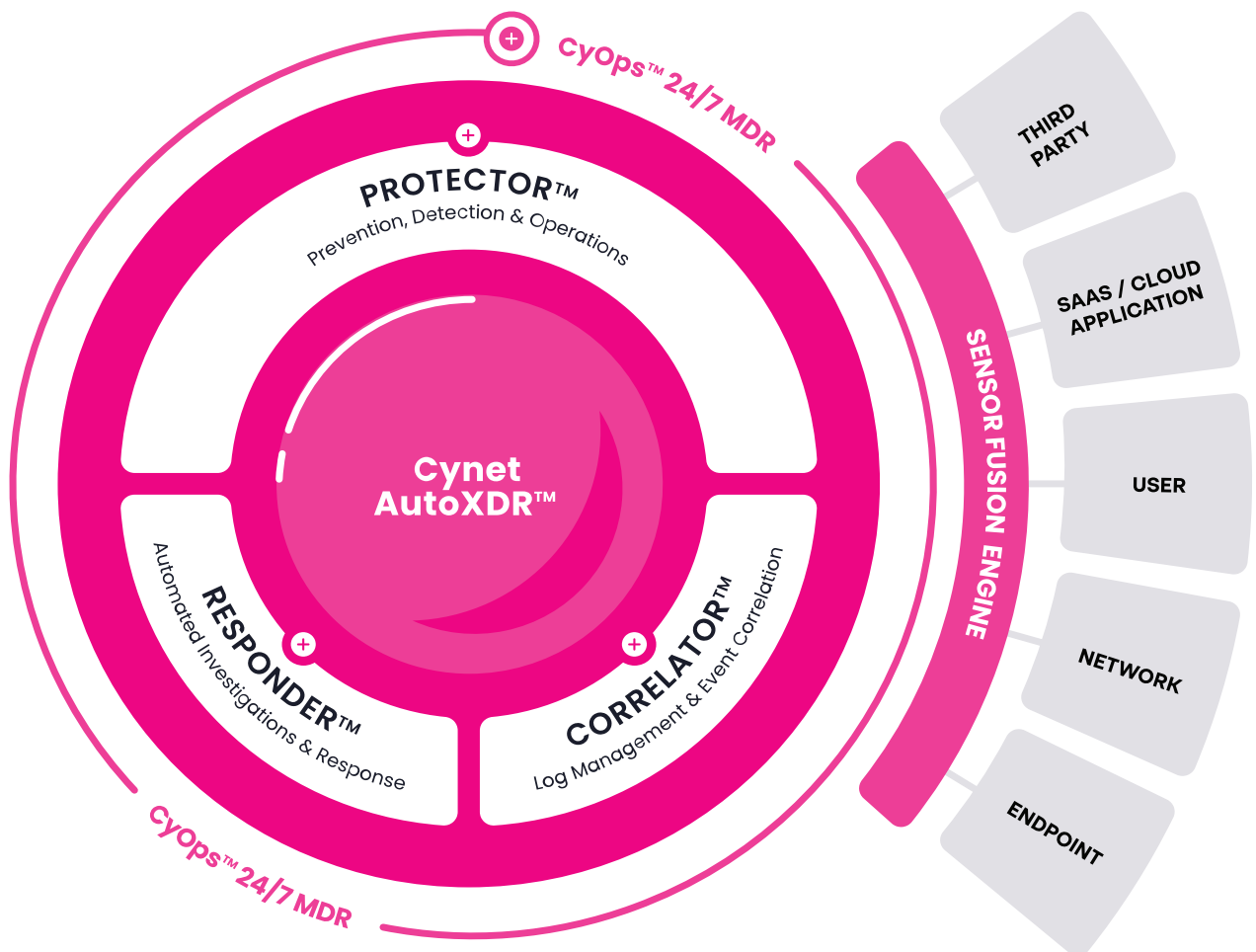
**Find out how we are helping
organisations like yours.**

visit www.integrity360.com





Cynet enables any organisation to put its cybersecurity on **autopilot** by natively consolidating the essential security technologies needed to provide comprehensive threat protection into an **easy-to-use XDR platform**, automating investigation and remediation across the environment, and providing a **24/7 proactive MDR service** - at no additional cost.



Download a free 14 day trial





Unlock the Value of Qualys VMDR to Drive a Risk-Based VM Program

Breaches, downtime, incidents — disruption is inevitable. It has become paramount for organizations to increase the resilience of their systems and processes, which enables them to bounce back and continue to innovate, no matter what arises.

In this guide, Splunk outlines five strategies that can increase the digital resilience of your organization:

- ▶ **Step 1:** Invest in analytics and automation to reduce burnout and increase agility
- ▶ **Step 2:** Adopt DevSecOps for more efficient, more effective application development
- ▶ **Step 3:** Improve observability to lower MTTD and MTTR
- ▶ **Step 4:** Employ AIOps to improve incident remediation
- ▶ **Step 5:** Consolidate vendors and embrace a platform approach for less burnout and better interoperability

Some findings include:

- ▶ Greater observability maturity is correlated with fewer outages, and 69% lower MTTR.
- ▶ AIOps measurably reduces MTTD (for 59% of organizations that adopt AIOps).
- ▶ Security vendor consolidation reduces complexity and improves risk posture for organizations.
- ▶ To download the full e-book, scan the QR code below



DON'T ASSUME, KNOW FOR SURE

Secure Configuration Management

Over 80% of ransomware attacks are attributable to device MISCONFIGURATIONS. A major pain-point for organisations as existing tools don't detect them.

Gytpol automates the detection & remediation of your misconfigurations and validates compliance on endpoint devices.

All of this with zero impact and zero fuss.
Saving you time and reducing your cost of ownership.

We are already helping many organisations transform ineffective manual methods via innovative automation.

FAST, ACCURATE, SECURE.

Contact us to find out more.



www.gytpol.com



20



Integrity360

your security in mind

**Build trust with
your stakeholders**
through robust
security measures



**Speak to our experts to find
out more about our Cyber Risk
Assessment and Mitigation
solutions.**

visit www.integrity360.com



WHY WORK WITH INTEGRITY360

Security should be First with any project involving IT. From moving to the cloud to deploying a database, you need the people, processes and platforms to support a secure and seamless transition.

Integrity360 specialists are experienced with a wide array of tools, frameworks and projects. With a variety of certifications and years of industry-specific experience to their name, they're able to tackle any problem or challenge head on.

Contact an Integrity360 advisor today to learn more about our services.

HEAD OFFICE

3rd Floor, Block D, The Concourse, Beacon Court,
Sandyford, Dublin 18, D18 P6N4 , Ireland
+353 1 293 4027

LONDON CITY OFFICE

46 New Broad Street, London, EC2M 1JH
+44 203 397 3414

NORTH LONDON OFFICE

Unit 4, Horizon Trade Park, Ring Way, Bounds Green,
London, N11 2NW
+44 20 8372 1000

Integrity360
your security in mind

Useful Resources

Scan the code below to get access to the Integrity360 Resource Library.



Integrity360: Your Trusted Cyber Security Partner

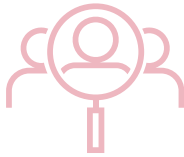
In today's digital age, cyber security is more critical than ever. As businesses face a growing number of threats to their networks, data, and reputation, it's crucial to have a reliable partner who can deliver effective, comprehensive solutions. That's where Integrity360 comes in.

A Security First Approach

Our Security First approach means that we prioritise security in everything we do. We empower our clients to make informed decisions about their cyber security, ensuring that they have the knowledge and tools they need to protect their businesses. With Integrity360, cyber security becomes an enabler for modern business, not a hindrance.



Cyber Security Solutions



Cyber Security Testing



Cyber Risk & Assurance



Incident Response



Managed Security Services



Managed Detection & Response

Why Choose Integrity360?

Choosing a cyber security provider is a critical decision for any business. Here are just a few reasons why you should choose Integrity360:

- **Experience:** With over 200 security consultants, engineers, and analysts, we have the global experience and expertise to safeguard your business from even the most complex and evolving threats.
- **Reputation:** We've earned the trust of over 300 global companies and have a strong reputation in the industry, built upon by exceptional technical expertise, a client-first attitude, and a proven track record on complex security projects.
- **Customised Solutions:** We take a personalised approach to cyber security, working closely with each client to understand their unique needs and recommend the most effective security solutions.
- **Passion and Commitment:** We're passionate about cyber security and committed to delivering the best possible protection for our clients' businesses.
- **Certifications:** Greatest level of technical certifications and capability
- **Partnerships:** Strongest vendor partnerships and support arrangements
- **Recognition:** Recognised by Gartner in three market guides
- **24x7 Secure Operation Centre**



Find out more

integrity360.com

Notes

Notes

#SecurityFirst2023

Integrity360

your security in mind

WWW.INTEGRITY360.COM