SECURITY FIRST

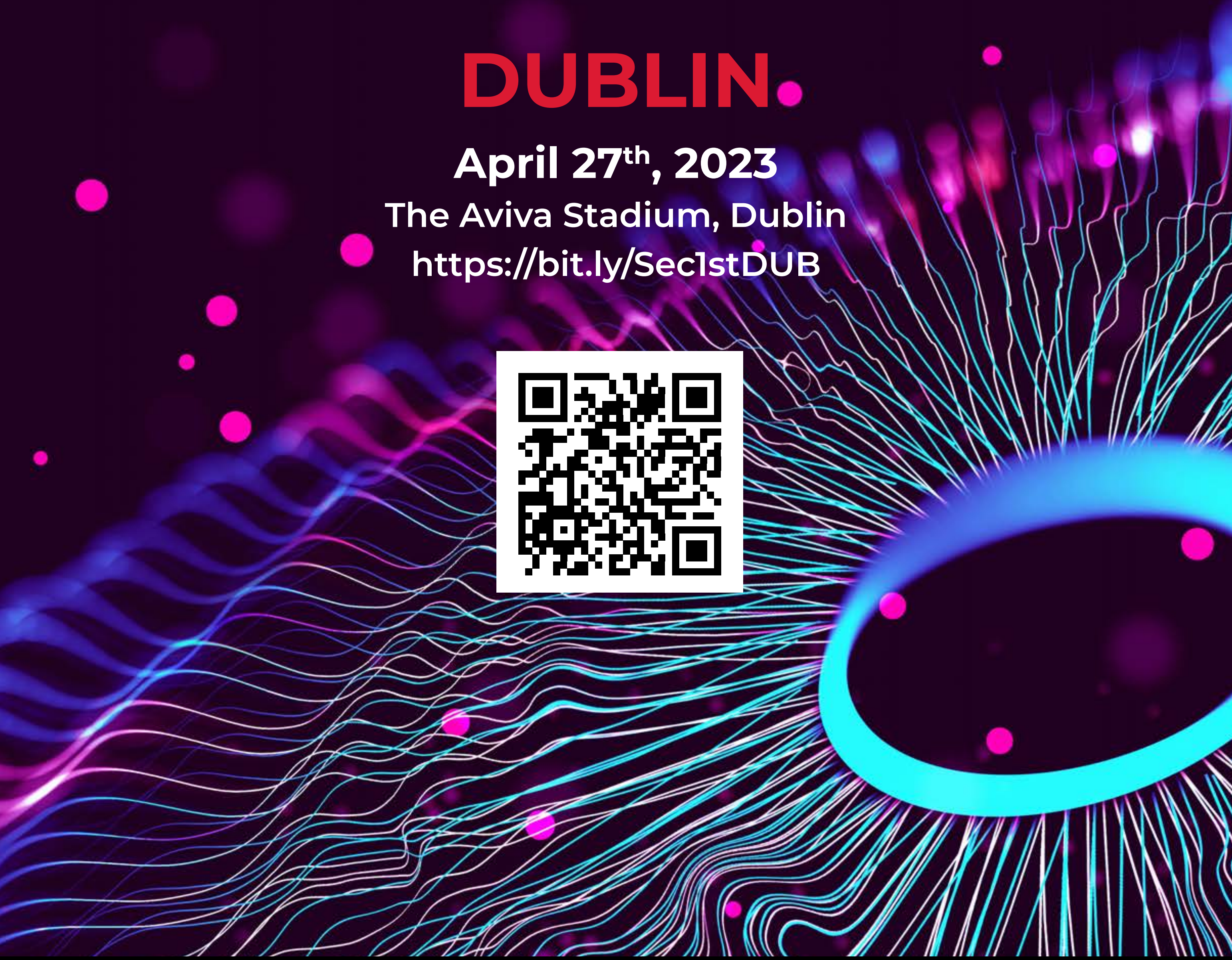
Cyber Security Conference 2023

DUBLIN

April 27th, 2023

The Aviva Stadium, Dublin

https://bit.ly/Sec1stDUB



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*

CHECK POINT™

Managing Cyber Risk: Why it's a Question of Business, Not IT

By Deryck Mitchelson, Field CISO, EMEA at Check Point Software Technologies

Most companies are now digital organizations, but during this journey of transformation, the focus has been on providing seamless customer experiences, instead of securing infrastructures. Check Point Research revealed that cyberattacks have risen by 38% in 2022 compared to the previous year, with an average of 1,168 weekly attacks per organization. Despite this, companies are not preparing for the associated business risks that an attack can have. Specifically, when it comes to outsourcing.

Where many businesses go wrong is that they place the responsibility firmly in the hands of the IT team. They don't acknowledge what responsibility the board has in securing their infrastructure. After all, if a business experiences a breach, it won't just impact its IT system. Hackers could potentially drain bank accounts, publish confidential customer information, or stop operations for days on end. This makes cybersecurity the responsibility of CISOs and executives, not just technology professionals. Cyber risk is a business risk. So, what can organizations do to switch up perspectives? Let's take a look.

What have we already seen?

The impact that a cyberattack can have reveals itself over years, not days. The recent breach of the NHS's third-party supplier, Advanced, which resulted in customer data being leaked, is a perfect example of this. Our health service is still suffering the consequences of another company not having a secure cyber strategy, months after being breached. This type of attack is not uncommon and is something we will continue to see heading into 2023.

It's also important to realize that this isn't a problem reserved for larger organizations, as we saw with the Okta Breach. Hacked by the group LapsuS$, 366 corporate customers were impacted by a security breach that allowed hackers to access the company's internet network. It impacted larger organizations including FedEx, but also companies such as Thanet District Council in Kent. That is why it is key that businesses of all sizes are taking the necessary steps to protect themselves.

Responsible Outsourcing

Many businesses that I interact with understand risk, but we need to articulate cyber risk in business risk terms. As a board member, CISO or CIO, your job is the understand risk, not to be a technical engineer. This is often miscommunicated. A successful breach could cripple your business, that's how severe the landscape is and that's why it's your job to mitigate it.

To do this successfully you first need to think - who has access to your systems? When you have a third-party supplier, they can't provide their service as a standalone, they have to access your systems somehow. That creates immediate risk if that is not managed or monitored appropriately. Don't just wait, there are solutions out there that can give access on an application-by-application basis through a web browser link, and this is a quick way to minimize risk.

Managing Cyber Risk: Why it’s a Question of Business, Not IT

By Deryck Mitchelson, Field CISO, EMEA at Check Point Software Technologies

Hold yourself accountable

If you’ve gotten this far and feel that you are responsibly outsourcing, it’s important to note that the challenge doesn’t end there. Ask yourself, are you following these best practices?

- Regular patching: Even when a vulnerability has been identified and a patch made available, devices are still left exposed. This could be because patching can be time consuming, or a company is simply not aware that they have an impacted device. Either way, routine patching is critical so don’t let it slip down the list of priorities.

- Looking for your own weaknesses: As a business grows, it’s unlikely that an accurate list of all hardware connected to the network is sufficiently kept up to date. This is problematic because these devices can still permit entry into your enterprise network. Therefore, it’s pivotal that a business takes stock of its technical estate because if anything is left unprotected a threat actor will find it.

- Consolidation: To have complete control over your cybersecurity strategy, you need to have one view of everything that is going on. This is why companies should opt for a single platform that allows you to spot any unusual activity faster and ensure you’re alerted before an attacker is given access, in other words adopt a consolidated approach.

Don’t Wait

Only when we shift perspective and understand that a holistic strategy means looking beyond technical insights will we be able to fully protect ourselves. We need to move away from cybersecurity being seen as a job for engineers or developers alone and realize that just one cyberattack will create long lasting damage. Threats are becoming more sophisticated than ever before, and it’s only by embracing a comprehensive, consolidated and collaborative security architecture can we keep our businesses safe.

Integrity360

your **security** in mind

Unlock the power of Visibility: Protect your Crown Jewels and improve your cyber security

By Matthew Olney, Integrity360

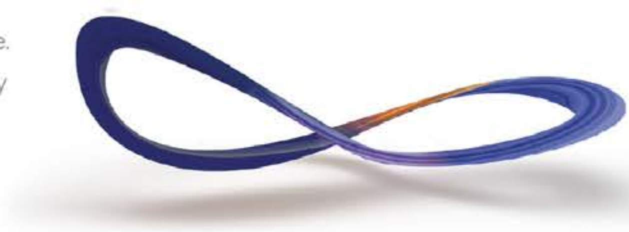
Protecting your organisation's crown jewels and improving your cyber security doesn't have to be overwhelming. By focusing on identifying and defending your most vital assets, networks, and systems, you can mitigate the effects of a security breach and reduce risk. This requires a team effort involving input from various departments, including the board, to identify critical assets based on financial impact, potential disruption, and reputational damage. Management buy-in is crucial to ensure these assets are prioritised in the organisation's security strategy.

Regularly reviewing and updating the list of crown jewels helps to ensure new assets and systems critical to the business's operations are added. Protecting the crown jewels requires ongoing monitoring and maintenance of the security measures in place. Incident response and recovery plans should be in place to respond to and recover from an incident.

Threat hunting and detection mechanisms such as Security Information and Event Management (SIEM) or Managed Detection and Response (MDR) systems and threat intelligence platforms can provide real-time monitoring and alerts on potential threats. Developing a tailored security strategy that focuses on protecting the specific crown jewels can include preventative measures such as access controls, encryption, and network segmentation, as well as detection and response capabilities such as incident response plans, security monitoring, and threat hunting.

Regular testing of incident response plans helps ensure all personnel are familiar with the procedures and can respond effectively in the event of an incident. By testing and exercising incident response plans, businesses can identify potential improvement points in the security process, which can help the organisation to improve their overall security posture.

Having clear visibility over your network is vital in being able to respond to an attack quickly. By knowing how and where your data goes in and out of your network, you can react to a breach quicker and respond more effectively. If you are worried about cyber threats or need help in improving your organisation's visibility, get in touch to find out how you can protect your organisation.



XM Cyber

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.**

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 AsssetView 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

UNINSTALL
QUARANTINE
REMEDIATE
KILL PROCESS

splunk>

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

SCAN ME

Integrity360
your **security** in mind

How MDR Assists in Risk Management

Matthew Olney, Integrity360

Due to growing threat complexity, most organisations lack the resources to create an in-house cyber security strategy to combat contemporary threats. As a result, many are turning to Managed Detection and Response (MDR) providers to cost-effectively enhance their existing cyber risk management approach.

MDR helps businesses bolster their cyber risk management by offering round-the-clock support from a Security Operations Centre (SOC). Security analysts in the SOC utilise up-to-date threat intelligence to conduct threat hunting, swiftly identifying intruders before they gain access to critical data.

These specialist teams possess the necessary expertise and resources to identify and contain advanced threats, addressing security incidents as quickly as possible. Leading MDR services offer various external support, including:

- Continuous detection, management, and containment of threats
- Comprehensive threat intelligence
- Proactive threat hunting
- Platform implementation, configuration, and tuning
- Incident management
- Change management

Organisations work with MDR providers to enhance their existing security controls and minimise cyber risk by optimising incident response capabilities. This enables them to detect and contain data breaches more rapidly, reducing operational impact.

MDR providers can help organisations identify their dependencies on people, technologies, and infrastructure and offer insights to develop proactive strategies to mitigate threats and maintain data privacy.

MDR can augment risk management strategies by:

1. Identifying and addressing priority risks and use cases: MDR providers can help mitigate cyber risk by pinpointing an organisation's priority risks and finding ways to address them, such as cloud compromise, phishing, social engineering, credential theft, ransomware, or malware.
2. Ongoing risk management and incremental improvement: MDR service providers can offer valuable guidance, security insights, and threat intelligence updates, ensuring security controls stay up-to-date and prepared to combat the latest threats.
3. Cost-effective incident response: MDR enables organisations to improve the cost-efficiency of their cyber security investment by providing access to optimal detection and response capabilities through a subscription-based service.
4. Insider threat management: MDR services can address the complexity of insider threat management by developing identity and access management strategies and proactively monitoring employee behaviour.
5. Proactive compliance management: MDR providers can make compliance management more manageable by identifying security gaps and suggesting controls to maintain compliance with regulations such as PCI, HIPAA, HITRUST, NIST, ISO, GDPR, and SOC 2.

MDR makes cyber risk management more manageable by offering expert guidance and increasing the cost-efficiency of security strategies. This expertise enables organisations to adapt to the latest threats and consistently meet regulatory expectations.

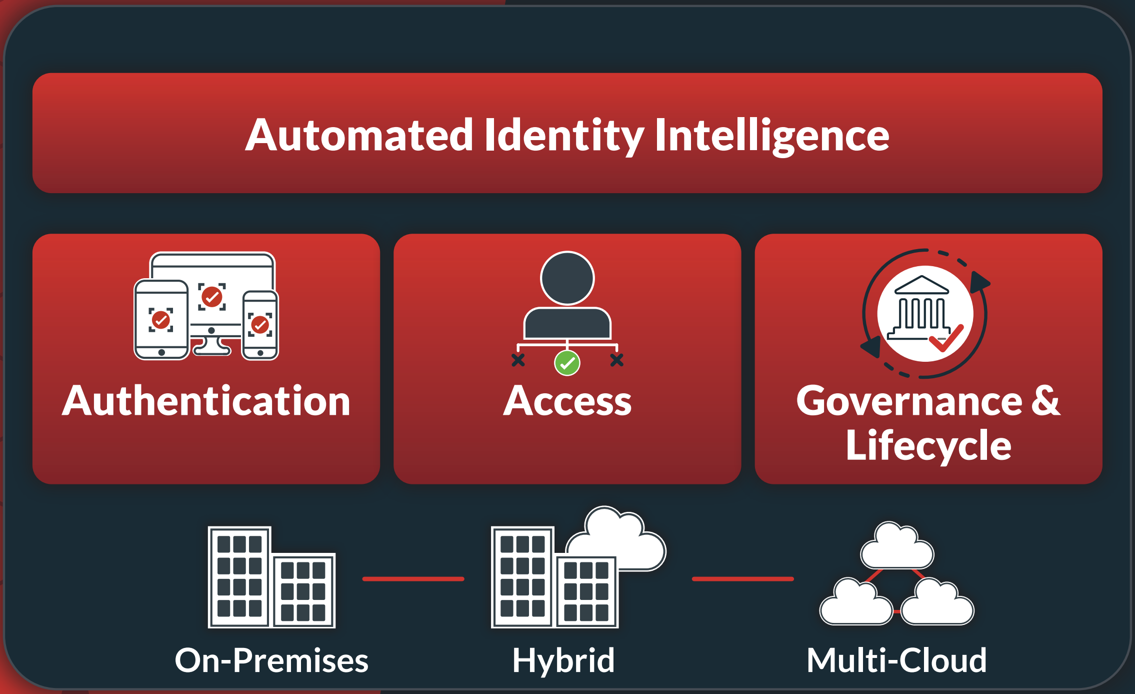
To find out how MDR can help simplify your cyber risk management, contact us today.

92% of companies are either using or plan to use AI and machine learning to bolster their cybersecurity.
5
Key SOES findings
mimecast
Cyber Risk Commands the C-suite's
FOCUS
The State of Email Security 2023
Reducing Cyber Risk through Cyber Awareness

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/



3 reasons to transform your security with XDR

Trellix

Imagine if your business could consolidate security tools into a holistic ecosystem that's always learning and adapting to keep you safe.

With extended detection and response (XDR), you can. It empowers you to identify and address incidents, simplify complex security products, and build a reliable security infrastructure.

Here are three reasons organizations adopt XDR:

1. Strengthen detection, response, and protection

As threat actors and attacks continue to evolve, risk management is becoming increasingly complex. Your organization must be able to detect and respond to threats in real time, powered by the right tools and insights.

20.9 hours

The average time to respond to a global incident is **20.9 hours**[1]

31%

Cyberattacks increased **31% from 2020 to 2021**[2]

2. Improve productivity

The security operations center (SOC) often has limited staff but an overwhelming number of security tools to manage. This hurts productivity and speed when you need it most—to stay ahead of growing threats.

70%

By 2025, **70%** of organizations will consolidate the number of vendors securing the life cycle of cloud-native applications to a maximum of three vendors[3]

3/4

By 2025, three-quarters of large organizations will be actively pursuing a vendor consolidation strategy, up from approximately one-quarter today[4]

3. Lower total cost of ownership

Organizations want to increase security operations efficiency. But buying best-of-breed products and building custom solutions is costly, and they may not be resilient enough for the future security landscape.

70%

70% of organizations have invested or plan to invest in XDR[5]

50%

By 2027, **50%** of midmarket security buyers will leverage extended detection and (XDR) to drive consolidation of workspace security technologies, such as endpoint, cloud, and identity[6]

Ready to breathe new life into your business with XDR?

Visit trellix.com to get started today. Or talk to one of our XDR experts to learn how Trellix can help grow your business.

1. Voice of SecOps, Deep Instinct, 2021
2. State of Cybersecurity Resilience 2021 , Accenture, 2021
3. Predicts 2022: Consolidated Security Platforms Are the Future, Gartner Research, 2021
4. Security Vendor Consolidation Trends—Should You Pursue a Consolidation Strategy? Gartner Research, 2020
5. ESG Research Highlights: Impact of XDR in the Modern SOC, Mandiant
6. Predicts 2022: Consolidated Security Platforms Are the Future, Gartner Research, 2021

netskope

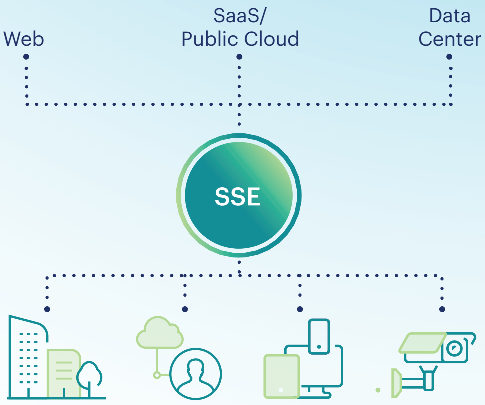
Ready for Anything

Intelligent Security Service Edge for a SASE Future

Cloud transformation and hybrid work have changed how networks and security need to work. Netskope sees and understands these changes and works to optimize and secure access to SaaS, web, and private apps on any device, anywhere, no matter what.

With Netskope:

- Use a simple, truly converged platform in the cloud
- Understand context and risk to protect data anywhere
- Create good digital citizens with a positive user experience
- Get blazing-fast security with one of the world's largest private security cloud networks



Netskope protects over 25 of the Fortune 100

2 of the world's 4 largest retailers	3 of the world's 4 largest commercial banks	5 of the world's 7 largest healthcare providers	2 of the world's 3 largest telecom companies

> "Netskope's partnership is very important to the success of our digital transformation, plus it's easy to use."
>
> **Network Manager at telecom company**

> "We rely on Netskope to ensure safe cloud and web usage across our organization."
>
> **CISO at a large bank**

Ready for Anything

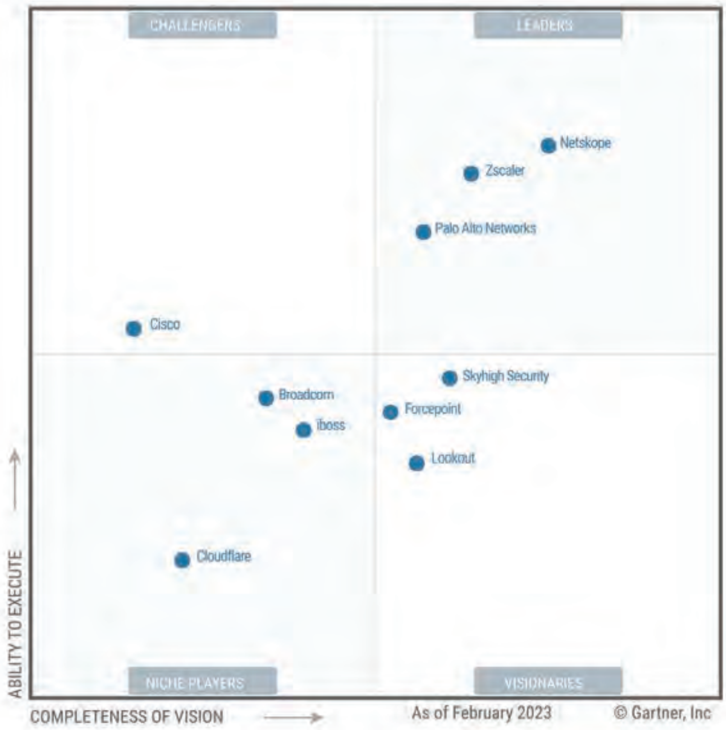
INDUSTRY RECOGNITION

Netskope named a leader in the **2023 Gartner® Magic Quadrant™** for Security Service Edge for 2nd year in a row

Highest in execution and furthest in vision

Get the report

Figure 1: Magic Quadrant for Security Service Edge



Source: Gartner

Netskope is built for performance and scale

The Netskope Security Cloud is the fast and secure onramp for more than 230 million users around the globe. Netskope processes more than 50 billion cloud and web transactions a day and scans more than 60 million files.

Netskope is known for innovation and culture

Netskope is regularly called out for product innovation, for the industry contributions of our leaders and customers, and for company culture. In addition to numerous industry awards, Netskope inventors hold more than 125 patents worldwide and that number continues to grow.

Our team is a competitive advantage

Established in 2012, Netskope was founded by early architects and distinguished engineers from security and networking leaders like Palo Alto Networks, Juniper Networks, Cisco, and VMware. As we've grown, our hiring philosophy has stayed the same. Hire people who are better than you, then empower them. Let them do what they know they can do. Let them be entrepreneurs. Give them the freedom to unlock their capabilities. This is how you build great products. This is how you build a great company. And this is how we continue to build Netskope.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Netskope. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

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

Skyhigh Security

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.

Integrity360
your **security** in mind

The Reality of Ransomware: What You Need to Know in 2023

By Matthew Olney, Integrity360

Ransomware has become a frequent threat to organisations since the WannaCry attack in 2017, and the trend is increasing. In the first half of 2022, over 236 million ransomware attacks were reported worldwide. These attacks now account for 10% of all breaches, including high-profile incidents targeting companies like semiconductor chip company Nvidia and car manufacturer Toyota. Criminals are developing new techniques to extort organisations, and it's crucial to understand what ransomware is and how it's evolving. Traditionally, ransomware attacks involve hackers breaking into a network, identifying critical data, and encrypting it. They demand a ransom to regain access to the data. But in recent breaches, hackers not only encrypt the data but also exfiltrate it to sell it if the victim doesn't pay. This puts the hackers in a win-win situation. Prevention is essential to avoid a ransomware breach.

4 Things to know in 2023

Ransomware attacks have evolved to threaten confidential information and pressure victims into paying the ransom. Here are four key things to know about ransomware in 2023:

1. Prevention is Critical: Hackers are gaining access to confidential data, and paying the ransom is often the only option to prevent public disclosure. Prevention is the best defence against encryption and leakage, so it's vital to ensure all computers have updated anti-malware software, and Managed Detection and Response (MDR) continuously monitors the network.
2. Hackers Aren't Only Financially Motivated: Cybercriminals are increasingly interested in IP theft, sabotaging companies for political reasons, activism, or whistleblowing. Some governments use cyber gangs for espionage to gain access to data for political aims.
3. Ransomware Attacks are Relying on Insiders: As the ransomware-as-a-service model becomes more popular, attackers are bribing employees to inject malware into their company's networks as part of an insider attack. These attacks are difficult to defend against and prove, making it essential to educate employees on detecting phishing emails.
4. Educating Employees is Key: Phishing emails are often the starting point for ransomware attacks. It's essential to educate employees on how to detect phishing emails through security awareness training and phishing simulations.

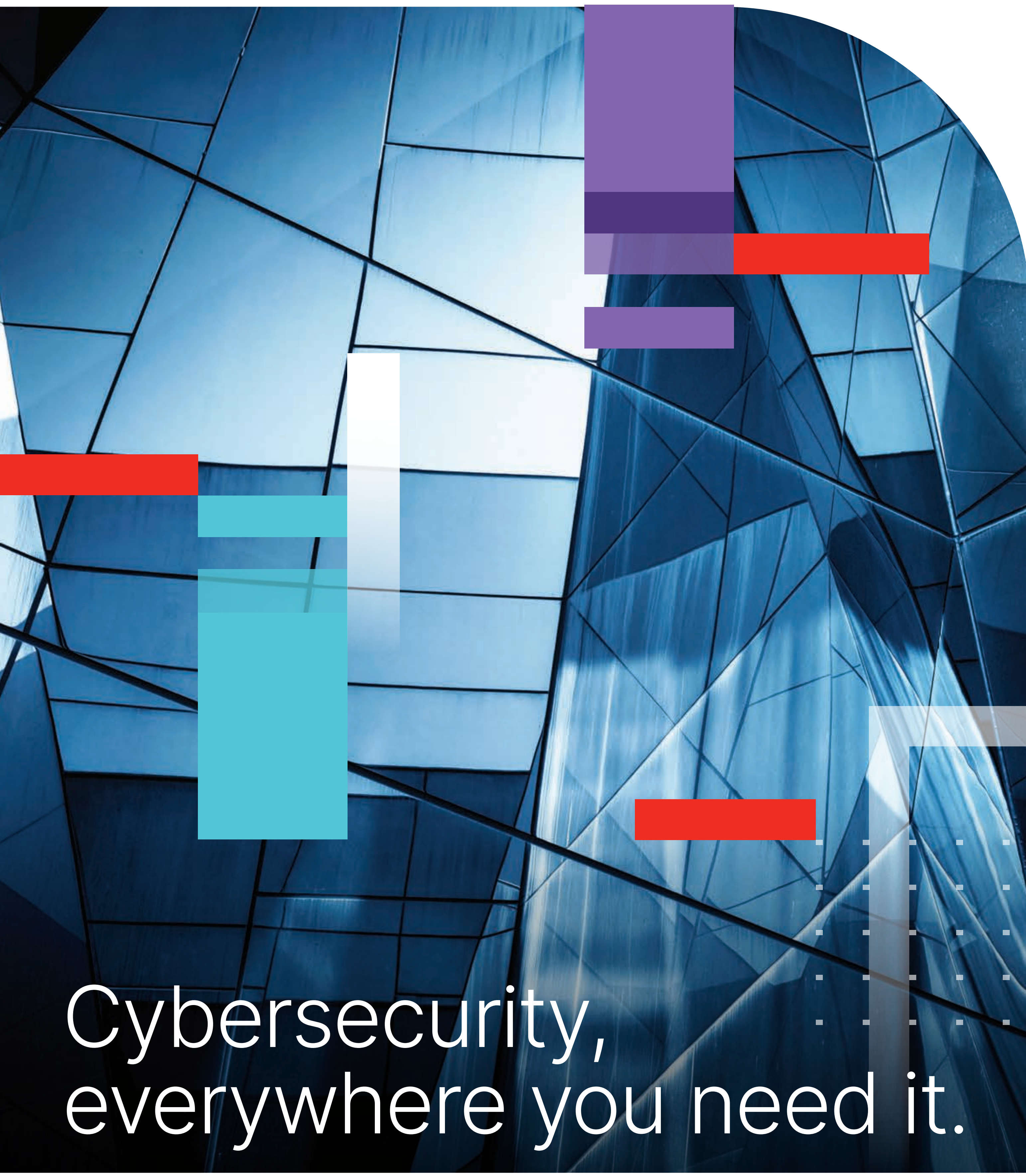
In 2023, organisations need to change their defence mindset and focus on prevention. Educating employees on the latest threats is critical to avoid mistakes and downloading attachments that put the organisation's data in a lose-lose situation.

www.forcepoint.com

Forcepoint

Security. Simplified.

9
SET
<J15>
23346287411
74%
//F1X-1533//
MODUL


Cybersecurity,
everywhere you need it.

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