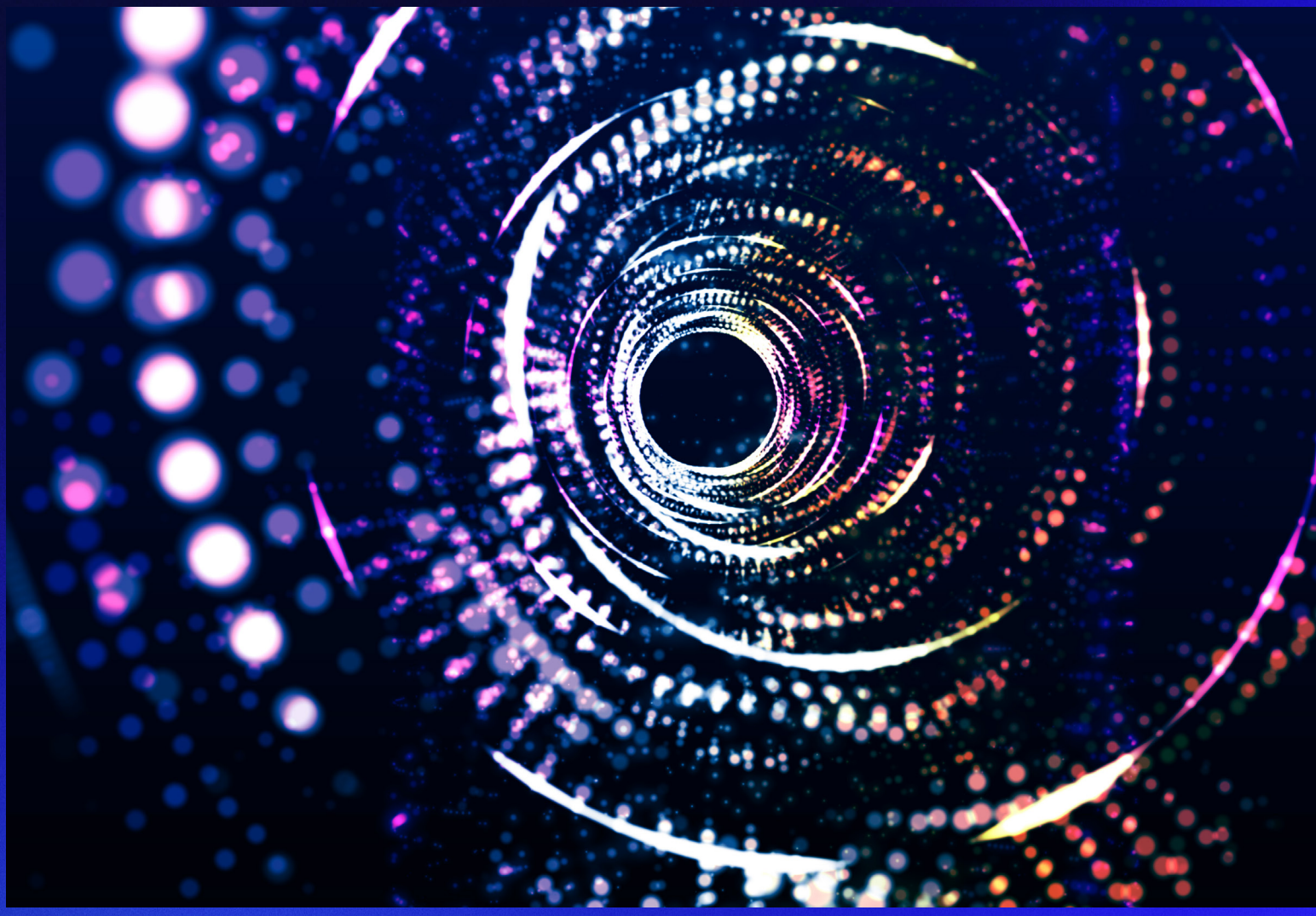
Secureworks®

WHITE PAPER

BEYOND THE ENDPOINT

Tackle Your Biggest Cybersecurity Problems Today



"Secure the endpoint" instructed the old model of cybersecurity. But endpoint-centric security can no longer protect your precious data the way it once was able. That's because cybersecurity incidents now originate from almost anywhere in the IT stack. And in the case of our 4,500 plus customers, over 60%[1] of essential threat event and detection data no longer comes from endpoints, meaning threats can bypass your endpoint detection completely.

For this reason, many organizations are now looking forward and considering how they can maximize security and efficiency at the same time. These realities are making many security organizations rethink how they should make their security both strategic and future-proof — and who will be the best partner to support them.

THE CURRENT STATE HAS CHANGED:

At one time, endpoint security was the be-all-end-all of cybersecurity health. Perhaps the most significant challenge facing organizations today is recognizing that things have changed. Today, their limited visibility of threat events outside the endpoint is a serious risk. The missing event data that would enable them to provide more effective and earlier risk detection and mitigations is being lost in the mix of cloud, apps, email, identity systems, and more.

This disconnect may help explain why 68%[2] of organizations indicated attack frequency increased over the past year. And when nearly two-thirds[1] of event data now stems from outside EDR telemetry data, organizations may be leaving far too many threats undetected and unknown until it's too late!

Everything has changed. Effective cybersecurity now depends on uncovering known and unknown threats as they happen and dealing with them rapidly and accurately to minimize any potential security issues.

What's next for organizations looking to make their security operations more effective and efficient while still harnessing the value of their essential EDR layer?
Let's start with what we know:

Cyberattacks continue to circumvent EDR

Unbridled growth in the volume and sophistication of attacks has been the inevitable result of (ironically) better endpoint malware protection and EDR security. Other factors include the growth in remote work, as well as the high rewards bad actors can obtain by a successful breach.

There's also the growing list of assets organizations need to protect themselves throughout digital transformation, including collection and storage of even more data and the resulting digital links to a growing cohort of customers, suppliers, partners, and contractors. These dynamics increase an organization's attack surfaces exponentially.

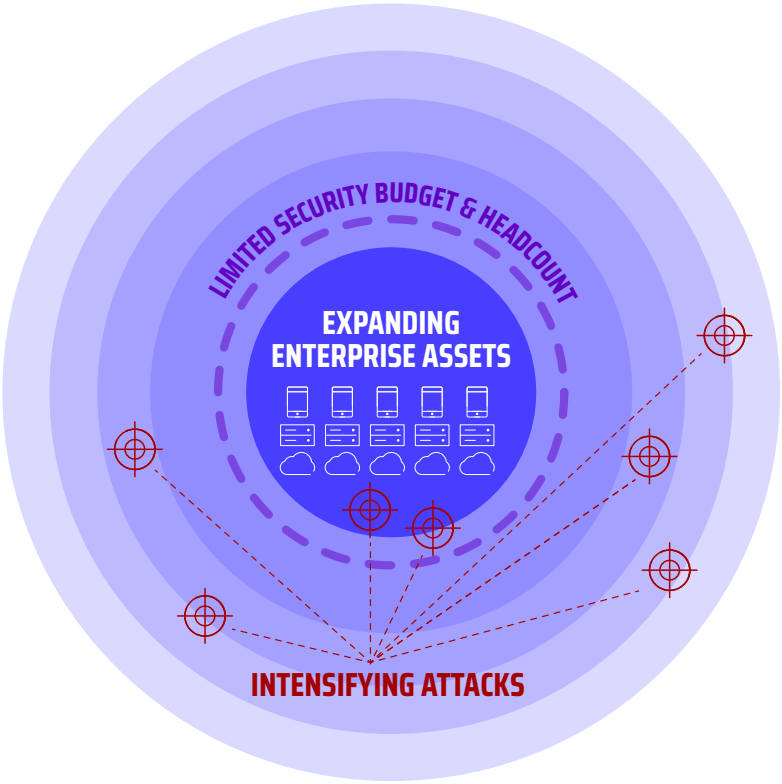
Threat actors know this and are being creative in attacking those areas outside the endpoint, or simply bypassing or neutralizing endpoint defenses.

[1]Source: Secureworks® Taegis™ XDR customer event and telemetry data
[2]Source: Ponemon Institute, Jan. 2020

SCALE IS ESSENTIAL — BUT EVERYTHING IS IN SHORT SUPPLY

Budgets are finite[3] and so is the supply of skilled and affordable security specialists[4]. Organizations must also consider limits to how many discrete security tools and services any security team can effectively integrate and successfully operate without being stretched too thin.

These complex circumstances challenge organizations to appropriately scale their security management operations in an efficient and cost-effective way, especially when facing vital needs to address the serious cybersecurity problems they face.



Given intensifying attacks, continued expansion of the enterprise environment, and finite resources, SecOps teams today need to mitigate cyber risk far more efficiently.

Looking deeper, organizations are facing what amounts to a "double whammy" of difficult conditions. Not only must they make their security operations more effective by scaling to cover the entire IT infrastructure, but organizations must also make security operations vastly more efficient as the process of recruiting and retaining skilled security staff becomes more costly and difficult than ever.

But the truth remains that unless organizations start to rapidly achieve the security efficiencies needed to neutralize attacks effectively and at scale, they will continue to face today's unacceptable levels of cybersecurity risk — and the astronomical costs that go with that risk.

[3] Source: Corporate cybersecurity spending rose about 11% in 2022, from $155B to $172B (Gartner)

[4] Source: Cyber Skills Shortage is Caused by Analyst Burnout

THE GOAL IS MAXIMUM MITIGATION EFFICIENCY:

There's a term we've created to help organizations evaluate and understand the overall ability of their unique organization to meet the challenges of running cybersecurity at scale: **mitigation efficiency**. A thorough evaluation of mitigation efficiency can help organizations get maximum business security value from their solutions, despite having finite resources and budgets.

Mitigation efficiency is the ratio between two metrics:

i) Total Mitigated Risk
ii) Total Cybersecurity Spend

Total Mitigated Risk:

This metric is based on the quantified cost impact that a successful breach could have on your organization. Those cost impacts will be unique to your organization — and they are not a raw count of how many different active threats you find or how many CVEs you patch. Rather, total mitigated risk looks at your potential real-world breach costs as an all-inclusive cost impact on the organization.

This also looks at how your current mitigation capabilities can affect that cost. For example, being able to identify and neutralize an active ransomware threat within a few hours of the initial ingress will result in significantly lower costs for total risk mitigation and higher savings versus if the mitigation was post-encryption and executing recovery.

Total Cybersecurity Spend:

This metric incorporates all the hours, tools, services, and other resources your organization currently requires to protect against and stop attacks.

This mostly consists of explicitly budgeted cybersecurity/security operations line items. It also includes the IT hours devoted to security-related activities, non-technical hours devoted to cyber hygiene training, and premium/differential pricing paid to vendors to ensure compliance with any rigorous security standards.

Getting Value from Mitigation Efficiency:

The practical application of mitigation efficiency is not in calculating a score for your organization. That's almost never as simple as a formula. Your environment may be too large and complex for you to accurately estimate the number of different business risks you're mitigating every day. You may have special industry factors that inherently increase your risk. Every organization is different. Instead, look at the practical logic of better efficiency.

A practical application of mitigation efficiency is in helping you to recognize the factors that will profoundly impact mitigation efficiency — and by understanding those factors be able to further justify addressing them immediately.

Ultimately, organizations must improve their efficiency to successfully meet the challenges of delivering cybersecurity at scale.

COMMON EFFICIENCY CHALLENGES

Common factors undermining the ability of organizations to boost their mitigation efficiency include:

Over-Emphasizing EDR

Today's threats have moved beyond the endpoint-centric, EDR view of adequate protection, as we now have perimeter-less IT infrastructures that need all assets covered under a single detection blanket. This includes remote endpoints, distributed networks, cloud systems, business systems (email, credentials), cloud applications, IoT and more.

Tactical vs Strategic Security

Such is the relentless nature of today's attacks that security teams often find themselves putting out fires all day, every day. This short-sighted, tactical action makes it difficult to look at the bigger picture and assess how time and resources may be more strategically and effectively allocated.

Siloed Security

Security operations toolkits have become larger over time and with that, renewal and operational costs have exploded. The average number of tools in use by an enterprise in 2022 is 76[5]! This makes licensing, training, learning, management time, and the inefficiencies resulting from toggling between tools greater than ever. What's more, many security layers operate in a security silo, raising the complexity and difficulties of seeing and responding early to threats.

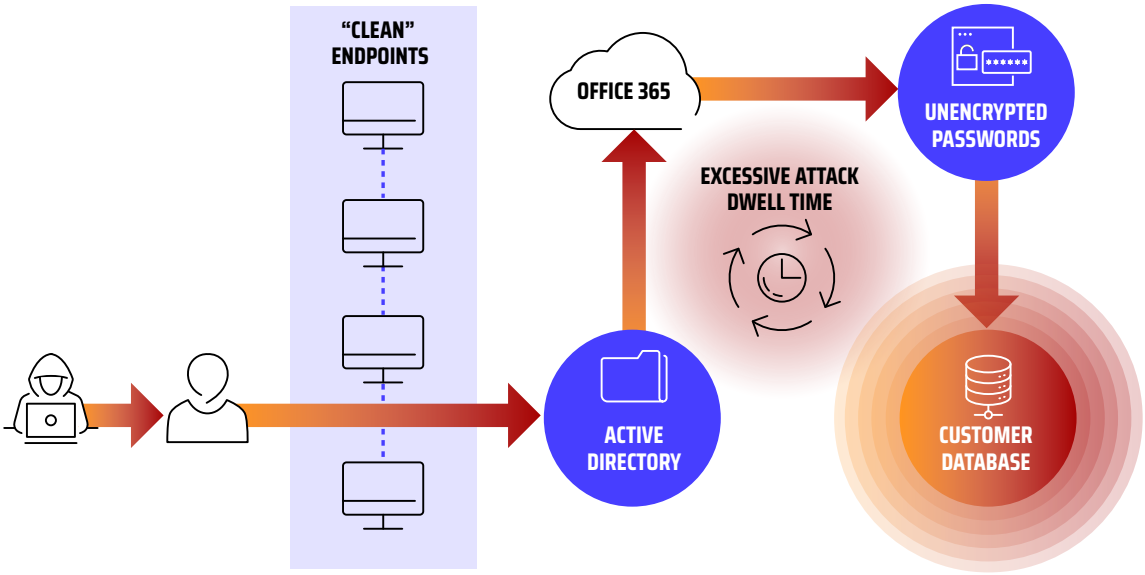
Lack of Transparent Security Partners

Very few vendors offer security solutions and services that maximize business value and tackle both cost effectiveness and efficiency. Instead, security teams are left to "make it work" despite fragmented toolkits, high workloads, and poor event visibility. Organizations need a trusted vendor security partnership that will make cybersecurity work for them, underpinned by a close and transparent partnership.

A Serious Lack of IT Personnel

Far too many organizations lack a dedicated or highly professional SecOps team that is available 24/7 — even though threats never take a break. Resource constraints often mean that organizations have only a few security analysts. Even worse, a small IT team may be left to deal with lackluster endpoint and/or network managed service providers, clouding visibility across the organization's risk landscape!

[5] Source: Panaseer Security Leaders Peer Report 2022



An obsolete endpoint/perimeter approach to security leaves organizations excessively vulnerable to sophisticated attacks that bypass traditional endpoint monitoring.

GO BEYOND THE ENDPOINT: FOUR WAYS TO WIN BETTER EFFICIENCY

What can you do today to increase efficiency and effectiveness and achieve the defense-at-scale necessary to meet the cybersecurity challenges you are facing?

Here are four essential steps that will immediately help you start winning at the mitigation efficiency game:

1. Make Mitigation Efficiency an Immediate Goal.

It's critically important to be able to scale your future business and cyber risk mitigation. To do this, you need to make a full commitment to efficiency and effectiveness by providing a strategic security operations solution that keeps your team from being forced into a constant pattern of tactical "firefighting."

Many organizations scale and yet miss the mark on efficiency — often turning to managed detection and response as a good solution. But for more complete visibility and tangible future-proofing, the strategic move to using outside help is opting for a managed extended detection and response (ManagedXDR) platform. This shared platform approach offers more collaboration and better insight, and often has little or no extra operational cost difference from MDR.

2. Harness EDR by Moving Beyond the Endpoint.

Organizations seeking better value and greater efficiency can benefit greatly by moving decisively away from a defend-the-perimeter, endpoint-centric defense model. That approach limits security visibility and doesn't help teams tackle all of their real risks.

EDR on its own misses too many threats and allows them to dwell for too long, undermining detection effectiveness and security team productivity, while also failing to boost any strategic mitigation efficiency efforts. That's why the visibility provided by XDR is so vital.

Increasing the overall event visibility that organizations have accommodates a move to a zero-trust, holistic cybersecurity approach. By combining all telemetry data within a single platform, organizations can facilitate rapid analysis and detection of active threats in near real-time.

3. Nix Friction, Maximize Value.

Security teams lose efficiency if they wait for a response or assistance from a vendor. It also costs valuable time to piece together telemetry data from different sources. And when teams lack a unified place to investigate and search for the proverbial "needle in a haystack," these factors can come together for a messy, costly, and — you guessed it — inefficient effort.

Only through integration, data unification, and automated analysis at scale can teams optimize their threat hunting, threat research and security mitigation responses. Small decisions, when powered by technical advancements like automation, can affect greater technical and human efficiency and ultimately provide real strategic value gains.

4. Identify The Right Security Mix.

With the shortage of security personnel and the disunity of many existing security solutions, it's critical that organizations can identify the correct combination of security solutions and services to meet their mitigation efficiency goals. But the reality is, most organizations struggle to retain security skills and expertise in sufficient depth to use EDR, never mind an MDR platform, effectively.

With MDR delivered on an open ManagedXDR platform, organizations can fine-tune the mix of in-house expertise and resources supplementation, leveraging on-demand security expertise and services to fill gaps on the fly. This on-demand model directly allows you to extend and partner outside resources with your security team as necessary. For example, you may wish to have a small internal incident response presence but want to access broad incident response support if a major incident occurs.

MDR on an open XDR platform also helps your team to learn from and maximize the value from existing security investments by integrating cybersecurity under a single defense blanket. Ideally, insights should be transparently shared with your team – which is why Secureworks® prioritizes this kind of transparency. Finally, MDR ensures your IT infrastructure is closely monitored 24/7/365, particularly during times when internal coverage may be reduced.

BEYOND THE ENDPOINT: THE STRATEGIC CHOICE

Given the importance of achieving mitigation efficiency, it's clear the strategic importance of deploying extended detection and response.

MDR delivered on an open XDR platform offers the flexibility to manage security operations with your own team, as well as work (in Secureworks case) with an XDR provider. Secureworks Taegis™ ManagedXDR provides an open, shared, and transparent XDR platform — because a true security partnership demands such collaboration. The delivery of MDR on an XDR platform is powerful because:

MDR on an XDR Platform Optimizes Your Current EDR Investment

XDR integrates your essential EDR endpoint telemetry defenses into a modern, holistic cybersecurity model specifically built to manage and respond to the changing nature of attack vectors across your IT environment.

Endpoint protection and endpoint telemetry data is essential, but with XDR you remove any overreliance on endpoint-specific defenses. The newly found visibility and holistic approach of XDR is ideal for helping organizations move to being able to closely monitor and support a Zero Trust model too.

MDR on an XDR Platform Integrates and Unifies for Immediate Security Improvements

XDR brings together extended telemetry and threat analysis in a way that EDR, SOAR, SIEM[6] and MDR can't achieve. An XDR platform immediately eliminates the inefficient screen-toggling that security analysts with multiple tools are forced to do, delivering a single diagnostic source that helps security teams work in a fully collaborative way to detect, identify, and stop threats. That collaborative speed is the key to quickly reducing adverse impacts and enhancing an organization's mitigation efficiency ratio.

MDR on an XDR Platform is the Most Powerful Way to Enhance Services and Support

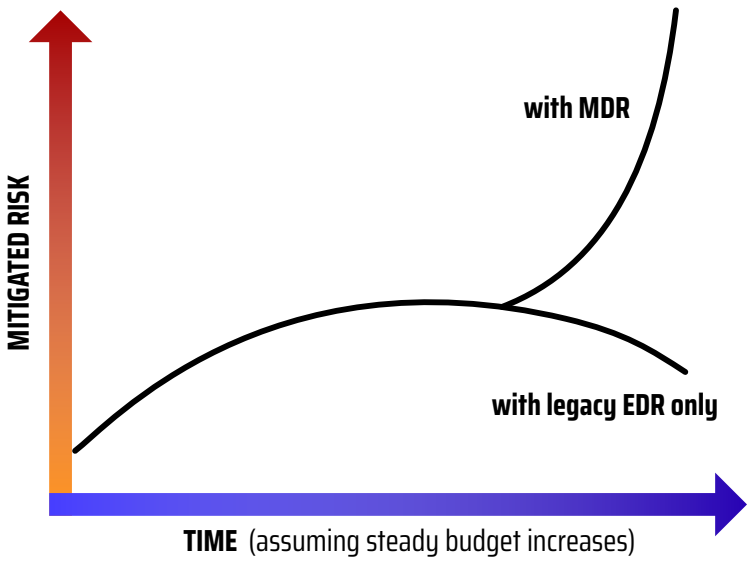
XDR is the ideal way to partner with security service providers. It allows organizations to improve security results and save money, while using comprehensive services to support their cybersecurity operations.

Whether partially or fully outsourced, the depth of security partnership you have is what really enables higher mitigation efficiency. An XDR vendor that offers a real depth of supplemental security expertise and support around incident response, threat hunting, adversarial testing, vulnerability management and other important cybersecurity services can only smooth the road to better security outcomes.

MDR Delivered on an XDR Platform Is Available Today, Right Now!

Historically, a key barrier to better efficiency has been a lack of enabling security operation solutions, there are few proven, established MDR as an open XDR platform solutions available today. That's not the case anymore. With Secureworks Taegis ManagedXDR, a security platform developed and purpose built using over 20 years of SOC management experience, so organizations can be up and running in less than 30 days.

[6] Source: XDR vs SIEM Choosing the Right Platform



MDR on an XDR platform enables security teams to continuously improve mitigation of the most serious cyberthreat well within most existing budget and staffing constraints

MDR AS XDR: THE FUTURE OF EFFICIENCY

Boosting mitigation efficiency for your organization is now within reach. Leaders who embrace MDR on an XDR platform for their cybersecurity are positioned to experience:

1. More effective cyber detection and defense at scale beyond the endpoint
2. Faster incident/event response workflows versus existing processes
3. Reduced dependence on scarce cybersecurity expertise
4. Improved access to high-value cybersecurity expertise and services
5. Better support for stronger organizational growth and agility
6. More favorable cyber insurance terms
7. Improved productivity of existing security staff
8. Better security visibility across their entire IT infrastructure
9. Security tool consolidation by better understanding of need and value
10. Few security gaps as tools and technology are unified and integrated

The only constant in cybersecurity is change — changing threats, changing technologies, and changing your approach to be able to successfully combat the adversaries you face every day. When your organization's digital presence extends everywhere and threats can come from anywhere, you must solve the problem of efficiency-at-scale. That means preparing for the realities of today — and the cybersecurity challenges of the future

To solve those problems of efficiency-at-scale you're going to need an MDR as an XDR platform at the core of your strategy, with the option for in-depth management services when you need them most. A solid XDR provider can deliver greater value than you've experienced with previous solutions, with battle-tested and proven XDR as the backbone of its managed detection and response solutions.

Reach out to Secureworks to speak to an expert who can discuss the tangible value and mitigation efficiency you can achieve with MDR as an XDR platform.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

CORPORATE HEADQUARTERS

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

EUROPE & MIDDLE EAST

France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111 00971 4
420 7000

ASIA PACIFIC

Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1800 737 817

Japan
Otemachi One Tower 17F
2-1 Otemachi 1-chome, Chiyoda-ku
Tokyo 100-8159, Japan
81-3-4400-9373
www.secureworks.jp