Security ADVISOR MIDDLE EAST

SPECIAL REPORT:

LINKSHADOW

PATRICK RAMSEYER, VP, EMEA

SPECIAL REPORT: LINKSHADOW

The Cyberthreat Landscape

The modern cybersecurity landscape is a battleground where cybercriminals continually innovate and adapt their tactics to exploit vulnerabilities. Traditional security measures, while effective to some extent, often fall short in the face of sophisticated threats. This dynamic environment demands a holistic, forward-looking approach that can identify and respond to threats before they cause significant damage. In fact, the current cyberthreat and security landscape presents a complex and ever-evolving challenge for organisations worldwide. As technology advances, so do the tactics and techniques employed by cybercriminals. In recent years, the cyberthreat-security landscape has become particularly challenging, with attacks becoming more rampant, diverse and highly organised. Some key trends and threats shaping this landscape include:

Ransomware: Ransomware attacks have surged, with cybercriminals targeting organisations of all sizes. Attackers

encrypt critical data and demand ransom payments in exchange for decryption keys, crippling businesses and causing substantial financial losses.

Supply Chain Attacks: Cybercriminals are increasingly targeting the supply chain to infiltrate organisations. Breaching a trusted supplier can provide access to multiple targets, making these attacks especially dangerous.

Nation-State Threats: Nation-states continue to engage in cyber espionage and cyber warfare. These attacks can have far-reaching consequences, disrupting critical infrastructure and posing national security threats.

Insider Threats: Malicious or negligent insiders remain a significant concern. Employees with access to sensitive data can inadvertently or deliberately compromise security.

AI-Powered Attacks: The use of artificial intelligence in cyberattacks is growing, allowing attackers to automate tasks, evade detection, and target vulnerabilities more effectively.

Challenges in Securing Critical Assets

Securing critical assets in this evolving landscape presents several formidable challenges for businesses:

LINKSHADOW'S COMMITMENT TO SECURITY IS UNWAVERING, AND IT PLACES PARAMOUNT EMPHASIS ON CUSTOMER INPUT.

Resource Constraints: Many organisations struggle to allocate sufficient resources to cybersecurity efforts. Smaller businesses may lack dedicated cybersecurity teams, while larger enterprises may face budget constraints despite recognising the importance of cybersecurity.

Rapidly Changing Threats: Cyber threats evolve at a breakneck pace. Keeping up with the latest attack techniques and vulnerabilities is a constant challenge for security professionals.

Complexity of IT Environments: Modern organisations have complex IT infrastructures, including on-premises, cloud, and hybrid environments. Securing these diverse systems and ensuring they work together seamlessly is challenging.

Trust-security balance: Managing insider threats is tricky, as organisations must balance trust and security. Implementing effective controls without stifling productivity can be a delicate balancing act.

Vulnerability Management: Identifying and patching vulnerabilities promptly is crucial. However, businesses often struggle with vulnerability management due to the sheer number of systems and applications they must monitor.

Regulatory Compliance: Navigating the complex landscape of cybersecurity regulations and compliance requirements is a significant challenge. Failure to comply can result in severe penalties.

Skills Gap: There is a shortage of skilled cybersecurity professionals. Recruiting and retaining talent is difficult, leaving many organisations understaffed and vulnerable.

Third-Party Risks: Businesses often rely on third-party vendors and service providers. However, these relationships can introduce security risks if vendors do not prioritize cybersecurity.

Security Awareness: Human error remains a leading cause of security breaches. Educating employees about cybersecurity best practices is essential but can be challenging.

Zero-Day Vulnerabilities: Cybercriminals are continually searching for unknown vulnerabilities (zero-days) to exploit. Businesses must be prepared for attacks that target these vulnerabilities before patches are available.

The current cyberthreat and security landscape demand constant vigilance and adaptation from businesses. Cybersecurity is no longer an option; it is a necessity to protect critical assets and safeguard organisational reputation. Meeting these challenges requires a multifaceted approach, including investment in technology, personnel, and training, as well as collaboration with industry peers and regulatory bodies. Ultimately, securing critical assets in today's digital world is an ongoing battle that organisations must be prepared to fight.

Enter LinkShadow

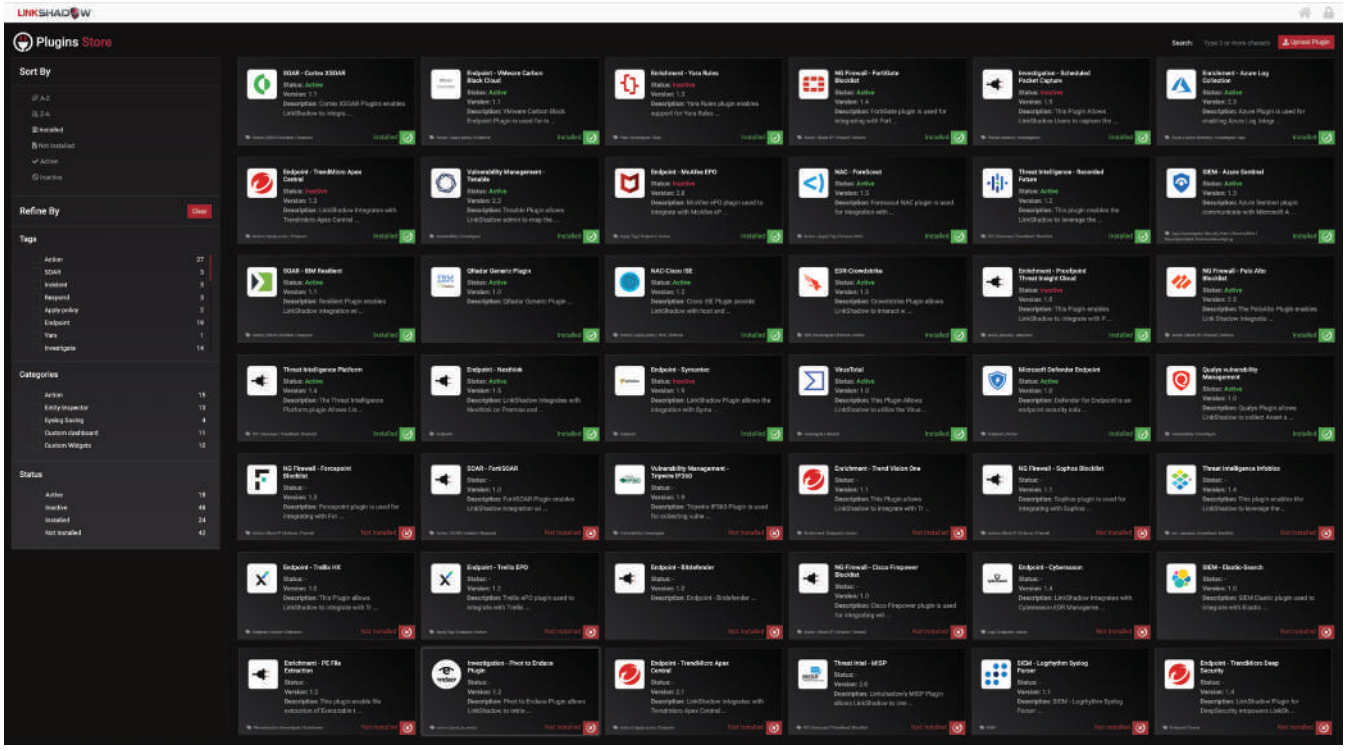
LinkShadow, founded by a team of cybersecurity experts, recognised the pressing need for a comprehensive solution that could address the challenges of the contemporary threat landscape. Established at a time when businesses were grappling with escalating cyberattacks, LinkShadow aimed to empower organisations with the tools and insights necessary to stay ahead of cybercriminals.

What sets LinkShadow apart is its holistic approach to cybersecurity. Instead of relying on siloed security solutions, LinkShadow offers an integrated platform that provides end-to-end visibility into an organisation's digital ecosystem.

LinkShadow's commitment to security is unwavering, and it places paramount emphasis on customer input. As an AI-focused company initially specialising in machine learning models, LinkShadow set out with a clear vision: to fortify organisations against advanced cyber threats, including zero-day malware and ransomware, all while offering rapid insights into the competence of their existing security investments. Over time, it evolved to provide cutting-edge Network Detection and Response solutions. In today's swiftly evolving threat landscape, where innovative cybersecurity approaches are imperative, LinkShadow stands out as a beacon of change.

LINKSHADOW PLANS TO INNOVATE AND INVEST CONTINUOUSLY IN R & D.

Patrick Ramseyer, VP, EMEA at LinkShadow, underscores the company's commitment to its customers and to the broader cybersecurity landscape. He emphasises continued focus on their global expansion strategy, with key upcoming distribution agreements set for the Far East, Africa, and Europe. "The focus remains on continuous growth, achieved primarily through a channel-centric approach. LinkShadow aims to collaborate closely with distributors, system integrators, and managed



security service providers (MSSPs). This indirect sales model aligns seamlessly with our go-to-market strategy," he adds.

In addition to expanding their reach, LinkShadow remains committed to enhancing its product offerings. The company intends to introduce new features that will further distinguish their solutions in the cybersecurity space. With an unyielding commitment to cybersecurity excellence, LinkShadow takes every step necessary to adapt to the ever-evolving threat landscape and ensure their customers have the tools and resources to strengthen their defenses against advanced cyber threats.

The Power of Many

LinkShadow recognises that no organisation can stand alone against the vast array of cyber threats. It actively collaborates with a diverse partner ecosystem and this approach ensures that its solutions are seamlessly integrated into an organisation's existing security infrastructure.

By working closely with its partners, LinkShadow extends its reach and helps organisations of all sizes access cutting-edge cybersecurity solutions. This inclusivity is essential in a world where cyber threats spare no one. Whether a small business or a global enterprise, LinkShadow's partner ecosystem ensures that everyone can benefit from robust cybersecurity measures.

By forging strong relationships with these vendors, LinkShadow leverages its expertise and technologies to enhance its own offerings. Through integration with best-of-breed security products, LinkShadow creates a synergistic approach to cybersecurity and this allows organisations to benefit from a unified and layered defense strategy.

In Patrick's words: "Collaboration is the way to stay ahead of a complex attack landscape. If you want to stop cyber criminals, if you want to stop anything bad happening, then the best way to do this is to get together. That's our philosophy, that's how we stay ahead of the curve. We leverage the best technology out there via our AI and ML capabilities. We integrate with all the top vendors in the cybersecurity market and all the top threat intelligence feeds. This creates a situation of one plus one plus one is five, because we combine the strength of all of these vendors in the market, that places us in a much more powerful position. The key to defeating cyber threats is alliances."

LinkShadow's commitment to forging strategic alliances with its partner ecosystem and leading vendors demonstrates its dedication to combating the intricate cybersecurity threat landscape. Through these collaborations, LinkShadow strengthens its ability to provide organisations with comprehensive, innovative, and adaptive cybersecurity solutions, ultimately helping them stay ahead of the evolving threat landscape and safeguard their critical assets. In an era where cybersecurity challenges continue to evolve, LinkShadow's collaborative approach stands as a symbol of resilience and adaptability.

A Different Take

The traditional siloed approach to cybersecurity relies on expecting a multitude of specialised teams and experts to safeguard an organisation's digital assets. In this model, a large organisation typically maintains a Security Operations Center (SOC)

comprised of various teams, each dedicated to specific security functions such as firewall management, endpoint detection and response (EDR), intrusion detection, and data loss prevention (DLP). However, the reality is that there is a shortage of qualified cybersecurity professionals globally, and the expertise required to excel in these roles demands a steep learning curve.

Moving from a tier one analyst to a tier three analyst involves a significant accumulation of experience and knowledge to effectively combat evolving cyber threats. This fundamental challenge is magnified by the siloed architecture, as it demands a specialist for each security area, which further exacerbates the scarcity of qualified professionals. The result is that organisations lack comprehensive visibility across their entire security landscape.

Consider this scenario: when an organisation attempts to consolidate reports from each specialised team, it can take a week or more to compile and analyse the data. In the fast-paced realm of cybersecurity, a week is an eternity, and the consequences of a cyberattack can be devastating in that timeframe. Moreover, the siloed approach can lead to gaps in threat detection and response. For example, one team may detect suspicious activity in the endpoint realm (EDR), while another remains unaware of the threat in the firewall domain. Savvy hackers can exploit these gaps to infiltrate an organisation's defenses undetected.

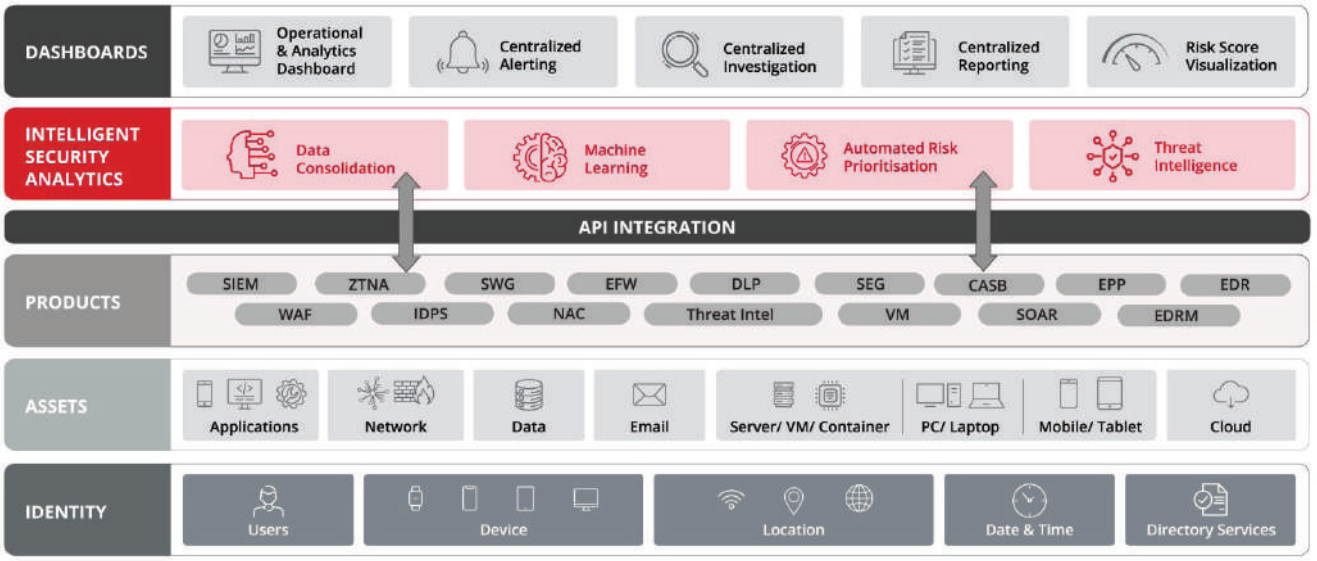
This is where LinkShadow takes a different route. It recognises that the siloed approach is no longer sustainable in today's rapidly evolving threat environment. Instead of expecting organisations to rely on an ever-expanding pool of specialised experts, LinkShadow's Cyber Mesh platform offers a unified platform that eliminates the need for silos. By providing a comprehensive view of an organisation's security posture and streamlining the monitoring of network traffic, LinkShadow enables proactive threat detection and response, bridging the gaps left by traditional, fragmented security architectures.

LINKSHADOW'S APPROACH ENSURES THAT ORGANISATIONS NO LONGER HAVE TO STRUGGLE WITH THE CHALLENGES POSED BY THE SILOED MODEL.

In essence, LinkShadow's approach ensures that organisations no longer have to struggle with the challenges posed by the siloed model. With LinkShadow, they can gain comprehensive visibility, consolidate reports efficiently, and respond swiftly to emerging threats. In a world where time and expertise are of the essence, LinkShadow's unified platform represents a monumental shift towards a more effective and efficient security paradigm.

Intelligent Security

LinkShadow's intelligent approach to security makes it a frontrunner in providing cutting-edge cybersecurity solutions. Take the case of its Network Detection and Response (NDR) solution, for instance. "Traditional NDR monitors network traffic in a 'North-South' direction, from outside to inside the network, plus a lateral East-West direction," Patrick says. "Traffic within the network is monitored by connecting to the core switch, the "Span Port." When this switch is connected, it gives a duplicate of all the traffic within the network, which allows IT teams to detect anomalies. LinkShadow's Intelligent NDR, on the other hand, is powered by AI and gives you a lot more. It actually provides Risk Exposure, which allows you to consolidate threats from all your cybersecurity tools and give you a clear



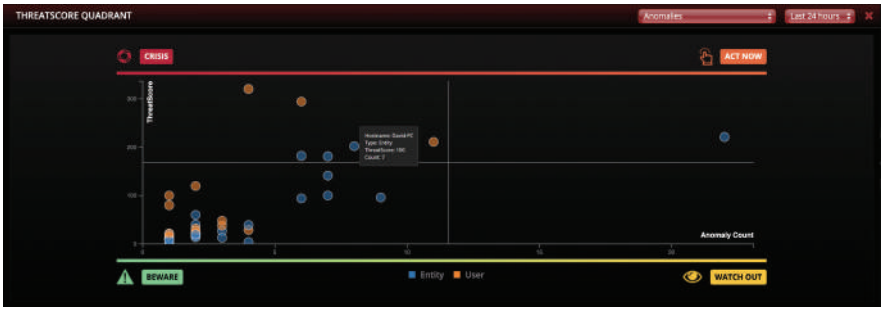
view about where you're most exposed and where your biggest risk is."

"One of the things that LinkShadow does very powerfully, is look at each device and user on a network and consider all the possible, associated risks. For example, on a computer, if the end point detection and response throws up suspicious files, if there are vulnerabilities within the OS, the security patches are not up-to-date, or if there is suspicious traffic, we'll consolidate of all this information, put it all together real-time, and give you the complete picture. In other words, we help reduce 'alert fatigue', a very real problem that security analysts and IT teams face every day. In the traditional security architecture, there is no way of knowing which alert is important. Using our Threat Score Quadrant, we prioritise the many alerts and put forward only what's really needed. We consolidate all the data sources and tell businesses where they really need to focus. Ask any SOC manager and they'll tell you that alert fatigue or 'noise' is one of their biggest problems. There are so many systems sending out alerts at the same time, that it becomes extremely challenging to differentiate one from the other. At LinkShadow, we help reduce this noise," he adds.

LinkShadow Cyber Mesh Platform

LinkShadow's Cyber Mesh Platform represents a modern and comprehensive approach to cybersecurity. Some of the advantages of this platform include:

Integration and Consolidation: Cyber Mesh integrates and consolidates security measures throughout the entire network. This ensures that security is not just an afterthought but is woven into the fabric of the network. This integration helps in closing potential gaps that might exist in a traditional siloed approach.



Better Visibility and Control: With a unified security platform, organizations can have a holistic view of their network. This enables them to identify vulnerabilities and threats more effectively, making it easier to respond to potential risks promptly.

Dynamic and Adaptive Defense: In a rapidly evolving threat landscape, adaptability is crucial. The cyber mesh architecture allows organisations to respond quickly to emerging threats. It ensures that security measures can be adjusted in real-time, helping in proactive threat mitigation.

Simplification and Reduced Complexity: Managing multiple disparate security components can be challenging and time-consuming. By consolidating security into a cyber mesh platform, organisations can simplify their security operations, reducing complexity and the resources required for maintenance.

Zero-Trust Approach: The adoption of a zero-trust approach is a significant advantage. Treating every user, device, and application as potentially untrusted means that strict access controls and authentication mechanisms are enforced. This helps in minimising the risk of unauthorized access and internal threats,

which are increasingly common in today's threat landscape.

In summary, the Cyber Mesh Security Architecture, exemplified by the LinkShadow Cyber Mesh Platform, offers a complete and forward-looking approach to cybersecurity. It addresses the limitations of traditional, siloed security measures by integrating security throughout the network, promoting adaptability, simplifying management, and emphasising a zero-trust model to enhance overall security posture. It's important for organisations to carefully consider such architectural approaches to stay ahead of evolving cybersecurity threats.

Technology Integration

With LinkShadow, technology integration is seamless and easy. The CSMA-Approach offers a dynamic and proactive approach to cybersecurity that empowers IT teams to integrate various technologies and provide enhanced visibility, agility, and a strong overall security posture.

LinkShadow already integrates with over 60 vendors and has a full team of developers dedicated to just system integrations, in Dubai alone. This means that whatever security tool a customer has, LinkShadow can integrate all of that within 15 working days, provided there's an open API. And this integration will be available to every other customer in the future. Moreover, it is built in such a way that the integration can be easily downloaded, just like an App, all plug and play. If a customer wishes to integrate an EDR, for instance, he can just download it and like any other app, it will install on his system and he will be guided step-by step on how to configure his EDR and his LinkShadow solution, so that they talk to each other.

"Our technology integration is as easy as an app. So, if a cybersecurity customer wishes to buy a new security tool, the likelihood is that it is already on LinkShadow, and if it's not, we'll integrate it for you. This is key to the Cybersecurity Mesh Architecture approach -the ability to integrate with other technologies."

The Real Benefit

In today's cybersecurity landscape, the boardroom is increasingly focused on understanding the strength of an organisation's security posture. It's not enough to simply have robust cybersecurity measures; businesses must also be able to generate comprehensive boardroom reports that convey how well-protected the organisation is. This involves showcasing the ability to consolidate and mitigate risks effectively. This is where LinkShadow helps enhance efficiency and streamline security operations.

"When it comes to investment decisions, decision-makers primarily consider two key factors: How will this benefit the organisation by reducing risk, and how will it impact the budget? It's crucial to demonstrate cost savings and operational efficiency improvements. LinkShadow achieves this by streamlining security operations. We optimise Security Operations Centers (SOCs) to enhance efficiency and reduce the need for excessive staff. This is achieved through automation and intelligent integration. One compelling example of our capabilities involves automating the integration of threat intelligence feed, saving a client an impressive two-and-a-half hours daily. This translates to 15 hours per week, equivalent to half a staff member's workload. Such integration and automation are pivotal in cost-saving strategies."

Automation is the lynchpin for financial prudence in cybersecurity. Organisations looking to make investment decisions should prioritise automation to reduce manual tasks, enhance their risk posture, and improve SOC efficiency.

Board members and CFOs require tangible evidence of the value brought to the business. They need to see a reduction in risk exposure as a direct result of adopting LinkShadow's solutions. This is especially critical when considering the average cost of a cybersecurity breach, which hovers around three and a half million dollars. In some cases, breaches can cost hundreds of millions due to extensive recovery efforts. The core of an investment decision lies in mitigating such potential financial losses.

To further understand LinkShadow's unique features and capabilities, we need to examine the metrics that matter to SOC managers. These metrics include mean time to detection, mean time to response, mean time to investigation, and dwell time. LinkShadow significantly improves these metrics by automating processes, correlating data, and leveraging AI and machine learning to enhance the efficiency of SOC operations.

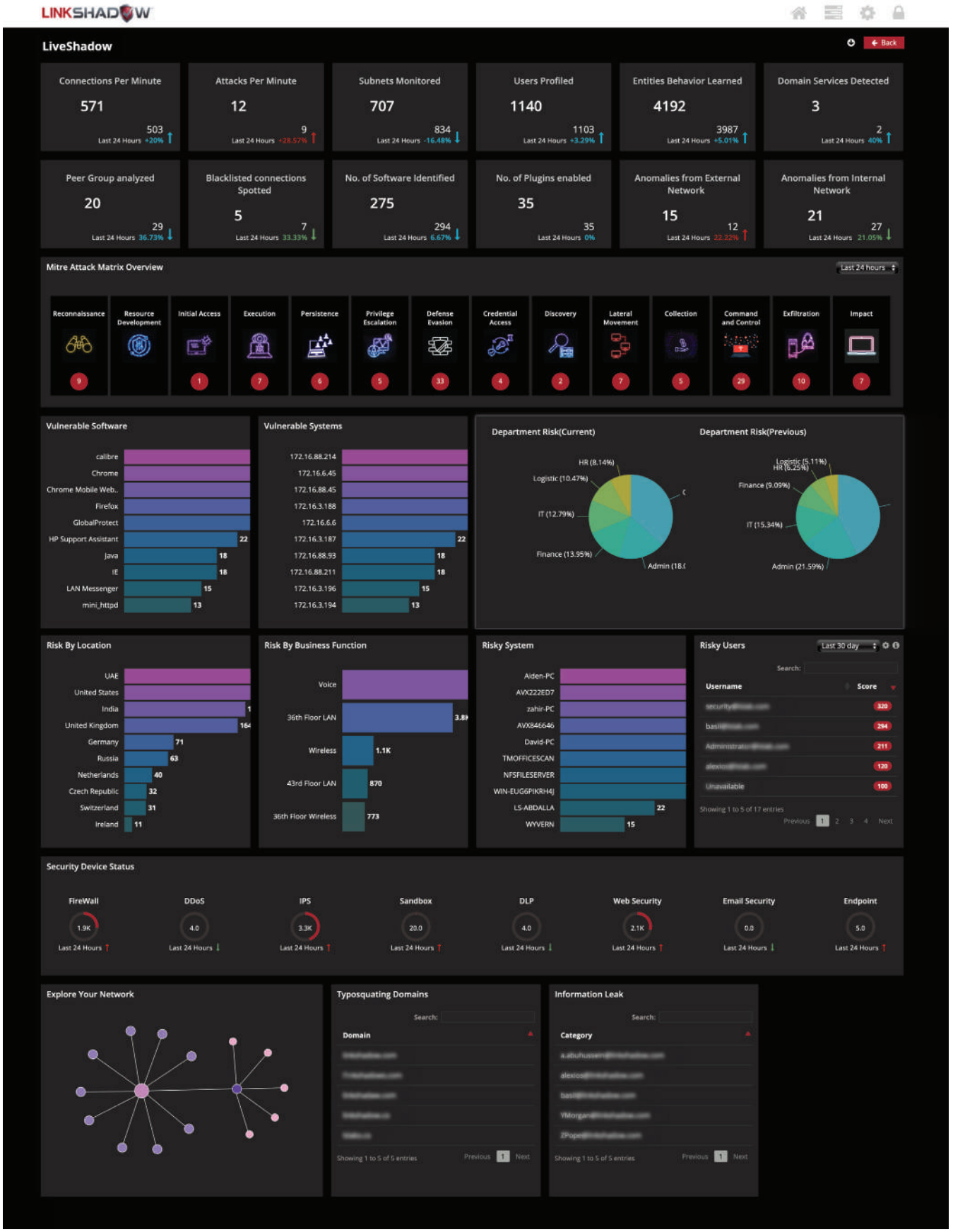
For instance, in the case of a malware threat resulting from a phishing email, LinkShadow's unified approach detects anomalies across multiple security tools. It brings together insights from EDR, email gateways, firewall reports, and other sources, providing a comprehensive view that significantly reduces the chances of oversight. This is a core aspect of SOC efficiency that has contributed to LinkShadow's strong reputation in the cybersecurity industry.

LinkShadow's ability to automate, integrate, and enhance SOC operations translates into tangible benefits for organisations, including reduced risk exposure, cost savings, and improved efficiency. These are the critical factors that guide investment decisions in today's cybersecurity landscape.

LINKSHADOW'S ABILITY TO AUTOMATE, INTEGRATE, AND ENHANCE SOC OPERATIONS TRANSLATES INTO TANGIBLE BENEFITS FOR ORGANISATIONS.

Staying Ahead

LinkShadow plans to innovate and invest continuously in R &D. At the heart of LinkShadow's success story lies its pioneering approach to harnessing the


LINKSHADOW
LiveShadow
Back
Connections Per Minute
571
503
Last 24 Hours +20%
Attacks Per Minute
12
9
Last 24 Hours +28.57%
Subnets Monitored
707
834
Last 24 Hours -16.48%
Users Profiled
1140
1103
Last 24 Hours +3.29%
Entities Behavior Learned
4192
3987
Last 24 Hours +5.01%
Domain Services Detected
3
2
Last 24 Hours 40%
Peer Group analyzed
20
29
Last 24 Hours 36.73%
Blacklisted connections Spotted
5
7
Last 24 Hours 33.33%
No. of Software Identified
275
294
Last 24 Hours 6.67%
No. of Plugins enabled
35
35
Last 24 Hours 0%
Anomalies from External Network
15
12
Last 24 Hours 22.22%
Anomalies from Internal Network
21
27
Last 24 Hours 21.05%
Mitre Attack Matrix Overview
Last 24 hours
Reconnaissance 9
Resource Development
Initial Access 1
Execution 7
Persistence 6
Privilege Escalation 5
Defense Evasion 33
Credential Access 4
Discovery 2
Lateral Movement 7
Collection 5
Command and Control 29
Exfiltration 10
Impact 7
Vulnerable Software
calibre
Chrome
Chrome Mobile Web..
Firefox
GlobalProtect
HP Support Assistant 22
Java 18
IE 18
LAN Messenger 15
mini_httpd 13
Vulnerable Systems
172.16.88.214
172.16.6.45
172.16.88.45
172.16.3.188
172.16.6.6
172.16.3.187 22
172.16.88.93 18
172.16.88.211 18
172.16.3.196 15
172.16.3.194 13
Department Risk(Current)
HR (8.14%)
Logistic (10.47%)
IT (12.79%)
Finance (13.95%)
Department Risk(Previous)
Logistic (5.11%)
HR (6.25%)
Finance (9.09%)
IT (15.34%)
Admin (21.59%)
Risk By Location
UAE
United States
India
United Kingdom
Germany 71
Russia 63
Netherlands 40
Czech Republic 32
Switzerland 31
Ireland 11
Risk By Business Function
Voice
36th Floor LAN
Wireless 1.1K
43rd Floor LAN 870
36th Floor Wireless 773
Risky System
Aiden-PC
AVX222ED7
zahir-PC
AVX846646
David-PC
TMOFFICESCAN
NFSFILESERVER
WIN-EUG6PIKRH4J
LS-ABDALLA 22
WYVERN 15
Risky Users
Last 30 day
Search:
Username
Score
320
294
211
120
Unavailable 100
Showing 1 to 5 of 17 entries
Previous 1 2 3 4 Next
Security Device Status
FireWall 1.9K Last 24 Hours
DDoS 4.0 Last 24 Hours
IPS 3.3K Last 24 Hours
Sandbox 20.0 Last 24 Hours
DLP 4.0 Last 24 Hours
Web Security 2.1K Last 24 Hours
Email Security 0.0 Last 24 Hours
Endpoint 5.0 Last 24 Hours
Explore Your Network
Typosquating Domains
Search:
Domain
Showing 1 to 5 of 5 entries
Previous 1 Next
Information Leak
Search:
Category
Showing 1 to 5 of 5 entries
Previous 1 Next

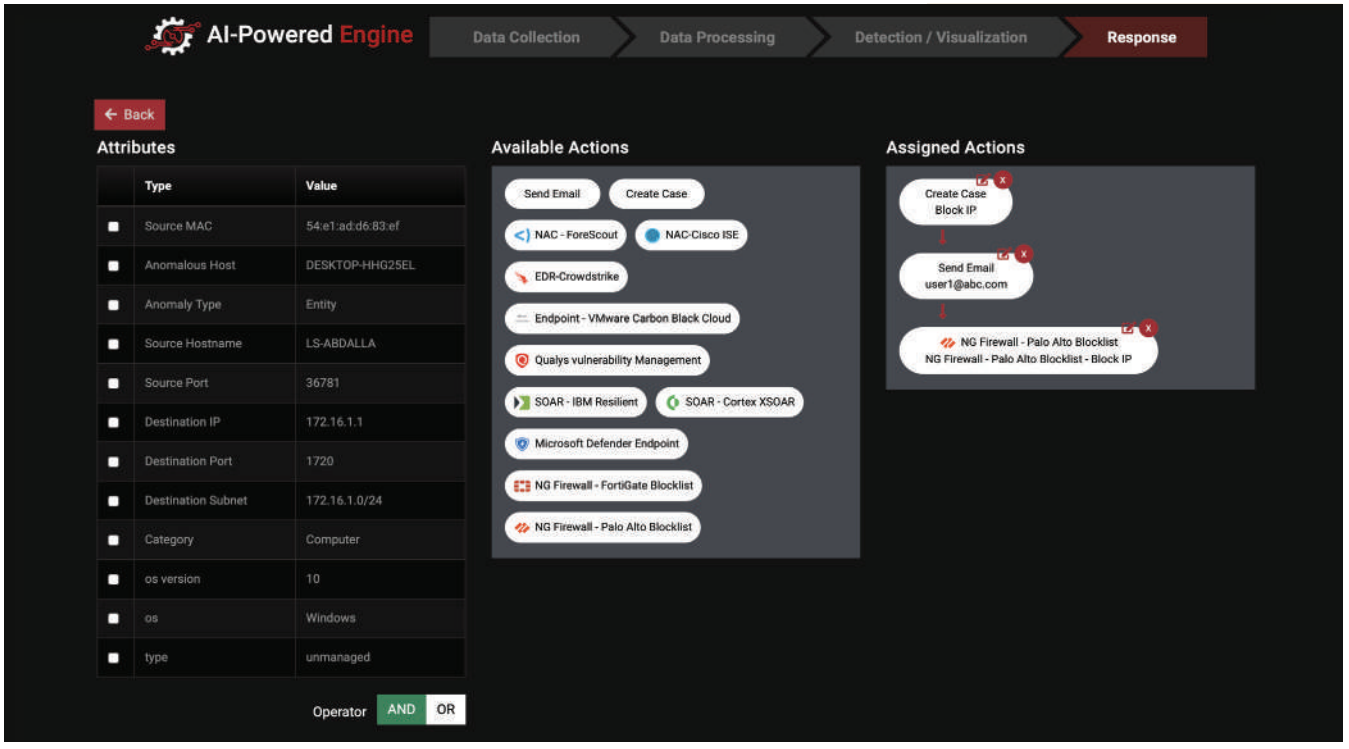
power of Artificial Intelligence (AI) in cybersecurity. While AI is often touted as a buzzword in the industry, LinkShadow recognised its true potential long before it became a ubiquitous term. The company's early realisation that AI's true strength lies in its ability to correlate and consolidate data from multiple sources set it on a path of continuous innovation.

"LinkShadow recognised early on that AI's greatest strength lies in its ability to correlate and consolidate data from multiple sources, providing a comprehensive overview of the cybersecurity environment. In the cybersecurity sector, we were discussing AI long before it became a buzzword or marketing gimmick. While some competitors also leverage AI effectively, we consider ourselves modern innovators within the industry. Our journey started with this realization and has since evolved. We've expanded our presence into various markets, including the Middle East, Asia, and Europe. Notably, we've gained the trust of major government and financial institutions, affirming the acceptance of our technology and our market positioning.

LINKSHADOW RECOGNISED EARLY ON THAT AI'S GREATEST STRENGTH LIES IN ITS ABILITY TO CORRELATE AND CONSOLIDATE DATA FROM MULTIPLE SOURCES.

Our approach has shifted from merely showcasing product features to addressing the broader business concerns of our customers. These concerns span financial, staffing, and security issues. This approach has resonated well with our customers and enhanced our reputation as a transparent company that offers a robust cybersecurity solution.

At LinkShadow, we believe in collaboration rather than claiming superiority over others. We focus on



synergy, where one plus one equals five. Personally, I'm convinced that LinkShadow is poised to become a global leader in this market due to its exceptional technology and approach.

To maintain our position at the forefront of the industry, we have a comprehensive roadmap in place. This encompasses AI advancements and numerous integrations. Our commitment to continuous innovation and substantial investment in research and development ensures that we stay ahead of the curve. Listening to our customers and sales teams remains paramount. Our approach is to understand their cybersecurity challenges and tailor solutions accordingly. In essence, our communication strategy revolves around three key words: listen, listen, listen. This approach will keep us at the forefront of cybersecurity for years to come."

LINKSHADOW CYBER MESH PLATFORM, OFFERS A COMPLETE AND FORWARD-LOOKING APPROACH TO CYBERSECURITY.

LinkShadow's innovative use of AI and machine learning has redefined the way organisations approach cybersecurity. It goes beyond marketing gimmicks and empty promises; LinkShadow integrates AI seamlessly into its solutions, enhancing threat detection, response, and investigation capabilities. This deep integration has allowed organisations to stay ahead of emerging threats, outsmart cybercriminals, and safeguard their digital assets effectively.

LinkShadow's journey is marked by significant milestones in the cybersecurity landscape. From its inception, the company demonstrated a remarkable vision, expanding its reach into various markets around the world. But what truly sets LinkShadow apart is its uncompromising stance on eliminating even the most complex of threats. In an era where cyberattacks have grown in sophistication, LinkShadow's solutions stand as a fortress against these evolving dangers. The company's dedication to bolstering security operations centers (SOCs) has resulted in remarkable improvements in critical metrics. Mean Time to Detection, Mean Time to Response, Mean Time to Investigation, and Dwell Time have all been significantly reduced, thanks to LinkShadow's intelligent automation and data correlation capabilities.

LinkShadow is not just a cybersecurity product vendor; it's a visionary trailblazer that has reshaped the industry's landscape. Its journey from recognising AI's potential to becoming a global leader is a testament to its dedication and commitment. The milestones it has achieved, combined with its unwavering focus on innovation and security, make it a formidable ally for organisations looking to protect their digital assets in an increasingly perilous cyber world.

In an age where threats constantly evolve and cybersecurity challenges grow in complexity, LinkShadow remains steadfast in its mission to safeguard organisations, and we can only anticipate greater innovations and achievements from this industry leader in the years to come. As the digital realm continues to expand, LinkShadow stands as a resolute guardian, ensuring that organisations can thrive in a secure and resilient cyber environment.

LINKSHADOW®

Intelligent NDR Cyber Mesh Platform

—The New Approach to Cybersecurity Posture —

GITEX GLOBAL

STOP BY HALL #25-C60
16-20 OCT 2023

E: info@linkshadow.com
T: +1 877 267 7313
W: linkshadow.com