IDC
ANALYZE
THE
FUTURE

MACHINE LEARNING-BASED THREAT ANALYTICS TOOLS: ENSURING A SECURE NETWORK

SURAJ GODSE
ERIC SAMUEL

SPONSORED BY:
LINKSHADOW
Combat the Dark

JANUARY 2020

IDC OPINION

The drive for diversification and growth has compelled government and private sector organizations around the world to take giant strides toward digital transformation (DX). However, as they upgrade their operations with 3rd Platform technologies and innovation accelerators like cloud, the Internet of Things (IoT), Big Data analytics, and artificial intelligence (AI), organizations are increasingly exposing themselves to serious cyber-risks, including hacking attacks by sophisticated criminals.

Transformation necessarily involves a reevaluation of an organization's security strategies. High-profile cyberattacks targeting sectors ranging from government and healthcare to financial services and aviation have highlighted organizations' vulnerabilities. Companies in developed countries are responding by adopting managed security services at a much faster pace than their counterparts in developing countries. Entities in developing economies are more often managing risks by investing in security products.

CIOs and CISOs want clear and constant visibility into their organization's security posture. Some organizations may be reluctant to outsource security management due to fear of losing control of their assets, country- or sector-specific regulatory restrictions, or resistance from internal risk and compliance teams. Many organizations are thus investing in security analytics tools to better manage their IT security environments.

Investments in security products should be complemented by an automated threat detection tool that helps IT teams identify and prioritize vulnerabilities. Such a tool eliminates false alarms and enables IT executives (who may not be cybersecurity experts) to reduce average threat detection and response times. The tool should have machine learning capabilities that make threat detection more intelligent over time. It should be capable of automatically discovering new IT assets in a client's operational environment (ensuring that organizations remain secure after they make new investments in devices and technology solutions). The tool should also be able to show how effective installed security products are in filtering risks, enabling IT executives to gain clear visibility into the effectiveness of their deployed security products.

As sophisticated data breaches are on the rise, IDC believes that one of the key solutions to solving this issue would be effective threat hunting and detection. There is no doubt that the threat hunter (security analyst) is the essential factor in tracking threats in the network, but it is important to understand that the growing amount of data being collected and analyzed is making the threat hunting process more challenging without the use of advanced technology solutions. Implementing machine learning technology in cyber security ideally addresses this challenge in threat hunting. By using behavioral analytics and applying dedicated machine learning for threat hunting, next-generation cyber security tools are enabling security analysts at all levels to track advanced attacks, prioritize threats and run threat investigations in real time. Considering the advanced cyberattacks being encountered by organizations and their growing complex network environment, IDC believes that adoption of machine learning based threat analytics tools will be critical for organizations in the coming years.

IN THIS WHITE PAPER

This IDC White Paper provides a high-level overview of the global IT security market, with a focus on vulnerabilities that pose significant risks to organizations. It discusses the challenges faced by organizations in responding to cyberattacks, highlights the importance of making investments in effective IT security solutions, and identifies best practices to ensure safe and secure operational environments. The document describes the machine learning-powered security products of LinkShadow, an innovative cybersecurity organization.

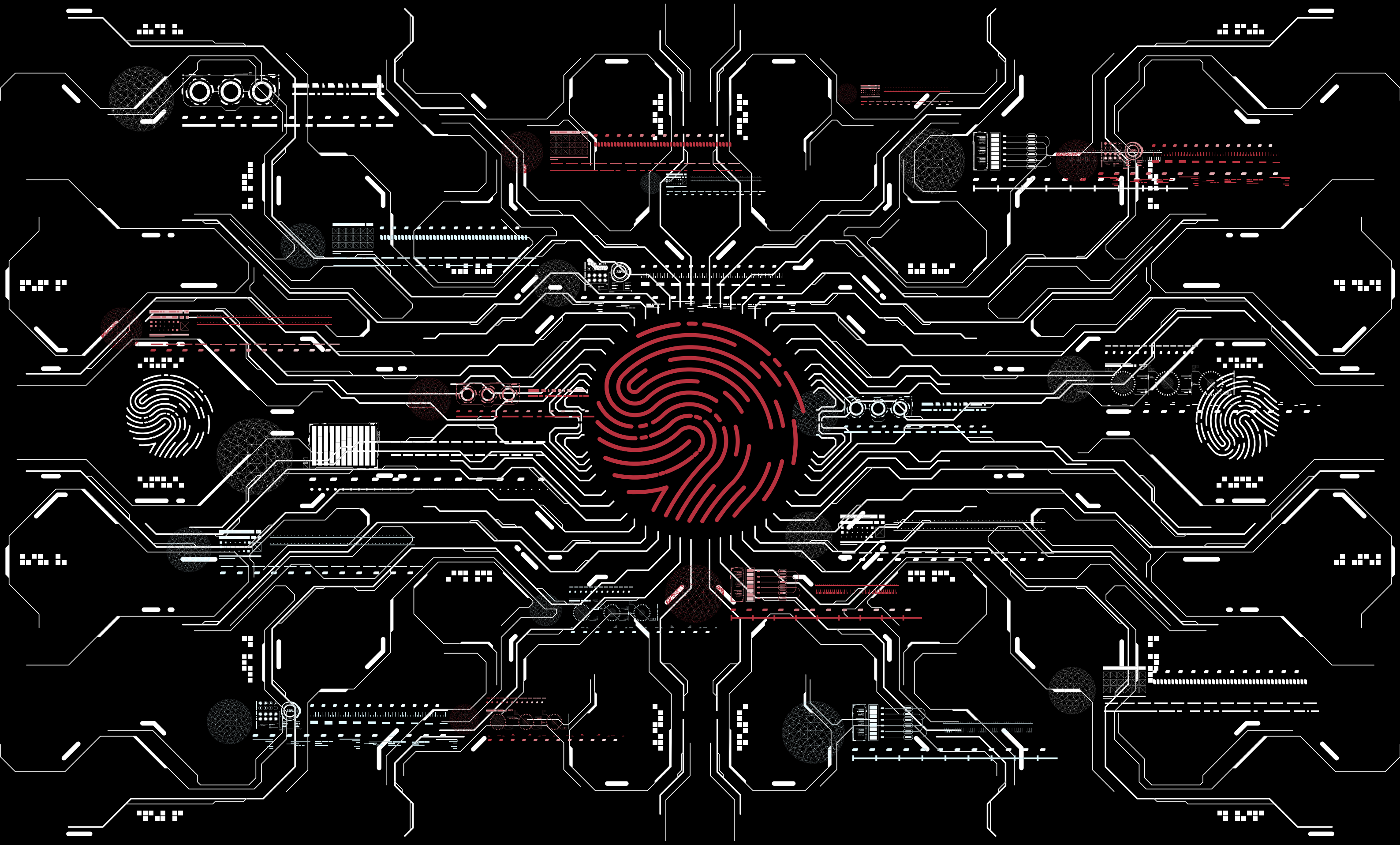
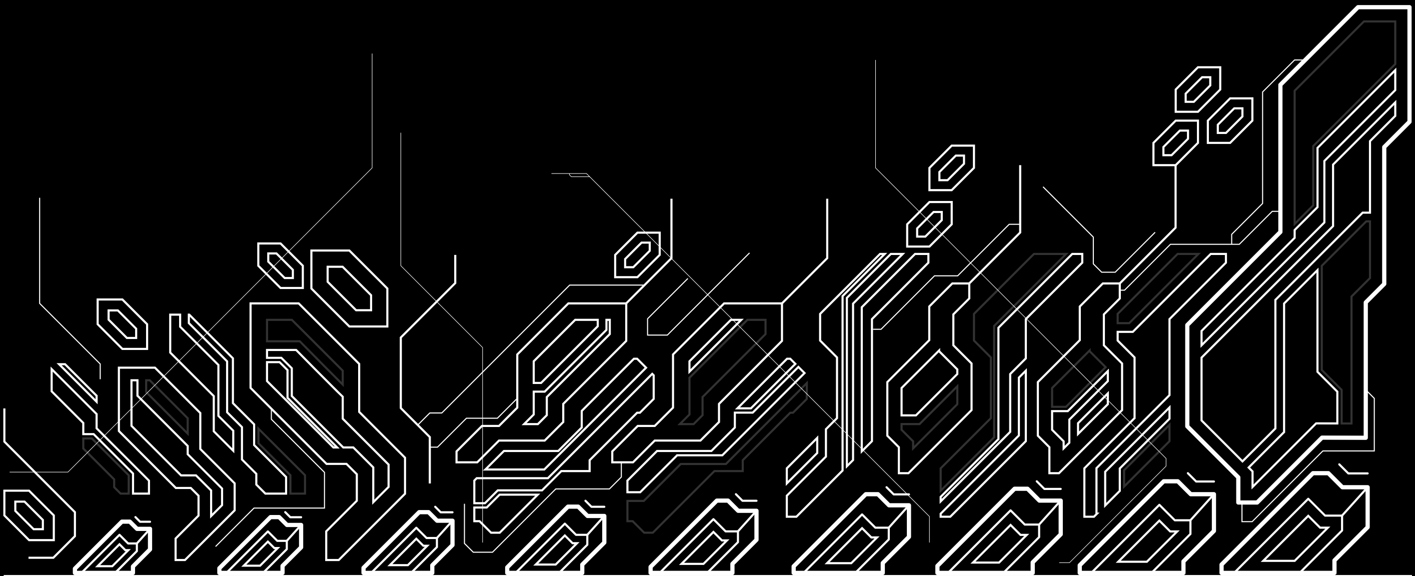
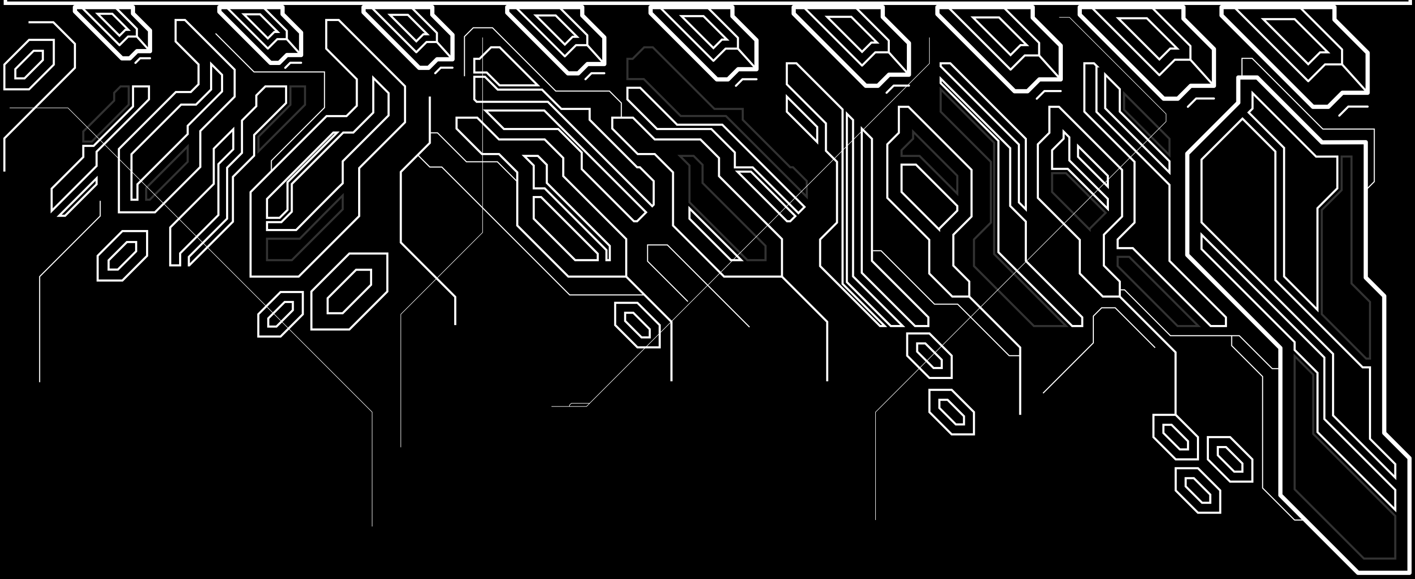


TABLE OF CONTENTS

LIST OF FIGURES





SITUATION OVERVIEW

The Global IT Security Market

Cybersecurity risks are increasing as organizations invest in new technologies, embrace open platforms, and collaborate with customers, partners, and suppliers using digital technologies. The death of the perimeter, accelerated by cloud technologies and the bring your own device (BYOD) model, is making it increasingly difficult for organizations to maintain IT security. There is a growing need for organizations to reevaluate their cybersecurity strategies and develop operational resiliencies.

According to IDC's Worldwide Semiannual Security Spending Guide, global spending on security-related solutions (hardware, software, and services) is set to grow 10.7% in 2019 to total $106.6 billion. Spending is expected to have a compound annual growth rate of 9.4%, rising to $151.2 billion in 2023. Growth will be supported by the determination of CIOs to build new trust environments that both defend against security breaches and manage reputational risks.

Nearly half, or $48 billion, of total IT security spending went to security services in 2019. Investments in security software totaled $38 billion, and $21 billion was spent on security hardware. Organizations are investing in a range of security products, including analytics tools, endpoint software, identity and digital trust software, intelligence, response and orchestration software, and network security products.

SITUATION OVERVIEW

FIGURE 1: Future View of the Security Market

Integrated Solutions

- Organizations need solutions that seamlessly integrate and talk to each other.
- Enterprises are preferring platform security that ensures the holistic protection of the entire compute platform.

Automation

- Automation can aid in increasing productivity across facets, such as configuration management, policy management, responding to alerts, and reporting.
- SecOps is a great messaging pack for organizations. This is possible only if automation is embedded into operations and development through continuous integration and continuous delivery (CI/CD).

Consolidation, M&A

- More feature sets are becoming part of broader security suites.

Open Source Standards

- Organizations are leveraging Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) open standards to improve prevention and mitigation.

New Contenders (Alphabet, Google, Microsoft)

- Data loss prevention (DLP), security information and event management (SIEM), API security, and more security features are being integrated into offerings.

Source: IDC, 2019

SITUATION OVERVIEW

Networks are becoming increasingly complex as organizations transform their business operations and deploy multiple security devices and products at different network layers. As complexity deepens, enterprises will seek management platforms that provide highly detailed visibility and that automate security and network monitoring. Vendors are investing and innovating to provide analytical tools that create transparent, safe, and secure networks.

The Biggest Vulnerabilities

Organizations face numerous internal and external obstacles that hinder their ability to deal with cyberattacks. CIOs cite external hacking as a top concern. Shadow IT systems and unintentional data leakages are cited as internal vulnerabilities. Internal risks may be minimized by enforcing security procedures and rectifying security gaps on an ongoing basis. Inadequate investments in tools that monitor and analyze IT environments, and a lack of personnel with security skills, will hobble an organization's ability to deal with internal risks.

The introduction of BYOD and cloud in the IT environment may complicate efforts to deal with cyberthreats. These technologies enable employees to connect to an organization's networks from across the globe, making it more complex for IT teams to track and secure assets. Maintaining cybersecurity will become increasingly intricate as organizations scale up DX to support on-the-move, borderless operations. An automated threat detection tool that keeps track of dispersed IT assets and triggers intelligent system logging alerts (based on the geographical movements of employees) provides organizations with the necessary capability to thwart cyberattacks.

External hacking, malware, and ransomware attacks are rising. Dealing with high volumes of such attacks may be difficult if organizations have insufficient numbers of security professionals. Organizations (even those with limited resources) can reduce this vulnerability by investing in risk-scoring tools.

SITUATION OVERVIEW

Security Challenges in the Current IT Market

Industry standards and government regulations can help guide organizations as they design their security systems. But day-to-day security management can still be daunting. Indeed, there are a range of challenges beyond budget constraints that may prevent organizations from improving their IT security postures.

Recruiting skilled security professionals remains a major challenge for organizations across the world. Another challenge is the reactive approach of many security products and solutions available on the market. These challenges are bound to elevate organizations' risk scores and keep them susceptible to cybercrime. Poor coordination between in-house security teams, weak breach detection capabilities, and the exclusion of security from software development life cycles are also challenges.

IDC research has found that IT security is not always the responsibility of the IT team: Accountability is sometimes shared with risk and compliance teams. An increasing number of IT projects are also being initiated by lines of business (LOBs). However, LOBs are often mostly focused on project outcomes and may overlook IT security. These factors may deter IT teams from effectively managing security (especially advanced threats).

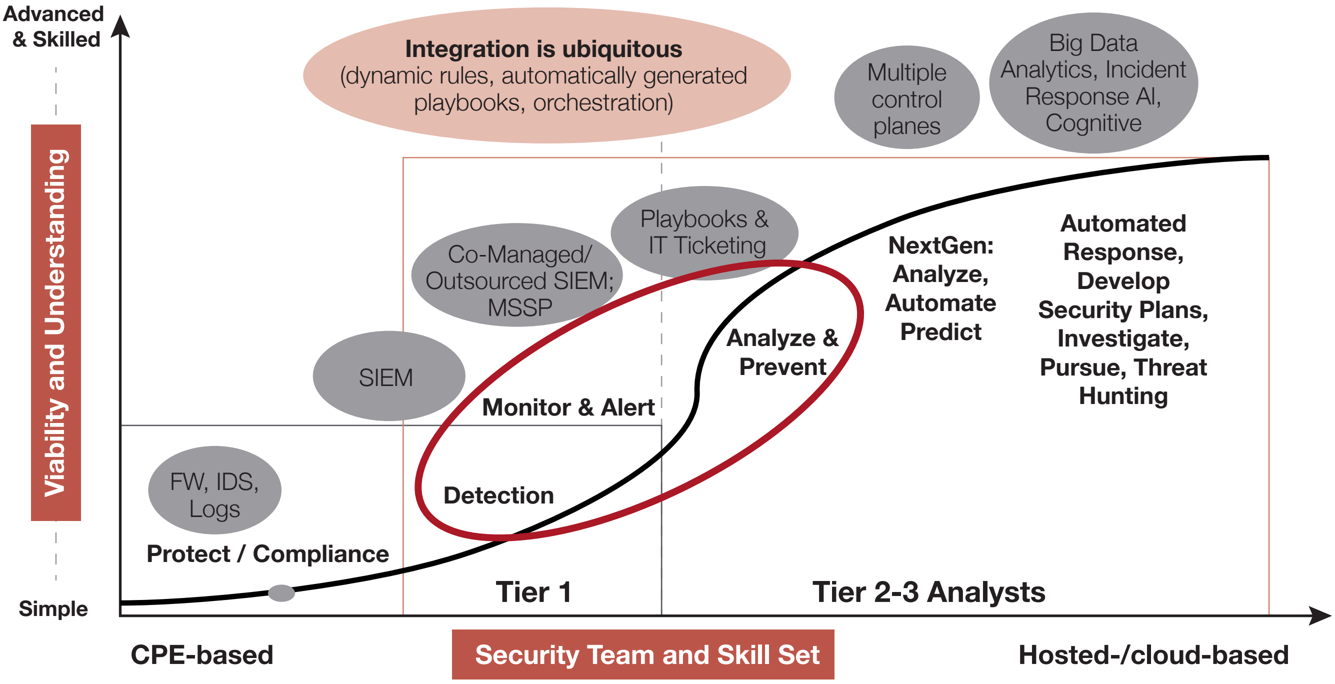
Most organizations still take a traditional, reactive approach to IT security (i.e., they invest in IT "boxes" in a bid to make themselves less vulnerable). In the digital era, however, organizations must deploy advanced and predictive security products to successfully counter cyberattacks. Many advanced products are available — but selecting and implementing the right products, and continuously monitoring security conditions, can be challenging. Some organizations are turning to managed security service providers that offer remote monitoring services or that can provide specialists to operate in-house security operations centers (SOCs). This approach may involve recurring annual costs and/or surrendering control over IT security — two things many organizations may not be comfortable with.

IT teams should consider investing in a threat detection tool that augments their capacity to detect and mitigate security risks. Internal and external risks can and should be monitored by an effective monitoring solution. A centralized or well-managed layered monitoring solution enables the security teams of different departments to respond jointly to threats and breaches. An effective detection tool enables the automatic discovery and monitoring of IT assets. It also helps IT teams measure the effectiveness of different products, enabling them to invest in solutions that improve their security postures.

Global Approaches to Expanding Security Threats

IT security has traditionally been viewed as overhead because it does not offer direct ROI. In earlier eras, security investments only rose to the top of CIO agendas after a breach in the organization or in a peer. Senior leadership typically became aware of potential financial and reputational damage to their organizations only after a breach. However, the situation is changing: Organizations understand the importance of proactive solutions and are taking the necessary steps to build strong security architectures. Organizations are moving beyond basic cybersecurity protections by fine-tuning their capabilities and leveraging advanced technologies. They are implementing tools that utilize AI, machine learning, and analytics to secure key assets and data, learn user behavior patterns, and track suspicious activities. Investments are rising in analytics, intelligence, response, and orchestration (AIRO) tools that can detect vulnerabilities in client environments and trigger automatic alerts.

FIGURE 2: Managing Security in the Digital Era


Advanced & Skilled
Viability and Understanding
Simple
Integration is ubiquitous
(dynamic rules, automatically generated playbooks, orchestration)
Multiple control planes
Big Data Analytics, Incident Response AI, Cognitive
Playbooks & IT Ticketing
Co-Managed/ Outsourced SIEM; MSSP
SIEM
FW, IDS, Logs
Protect / Compliance
Monitor & Alert
Detection
Analyze & Prevent
NextGen: Analyze, Automate Predict
Automated Response, Develop Security Plans, Investigate, Pursue, Threat Hunting
Tier 1
Tier 2-3 Analysts
CPE-based
Security Team and Skill Set
Hosted-/cloud-based

Source: IDC, 2019

These tools are of great interest to organizations that are investing in 3rd Platform technologies, innovation accelerators, and cloud-based solutions. Investments in such technologies expand the borderless organizational perimeter — and AIRO tools are essential to manage them (especially in organizations with complex IT environments).

As a step towards securing these complex IT environments, security analysts are taking more interest specially in machine learning to automate threat-hunting. Today, with the advent of big data, the quality and amount of information being captured is impressive. Threat hunting tools which are typically placed on top of all network equipment in an organization, capture the data of all the ports and protocols in the network along with the traffic and endpoint activities. This data is used as an input for machine learning algorithms which observe and analyze behavioral patterns of different entities present in the network. Machine learning algorithms process this data and present insights to the security analyst which enable them to identify threats on a real time basis and take necessary action as and when required. Machine learning is being leveraged to detect cyberthreats and give security teams time to respond to an incident before any serious damage occurs. Many of the organizations globally are adopting such machine learning powered threat hunting tools which can process any piece of captured data in the network and analyze it to present useful insights.

SITUATION OVERVIEW

Factors Driving IT Security Investments

The Rising Complexity of Cyberattacks: According to the Global Risks Report 2019 by the World Economic Forum, data theft and cyberattacks are among the top risks facing global businesses.[1] The rate of significant cybersecurity incidents in major economies has risen in recent years as organizations have actively pursued DX. Hackers are using the same innovative technologies to attack organizations — and traditional security solutions are usually incapable of detecting sophisticated threats. Organizations urgently need to make investments in advanced security solutions.

More Regulation: To protect citizen data and ensure transparent business practices, regulatory authorities are keeping a close watch on public and private sector organizations. Regional and national regulators are compelling organizations to invest in IT security solutions. In the future, there is a strong possibility that national governments will create even stricter regulations and enforce penalties for noncompliance. Expanding compliance requirements are creating another reason for organizations to invest in IT security solutions.

Enhanced Focus on Data Protection: As they implement digital strategies, organizations are exponentially increasing the amount of business data they collect — and they understand the potential of this data to create customer-centric products and services. However, capturing, collating, and storing structured and unstructured data from a range of sources may make organizations more vulnerable to data leakages. With regional and national authorities increasingly enacting data protection regulations (e.g., the California Consumer Privacy Act or the EU›s General Data Protection Regulation), organizations will need support to manage and protect the data they collect.

Increasing Numbers of Endpoints: Organizations are realizing numerous benefits from shifting applications to cloud (e.g., enabling remote staff to access centralized networks). They are also creating flexible work environments (e.g., BYOD and home office policies) that enable employees to access internal systems via unsecured networks. This vastly enlarges the number of endpoints that need to be monitored and managed — and is prompting organizations to invest in endpoint security solutions to minimize risks.

[1] The World Economic Forum Global Risks Report 2019

SITUATION OVERVIEW

Trends Shaping the IT Security Market

Scarcity of Security Professionals: The lack of skilled security professionals is one of the biggest challenges facing the global cybersecurity industry. Without trained staff, organizations cannot deploy effective controls or develop specific security processes to detect and prevent cyberattacks. Employers must strive to retain top talent, usually through generous monetary compensation and perks. High recruitment expenses, however, may exceed budgets and CIOs may not approve expensive hiring plans, compromising existing resources. The shortage of cybersecurity professionals also increases the risk of human error (i.e., employees have larger workloads and added responsibilities). The staffing problem will only get worse unless some personnel are replaced by monitoring tools or the workloads of IT security teams are reduced/reprioritized.

Difficulty Calculating ROI: In an era of limited budgets, CIOs must justify investments. However, evaluating the ROI of security solutions is difficult. There is no measurable way of quantifying all the benefits. The ROI of a product or solution may vary depending on the type of organization, region, sensitivity of data, and other factors. Depending on the complexity of its network, an organization may require different products at different layers. Assessing the value of these products may be challenging. These issues are addressed by a solution, now available on the market, that is capable of analyzing and correlating threat information and assessing the effectiveness of multi-layered, defense-in-depth infrastructure.

Best Practices to Secure an Organization

Data breaches can be expensive — and organizations are upgrading their security programs to guard against them. Security budgets have risen in recent years, but many organizations believe they are still not spending enough to protect themselves. Some security officers believe that even bigger budgets will enable them to evaluate and select the right solutions for their requirements (so long as they can justify the investments to their superiors). Hiring security professionals and building SOCs, however, can be prohibitively pricey (e.g., recruiting a data protection officer who has both IT security and legal expertise). Organizations must also purchase the necessary IT tools and establish new processes. Organizations must conduct careful analysis to select the right solutions for their industry, size, and geographic area.

A broad range of security products and services are offered by cloud and managed services providers, value-added resellers, product suppliers, managed detection and response providers, and consulting players. The expansive (and often expensive) range of offerings may create dilemmas for buyers. Buyers must also contend with IT infrastructure advancements that may increase both managerial complexities and the volume of threats. Buyers should remember that their goal remains the effective detection, response, and recovery from cyberattacks. With the threat landscape continuing to expand, companies should strive to operate a holistic, enterprise-wide security program that is proactive and predictive. They should build enhanced threat intelligence and advanced analytics capabilities and secure professional talent that can interpret and act on malicious activities.

SITUATION OVERVIEW

Organizational security has three critical elements: people, processes, and technology. Data breaches are mostly initiated at endpoints (e.g., by employees unintentionally clicking on false advertisements or links that give hackers entry into the organizational IT environment). Identity theft is also common.

As a first step, organizations should offer security training and awareness programs to help prevent employees from falling prey to cyberattacks. Providing proper education and defining user rules strengthens an organization's cybersecurity processes. Security officers must also determine whether existing IT systems align with policies. A comprehensive security management system should include integrated programs that work in sync to reduce risks and ensure compliance with policies and regulations. After organizations have deployed security products, they should invest in monitoring tools that automatically detect threats and that gauge the effectiveness of each product.

Threat detection and monitoring tools should have the following features:

- **Machine Learning and advanced analytics** – Machine learning when implemented in IT security, provides a platform that enables the system to run automated algorithms on a network and record user behavior and understand patterns to alert uncommon activities by users. There is tremendous amount of data flow in the network. It is challenging for the security analysts to inspect every packet of data and understand the user behavior. Therefore, analytics and machine learning can play a significant role in solving this challenge by providing the right insights and highlighting suspicious activities in the network. Machine learning basically addresses the following three critical areas of cyber security:

  1. **Machine learning for advanced threat hunting** – In occurrence of a security breach or compromise of the security network, the security analyst is usually flooded with alerts and notifications. Very often the window between a security breach and damage caused is very small. Attackers these days exploit such situations to accomplish their goal while the security analyst is occupied in taking further precautionary measures such as applying changes in the network or cleaning up compromised systems. At such instances machine learning helps deploy algorithms that can run through large amounts of data, bringing the most important and critical information to the front for a security analyst to take the required action.

  2. **Machine learning for malware detection** – Malware or a malicious software is an umbrella term that describes computer viruses, worms, trojan horses, spyware or any other malicious program or code that can cause harm to the system. Malwares usually infect programs or files and even spread in a computer or network environment which can make them corrupted, inaccessible, or impractical to use. Machine learning algorithms for malware detection can analyze actions which are characteristics of malicious software and flag them for further action. Over the time, these algorithms learn as they review more software and detect new malware exposing them as threats to the system.

3. **Machine learning for risk scoring** – Risk scoring can be simply defined as assigning a value/score to a threat which is determined by factors such as attack likelihood, impact of attack (if successful), and degree of exploitability of a threat on the network environment. It is difficult for organizations to allocate a risk score to all known and existing vulnerabilities by a security expert considering the time and resource it would require. Therefore, risk scoring by machine learning is a much better, data-driven and quantitative approach compared to a domain expert interpretation. This approach helps in assigning a precise point estimate to a risk which enables informed decision making for future threat scoring. However, machine learning–curated cyber risk scores also consider domain expertise and subjective inputs. Expert inputs are ingested in machine learning algorithms to have a precise risk score allocated to a threat.

- **Management Dashboard:** Managing daily security operations can be a challenge for CISOs. Having access to a dashboard that provides an overview of an organization's security posture on a real-time basis (including performance and risk indicators) is essential to enable senior management to make quick decisions in case of a breach. Such a dashboard offers key insights about an organization's current security posture and improves a company's risk scoring.

- **Auto Discovery of Assets:** Organizations and their networks are constantly growing. Multiple functions, applications, and innovative technologies are used each day. Organizational expansions involve the addition of new users. Network equipment is routinely upgraded or replaced to increase capacity or enhance functionality. In this context, automatically tracking changes is essential to avoiding system intrusions, keeping networks up to date, and monitoring devices connected to them.

- **Privileged Access Monitoring:** Only a few people in any organization have administrator controls or rights to carry out certain tasks or authorize certain requests. Because breaches of such accounts could cost an organization dearly, privileged users must be monitored. Checking if a user has been wrongly provided with privileged rights is crucial (such users should immediately be flagged, with their privilege rights removed or reduced). Tracking the access rights and permissions of privileged users is essential to protect critical assets.

- **Block Count Trends:** Organizations implement security solutions at different layers of the network. These solutions include firewalls, intrusion prevention systems, sandboxes, data loss prevention systems, web security applications, and email security tools. Security teams can ascertain the effectiveness of solutions on individual network layers by analyzing the number of detected and blocked threats. Such calculations can help security officers decide whether a security product needs to be replaced.

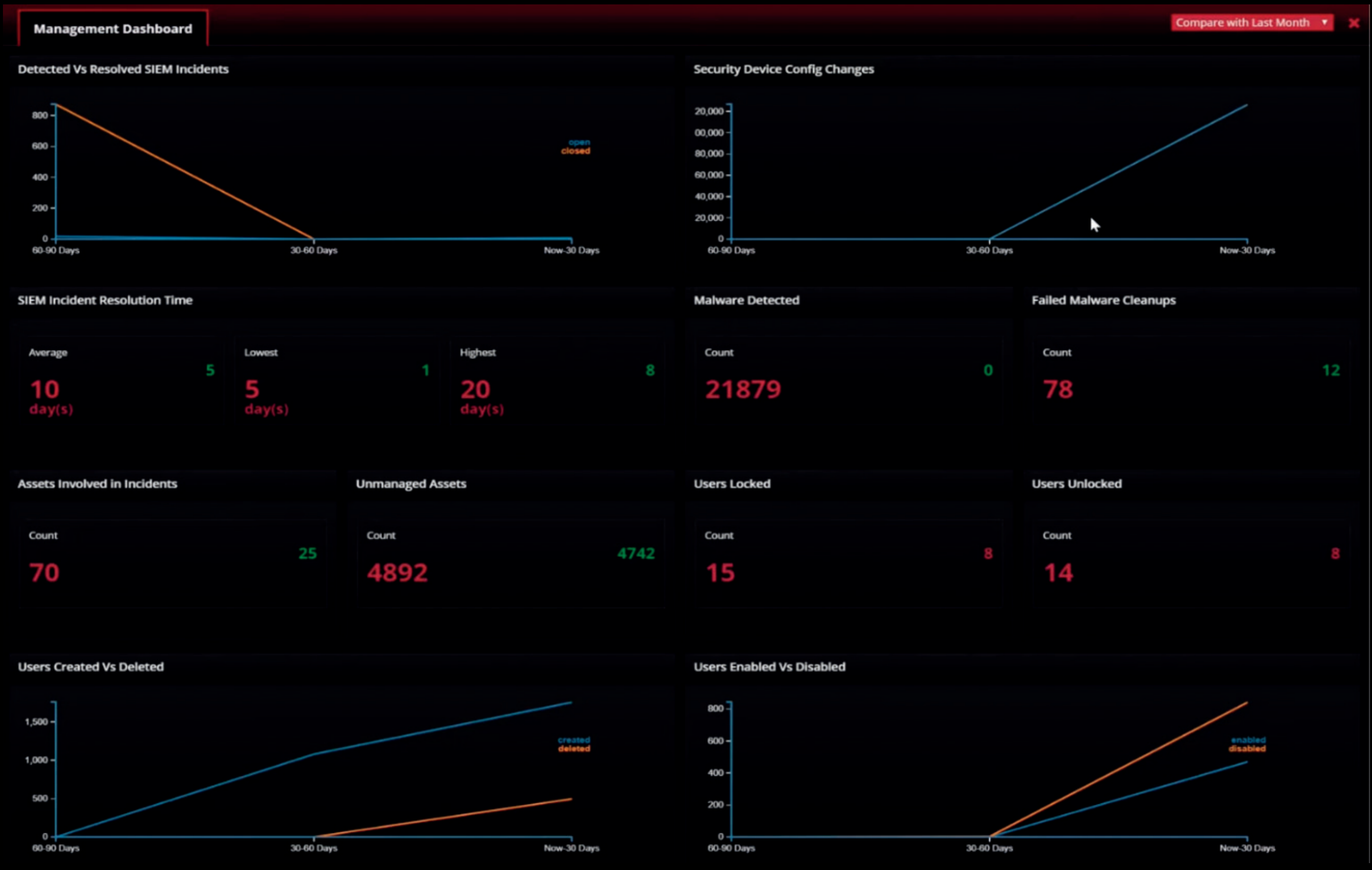
- **Real-Time Analysis and Reporting:** A hacker can penetrate a system and conceal a virus or other weapon that may lay dormant in a network for months or even years. The threat may later emerge to attack and damage internal assets when an organization least expects it. A capable threat detection tool can detect dormant threats by monitoring the network on a real-time basis.

ABOUT LINKSHADOW

LinkShadow is a cybersecurity product built by a team of experts and solution architects to enhance organizational defenses against sophisticated attacks, zero-day malware, and ransomware. It is a technology platform that provides a user-friendly dashboard and other critical functions to monitor an organization's live security posture. LinkShadow automatically detects critical issues in the network, enabling users to respond quickly to malicious activities. Unique features of LinkShadow include behavior analysis (using machine learning), automatic discovery of assets, and a CXO dashboard designed to present key indicators to senior management.

The CXO dashboard is completely configurable. It allows users to choose widgets to represent the organization's security threatscape and to access information needed to monitor and make decisions. This dashboard can present key security metrics (e.g., malware detected, users blocked, and intrusions halted) on a quarterly or monthly basis.

FIGURE 3: Management Dashboard Snapshot



SIEM Incident Resolution Time

Average 5
10 day(s)

Lowest 1
5 day(s)

Highest 8
20 day(s)

Malware Detected

Count 0
21879

Failed Malware Cleanups

Count 12
78

Assets Involved in Incidents

Count 25
70

Unmanaged Assets

Count 4742
4892

Users Locked

Count 8
15

Users Unlocked

Count 8
14

Source: LinkShadow

Enabling threat hunting with the use of machine learning is one of the core value propositions of LinkShadow. LinkShadow strengthens the security of organizations with advanced threat hunting capabilities supported by machine learning algorithms that detect, analyze, respond, resolve and mitigate incidents in much lesser time.

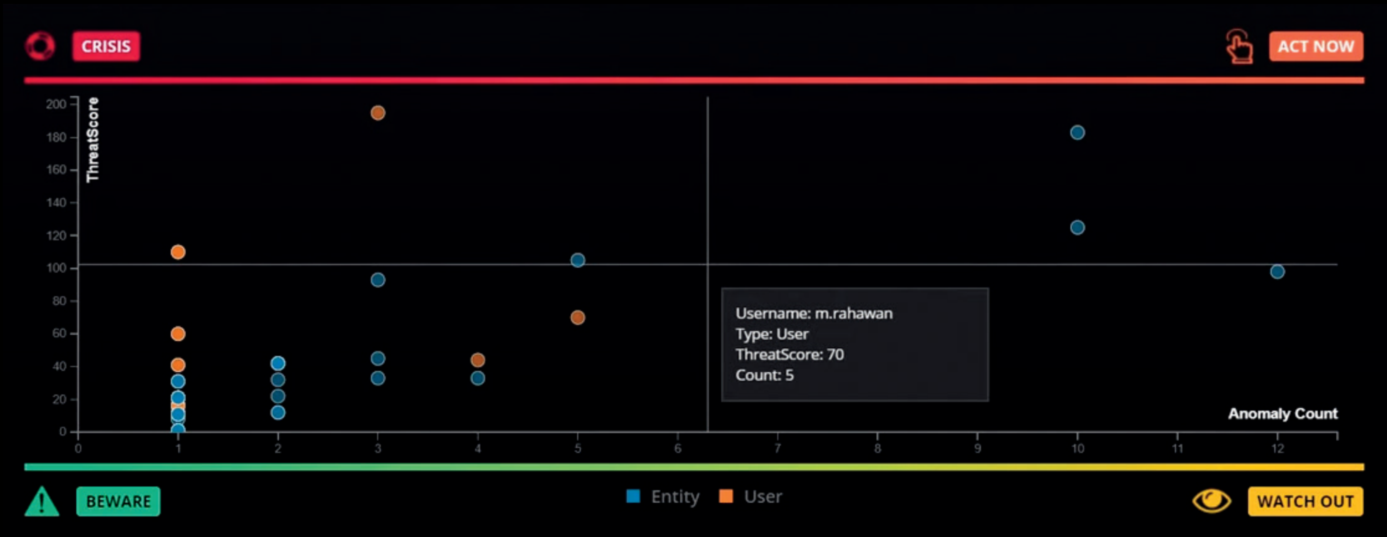
ABOUT LINKSHADOW

Some of the Machine Learning-enabled features of LinkShadow include:

ThreatShadow – This feature provides a compiled view of all the threats identified in the network using machine learning algorithms and present it on a dashboard for the security officer of an organization to focus on threats that really matter. This feature runs more deeper investigation into the system to track where a threat originated from and understand its pattern of operating to find where it is heading in case it is identified in real time. This feature uses threat scoring machine learning algorithm and collective profiling of entities and users in the network to identify the probability of an incident. ThreatShadow also compares the network situation of an organization at a given day with a situation of a previous date to verify if certain threats are persisting over a time in the system. This feature helps the security officer identify the most vulnerable assets and users as well as evaluate the efficiency of other security systems such as firewalls and end-point security in the network.

Identity Intelligence – This feature detects whether a user is behaving normally by comparing his/her current actions with historic authentication patterns, application usage habits, etc. This feature focuses on visual trend analytics on user behavior to pinpoint high risk users based on machine learning to constantly monitor high profile users by adding them to the "Watch list". This feature groups certain user profiles based on their functionality and authority. One of such user groups is "super users" who are entities in a network with higher authorities. Adding these super users to the watch list enables continuous monitoring of these accounts to ensure they are not compromised. Many other such critical users are grouped by top inactive users, users with failed logins, users connected to most assets, risky users, and many more which are continuously monitored. The profiling and monitoring of these users in different groups on real time basis is possible by use of machine learning.

ThreatScore Quadrant –There are several threats detected daily in a network, out of which few may be very critical or serious to address. With the help of machine learning ThreatScore plots entities and users based on the threat they behold to the network on a chart for the security officer to take action. This feature detects anomalies through behavioral analytics performed on user logs and network packets using machine learning algorithms to graphically position threats on a chart based on two values that is the "anomaly count" plotted on x-axis and the "threat score" plotted on y-axis respectively. Following snapshot of the threat score quadrant gives a clear representation of the same :



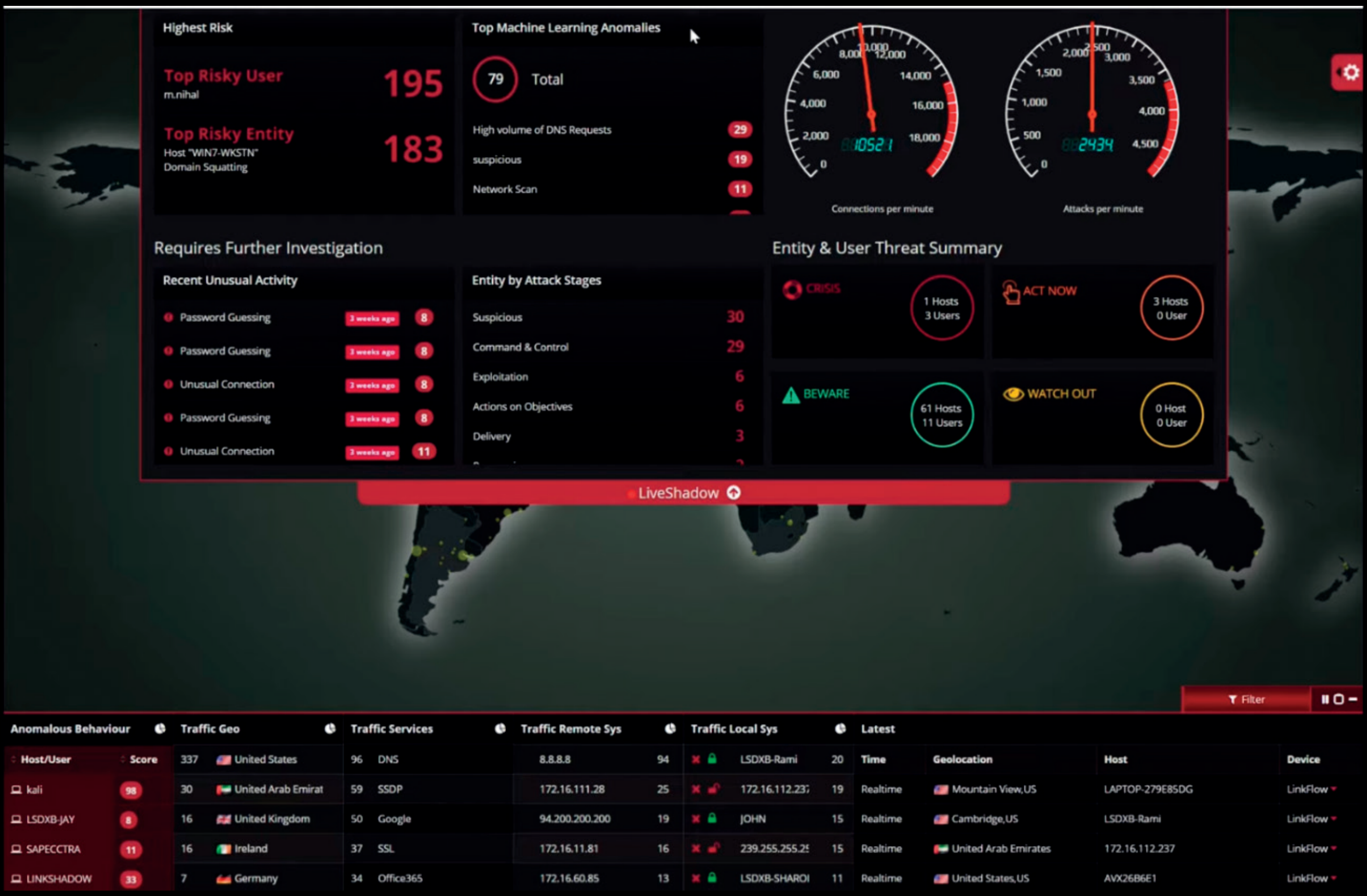
Username: m.rahawan
Type: User
ThreatScore: 70
Count: 5

Source: LinkShadow

ABOUT LINKSHADOW

The x-axis measures the anomaly count of an incident using machine learning algorithms, hence the more the behavior of an incident (of an entity or user) is abnormal the more it goes to the right section of the graph towards the 'Watch Out' quadrant. While the y-axis measures the threat score of the incident where threat feeds comes into play along with machine learning. For example if the IP of an entity is communicating with a blacklisted IP the threat score will increase and plot the entity up towards the 'Crisis' quadrant. However, when both the anomaly count and the threat score is high the incident lands in the 'Act Now' quadrant where the security analyst needs to take immediate action. The 'Beware' quadrant however is the section where most of the incidents are present which are not very critical but have to be monitored as they may move to other quadrants. This feature of LinkShadow is another key value proposition of its threat hunting tool which runs in real time and gives instant updates.

FIGURE 4: LiveShadow Feature Snapshot



Highest Risk

Top Risky User 195
m.nihal

Top Risky Entity 183
Host "WIN7-WKSTN"
Domain Squatting

Top Machine Learning Anomalies

79 Total

High volume of DNS Requests	29
suspicious	19
Network Scan	11

Requires Further Investigation

Recent Unusual Activity

Password Guessing	3 weeks ago	8
Password Guessing	3 weeks ago	8
Unusual Connection	3 weeks ago	8
Password Guessing	3 weeks ago	8
Unusual Connection	3 weeks ago	11

Entity by Attack Stages

Suspicious	30
Command & Control	29
Exploitation	6
Actions on Objectives	6
Delivery	3

Entity & User Threat Summary

CRISIS	1 Hosts 3 Users
ACT NOW	3 Hosts 0 User
BEWARE	61 Hosts 11 Users
WATCH OUT	0 Host 0 User

Anomalous Behaviour		Traffic Geo		Traffic Services		Traffic Remote Sys		Traffic Local Sys			Latest			
Host/User	Score	337	United States	96	DNS	8.8.8.8	94	✕ 🔒	LSDXB-Rami	20	Time	Geolocation	Host	Device
kali	98	30	United Arab Emirat	59	SSDP	172.16.111.28	25	✕ 🔓	172.16.112.23	19	Realtime	Mountain View,US	LAPTOP-279E85DG	LinkFlow
LSDXB-JAY	8	16	United Kingdom	50	Google	94.200.200.200	19	✕ 🔒	JOHN	15	Realtime	Cambridge,US	LSDXB-Rami	LinkFlow
SAPECCTRA	11	16	Ireland	37	SSL	172.16.11.81	16	✕ 🔓	239.255.255.2	15	Realtime	United Arab Emirates	172.16.112.237	LinkFlow
LINKSHADOW	33	7	Germany	34	Office365	172.16.60.85	13	✕ 🔒	LSDXB-SHARO	11	Realtime	United States,US	AVX26B6E1	LinkFlow

Source: LinkShadow

ABOUT LINKSHADOW

Additional features include:

- **Asset AutoDiscovery** allows users to classify nodes through the automated discovery of all IT infrastructure within the enterprise. This feature ensures that all assets are protected and updated for compliance audits.
- **Shadow 360** provides an in-depth view of all activities that occurred in a network before and after an anomaly.
- **User Investigator** provides a user behavior heat map to help prevent insider attacks, compromises to privileged accounts, and other insider threats to a network.
- **TrafficSense Visualizer i**dentifies, monitors, and blocks network communications based on source or destination IP addresses. It uses geo-intelligence technology to obtain insights on where traffic is coming from, enabling security officers to decide whether permissions should be granted.
- **Attackscape Viewer** provides a view of the latest global attacks so that users can take proper measures to avoid an incident affecting their organizations.

These features can be accessed and represented on the customizable LinkShadow dashboard. The dashboard has drag-and-drop features and enables the installation of widgets according to customer preferences and requirements.

LinkShadow offers three variants of its platform: the LS 1000, LS 3000, and LS 10000. These come with 1GB, 3GB, and 10GB of network throughput, respectively. They can be complemented by LS Insight software that provides insights into endpoints and end users, including activity monitoring, file and registry integrity monitoring, and automated response functionalities.

CONCLUSION

IT security is critical — and CIOs and CISos are making concerted efforts to improve and strengthen the security postures of their organizations. However, the expanding range of cyberthreats and the dizzying array of products offered by security vendors present persistent challenges. The scarcity of skilled security experts is another obstacle. Not all companies can afford a SOC or are ready to opt for a managed security provider. Organizations are seeking vendors that can provide efficient and affordable solutions.

DX initiatives that leverage IoT, mobility, cloud computing, and Big Data and analytics are exposing organizations to increased network vulnerabilities. In many organizations, it remains unclear who is responsible for managing the security of migrated data and applications stored on cloud platforms. Organizations should understand that IT security must be a shared responsibility between the vendor and the customer. Cloud vendors should take the necessary steps to ensure the overall security of data. Organizations have the duty to monitor data flows and identify any suspicious activity. Demand is rising for threat analytics products that are easy to integrate and are more affordable than a managed security service provider.

Threat hunting has become a critical part of the security architecture of organizations, and as more and more organizations realize the practical value of these threat hunting tools, the better it would be for their security teams to quickly uncover and handle advanced threats. While technology advances at incredible speed, threat hunting tools using machine learning technology are creating exceptional value in the market by providing solutions that strengthen organizational security. Machine Learning helps in building powerful tools to improve the cybersecurity posture and influences the development of many other security technologies from the data collected on malware, incidents, processes, and other indicators of breach.

Organizations need to take a balanced approach that enables them to implement a high level of security while staying within their budgets. Of course, even with effective systems in place, organizations may still encounter cyberattacks. LinkShadow addresses this situation with its efficient, cost-effective, and easily integrable threat detection capability. Built by a team of security experts that understand market pain points, LinkShadow uses machine learning capabilities to identify internal and external threats. It provides a single, holistic view of a network across different departments and functions, enabling IT administrators to monitor overall security status in real time. It also enables decision makers to receive performance-based quantitative analyses of their security investments. LinkShadow can be customized according to clients' specific business requirements.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world›s leading technology media, research, and events company.

IDC Middle East/Africa

Level 15, Thuraya Tower 1
Dubai Media City
P.O. Box 500615
Dubai, United Arab Emirates
971.4.3912741+
Twitter: @IDC
idc-community.com
www.idc.com

IDC ANALYZE THE FUTURE

Copyright Notice