Market Share

Worldwide Network Intelligence and Threat Analytics Market Shares, 2019: How the Network Is Used to Unmask the Adversary

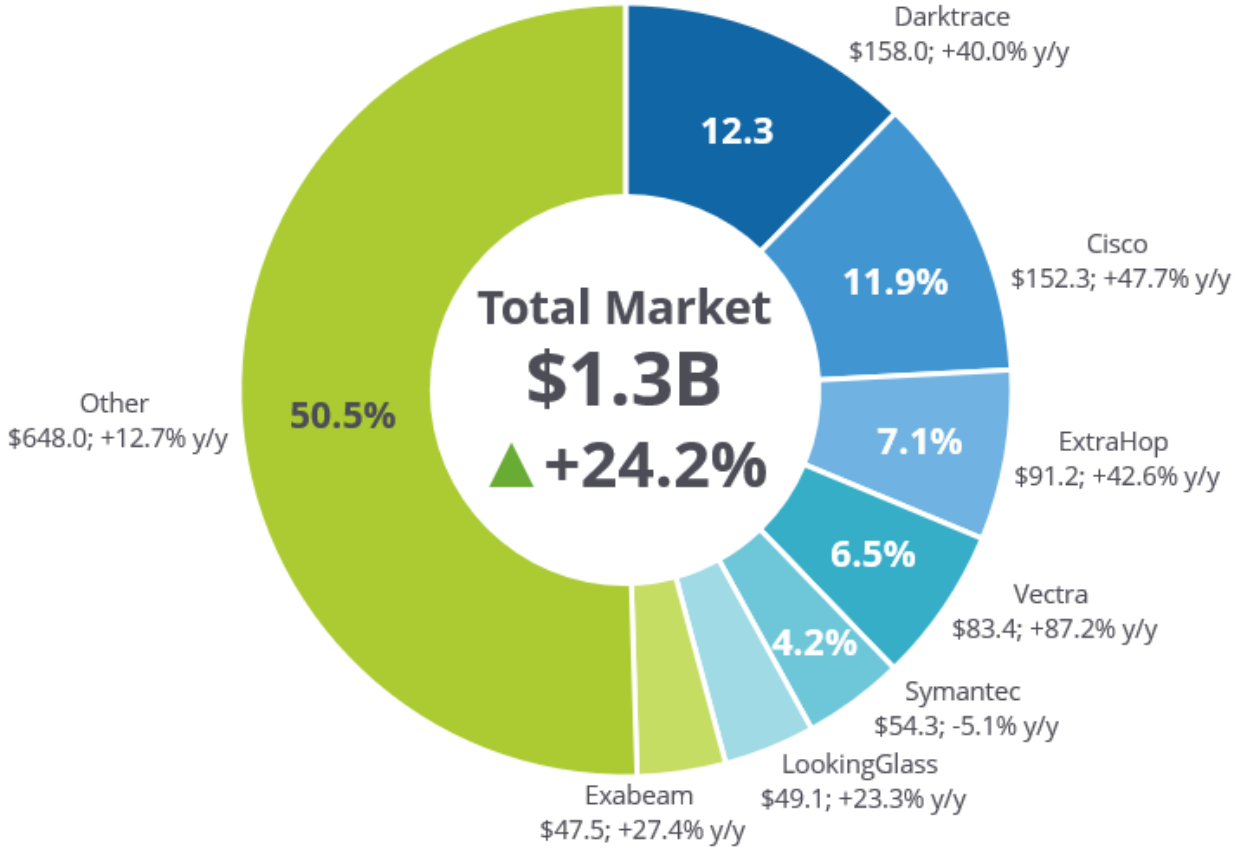
Christopher Kissel Frank Dickson

THIS IDC MARKET SHARE EXCERPT FEATURES IRONNET CYBERSECURITY

IDC MARKET SHARE FIGURE

FIGURE 1

Worldwide Network Intelligence and Threat Analytics 2019 Share Snapshot



Note: 2019 Share (%), Revenue ($M), and Growth (%)

Source: IDC, 2020

December 2020, IDC #US46351020e

IN THIS EXCERPT

The content for this excerpt was taken directly from Worldwide Network Intelligence and Threat Analytics Market Shares, 2019: How the Network Is Used to Unmask the Adversary (Doc # US46351020). All or parts of the following sections are included in this excerpt: Executive Summary, Market Share, Who Shaped the Year, Market Context, Appendix and Learn More.

EXECUTIVE SUMMARY

In 2019, global network intelligence and threat analytics (NITA) vendors sold just short of $1.3 billion in products and related services, and this was better than a 24% gain YoY. There are several reasons for the strong growth in revenue, among them:

- **Refining alerts and defining outcomes.** Generally speaking, cybersecurity point products such as security information and event management (SIEM), endpoint detection and response (EDR), next-generation firewalls (NGFWs), intrusion detection system (IDS) and intrusion prevention system (IPS), and data monitoring products are strong in silos. When properly deployed, NITA platforms can correlate different cloud, network, and security point product events into either a singular string of events or probabilistic outcomes based upon risk-based events, likelihood of an intruder, and exploitability of the worst exposures.
- **Working from a holistic view of the network.** Along the same lines of alerts coming from discrete cybersecurity platforms, NITA platforms assume an analytical view of the network (i.e., a bird's eye view). NITA platforms can monitor for configuration drift and look for indicators of compromise (IoCs) from sessions, telemetry coming from IT and cybersecurity tools, or artifacts coming from the metadata of the files themselves.
- **Maximizing heterogeneity.** NITA platforms can ingest sources from batch data, endpoints, and applications. In addition, many of these platforms can be extended to include several branch offices. Analysts do not have to be on premises to gain perspective from multiple networks.
- **Incorporating user behavioral analytics (UBA).** To be clear, establishing statistical baselines and UBA for individual users is almost table stakes for platforms in EDR, SIEM, NITA, and even for identity and access management (IAM). However, UBA might find anomalies not obvious from other means of detection. In NITA, statistical baselines not only involve specific user but activities are also reconciled with peer groups, machine types, and unusual access activity. What is an underappreciated aspect of statistical baselines is that to establish a baseline, a company must have a solid understanding of its ideal state of its network and configuration — which can serve as a redundancy for disaster recovery (DR) or as a reference guide to add new machines/users.
- **Achieving performance consistent with investments.** YoY growth is easier to achieve when companies in a newer technology group start to reach a certain level of maturity. Some of the biggest companies such as Darktrace, **ExtraHop,** and Vectra attained velocity as they reached revenue of roughly $50 million and then received additional funding. The growth rates in this industry will fall if only because it is tougher to gain YoY growth as companies in fact realize revenue in proportion from a smaller total available market (TAM) market opportunity.

NITA roughly tracks to a more common industry acronym: network detection and response (NDR). Other syndicated research firms use NDR for the analytics sets that monitor Layers 3–7 of the OSI

layer for indicators of compromise. This technology stack maps with "network intelligence" in our nomenclature. However, IDC identified three other major technology headings where the "network" is used to find IoCs: network performance monitoring (NPM) and full packet capture (PCAP), emulation and deep packet insights, and deception (these technologies are explained throughout the document and specifically in the Market Definition section).

This IDC study provides the market shares by 2019 revenue for vendors in the NITA market. (Note: The topline number and forecast is kept continuously within the Security and Trust group. In addition, the Market Share and Market Forecast documents will be refreshed in 1Q21 to include the calendar year 2020 in the Cybersecurity Rollup 2021). IDC did not ask participating vendors for market revenue estimates for 2020, but many volunteered that their revenue was not only ahead of revised guidance but pacing with pre-COVID-19 guidance, many actually have revenue-breaking quarters.

"What seems like a natural extension of the network is that the mobility of data, the actions of users, and performance-related criteria could be turned on its head to be used to find indicators of compromise (IoCs), and chart the path of the adversary," says Chris Kissel, research director, Security and Trust Products at IDC. "What has been somewhat surprising is that by way of extending the network to include work-from-home employees, network intelligence and threat analytics (NITA) vendors have been a large part of the cybersecurity stack in 2020."

ADVICE FOR TECHNOLOGY SUPPLIERS

Regardless of the technology, cybersecurity vendors of every stripe have a few select common missions: protect an enterprise's assets and detect anomalies, and accomplish these tasks compliantly while reporting compliance adherence. Here is how NITA tool providers help articulate this vision to existing and potential customers:

- **Explain what their tools do explicitly.** At the time this document was written, it is the Thursday before the U.S. presidential election and the United States has had a surge in COVID-19 cases. The FBI has issued a formal warning to hospitals and healthcare providers that there is "an increased and imminent cybercrime threat." Specifically, FireEye identified a threat actor it calls UNC1878, which is deploying Ryuk ransomware. In short, if your NITA can identify Ryuk on the network (or whatever malware flavor of the day at the time of proof of concept [POC]), say so.
- **Map to the MITRE ATT&CK framework.** The most current MITRE ATT&CK Matrix describes 14 different techniques used by the adversary to infiltrate and exploit an enterprise network. (Recently, Reconnaissance and Resource Development have been added left of and before Initial Access.) In the past two years, using MITRE ATT&CK as a reference architecture for tool development has gained critical momentum among cybersecurity tool providers for important reasons. The ATT&CK framework approximates the adversarial life cycle – that is to say that if a tool finds evidence of Defense Evasion, you should next try to find whether the attributed malware is attempting Credential Access. A security operations center (SOC) team can then initiate the proper response based upon the greatest achieved MITRE ATT&CK stage. Adjacent to this, SOC analysts are increasingly trained to think of detection and response functionally, and threat intelligence feed providers often contribute findings to the ATT&CK Matrix. It is a *major* advantage to a software provider if it can show on its dashboard where a SOC analyst can mouse-click on a screen and the information maps to the ATT&CK Matrix and to the catalog of sub-techniques.
- **Demonstrate old-school sales tactics at the POC.** An iconic image in the mythology of the American business ethos is the superstar salesman full of brim and bravado making a splashy

but efficacious sales pitch. What a NITA tool provider often can do is tell a prospective client, using batch data or sensors, what potential exposures there are on the client's network based on port activity, observed malware colliding with a network perimeter, and bad or questionable domain access. A NITA vendor would be wise to demonstrate a priori knowledge of the cybersecurity posture of the network it hopes to protect.

- **Public cloud visibility is a must, and specific application detection services is strongly suggested.** One of the appeals to NITA tools is that these can derive insights from batch data and clod flows and logs. Differing levels of expertise occur in cloud and application visibility, but even in the most basic capacity, user behavior analytics can be applied to behaviors from ingress/egress logs. However, NITA achieves real value when it can detect anomalies in real time from traffic mirroring or virtual test access port (TAP) or tokens placed in cloud environments. The majority of NITA vendors provide a ubiquitous and continuous defense in the majority of hybrid architectures. Having a specific module for Microsoft Office 365 or Salesforce is a killer differentiator.
- **Network coverage must be both wide and deep.** COVID-19 created radical changes in the cyberdefense of networks. Enterprises had to adapt to a work-from-home (WFH) workforce. From a visibility standpoint, SOC analysts wanted device visibility dynamically tied to local directory access protocol (LDAP), a centralized management console to oversee new virtual private networks (VPNs), and further integration with data security products. While NITA platforms often differentiate because they can monitor IoT devices and mobile devices, these use cases will be far more common in the near future.
- **Recognize NITA vendors are one tool of many in a SOC.** A successful SOC is the combination of "people, processes, and technology." A vendor's NITA tool has to be ergonomically correct for analysts to use. The expression of detection anomaly must plug-and-play into the response cycle and a company's IT/security ticketing process, and the technology must integrate with other tools.
- **Soft values are more important than ever.** In 1H20 studies, IDC emphasized COVID-19 kindness. This pandemic created economic austerity, anxiety, and technology gaps. New cybersecurity contracts often involved on-premises training. Many of the ways that vendors could add profitability within an account was to stairstep services (greater access to help desks, code development support, etc.). The vendor has to be flexible in offering shorter-term contracts, extended support and, possibly, complementary seat licenses or additional workloads. But adversity forges character and relationships created now are likely to have a greater impact than relationships made in less stressing times.

How the Study Is Designed

IDC was able to qualify 33 vendors for this study, meaning we felt like we were able to map their technology segments into our taxonomy and could produce an estimate of revenue (Note: IDC will *not* comment on the *source* of revenue estimates). For a quick reference, Table 1 explains where the various vendor products and platforms lined up within our NITA taxonomy.

The reason for "NITA" is that IDC wanted to include all the ways in which the network itself is used for detection. In our taxonomy, as mentioned previously, there are four discrete technologies that become the totality of NITA: network intelligence, full packet capture and network performance monitoring, emulation and deep packet insights, and deception (these technologies are explained in the Market Definition section).

At different points in this study, the term *NITA* will be used most often to encompass the overarching set of tools. This larger hierarchy is reasonable in most cases because network, data security, security

information and event management (log management), applications, identity, cloud security and perimeter defenses (intrusion prevention and detection systems, endpoint protection [EPP], and endpoint detection and response) represent different control/access planes. The concept of NITA should be assumed; however, IDC will be careful to present discrete technologies when the analysis requires this.

TABLE 1

Companies and Platforms Mapped in IDC's NITA Study

Network Intelligence	PCAP/NPM	Emulation and Deep Packet Insights	Deception
Arbor Networks	Cisco (Stealthwatch)	Core Security	Acalvio (ShadowPlex)
Awake Security (now Arista)	NIKSUN	Lastline	Attivo Networks
Bay Dynamics (now Broadcom)	Riverbed Technology	LookingGlass	Fidelis
Bricata	Symantec Security Analytics (Broadcom)	ReversingLabs	Illusive Networks
Corelight	VIAVI Solutions	Spirent	TrapX
Darktrace			
Exabeam			
ExtraHop			
FireMon (Lumeta)			
Gigamon (ThreatINSIGHT 3.0)			
Gurucul			
IronNet Cybersecurity			
MixMode			
Plixer			
Skybox Security			
Stellar Cyber			
Vectra			
Verizon (was ProtectWise)			

Source: IDC, November 2020

MARKET SHARE

IDC presents the revenue for 33 companies that have specific products in network intelligence and threat analytics. We wish to add the following provisos:

- There are often elements of NDR in different security point platforms, but NDR is found most commonly and increasingly in SIEM. For instance, there is an NDR module in the LogRhythm SIEM. Security analytics with an optional NDR are add-on features of the NetWitness SIEM, and IBM QRadar offers a Network Insights module. In this study, we focus on discrete companies that have unique SKUs for NITA.
- Using much the same logic, network insights may be a part of a larger framework. For this reason, the Fortinet Security Fabric is not included in this study. It should be noted that the Fortinet Security Fabric can be mapped to eight separate but related elements:
  - Open Fabric ecosystem
  - Cloud infrastructure
  - Applications
  - Security operations
  - Endpoint
  - Secure WLAN/LAN
  - Network access
  - Fabric management center
- This document does not consider platforms that are identified as cross-platform detection and response (XDR) (see the Competitive Landscape section for how IDC views XDR and how it competes and sometimes complements NITA). NITA products ostensibly compete with XDR but are also sometimes the analytics engine of an XDR architecture. XDR is still evolving, and there are several architectural options for businesses to use and vendors to integrate with to build a threat detection and response posture. One of the most common XDR use cases would be network intelligence as analytics overlay layer complementing SIEM and sending enriched data back through the SIEM engine that is connected to security operations and response (SOAR) to initiate ticketing, case management, and a response.
- The public cloud providers have different detection services, but at this time, these platforms are only using telemetry and connected to SPAN or TAP port, These platforms create valid insights but are not considered to be NITA appliances currently.

This IDC Market Share Report reviewed 33 different companies, and the order is based on size of business by revenue. Revenue estimates are presented for calendar years 2019 and 2018. For this excerpt, a brief profile of one vendor is featured below, and additional analysis as warranted is added.

IronNet Cybersecurity has an interesting approach to crowdsourcing for protecting alike companies in vertical markets and is profiled in the Who Shaped the Year section.

TABLE 5

Worldwide NITA Revenue by Vendor, 2018 and 2019: Ranked 16 to 20 ($M)

Rank	Company Name	2018	2019	2018–2019 Growth (%)	Brief Profile
17	IronNet Cybersecurity	19.6	24.0	22.6	IronNet Cybersecurity is a network intelligence threat detection company. Its architecture includes hardware or virtual sensors that sit on SPAN/TAP ports, public cloud sensors, and log forwarding that send data to the IronDefense back end. A big differentiator is the IronDome Collective Defense system that allows enterprises across an industry, a supply chain, and so forth to share collective intelligence (machine based and human intelligence) in real time.

Source: IDC, November 2020

WHO SHAPED THE YEAR

For this document, the emphasis on vendors who shaped the year went toward vendors that provided unique use cases. IronNet Cybersecurity is mentioned because its IronDome architecture helps extend the cybersecurity postures of alike businesses (i.e., financial services industries can share anonymized data and tactics to fortify defenses with other financial industry client appliances).

While we are citing these vendors in particular, do understand that NITA vendors of different stripes had strong developmental years, performed well in 2019, and continued many of the gains into 2020.

IronNet Cybersecurity

IronNet Cybersecurity offers its IronDefense network behavior and response solution to collect data from network metadata, network logs, and other sources of information. We describe the data collection and threat intelligence, but it is IronNet's IronDome solution that is a differentiator.

The IronDome collective defense system is an add-on subscription that allows enterprises across an industry, a supply chain, a region, or any other custom grouping of participants to share collective intelligence (machine based and human intelligence) in real time. The advantage is that the collection within the industry enables clients to collaborate on detection and response against cyberthreats germane to both industry-specific and cross-sector threats. For critical infrastructure in the United States, there is an optional capability to anonymously share real-time threat insights with the U.S. government to provide visibility and to allow them to take action (if they choose) using all elements of national power (cyber, political, economic, diplomatic) available. This capability is a noticeable differentiator in light of the rise of nation-state level cyberthreats against critical infrastructure, including threats to the grid. In addition to enterprises, the IronDome approach would be attractive to professional service providers, managed security providers (MSPs), and managed security service providers (MSSPs) as they try to craft differentiating services.

IronDefense is the analytics engine of the IronNet cybersecurity platform. The following are the most important elements of its analytics:

- **IronDefense deploys behavioral analytics.** Like many companies in NITA, IronNet develops statistical baselines. By contrast, IronNet also includes supervised and semi-supervised ML across network metadata and probabilistic algorithms including Xgboost, random forests, and Ladder Networks to solve the problem of identifying malicious network traffic. Unsupervised learning modules can look for techniques indicative of lateral movement and beaconing (as examples) and address data loss prevention use cases.
- **IronDefense with IronDome drives collective intelligence at the community level.** For customers with an IronDome subscription, IronDefense automatically shares anonymized detection metadata within their IronDome community for higher order threat analysis. In return, individual enterprises receive collective intelligence on correlated threats in their environment, including risk prioritization details, suggested practices on how other SOC teams in their communities have triaged similar threats, and other insights that improve the speed and efficiency of response.
- **IronDefense includes an expert system.** This integrated expert system automatically orchestrates the acquisition and applications of investigative playbooks for each behavioral analytic to further prioritize detected anomalies by risk to the organization. In this module, IronDefense can leverage external sources such as Whois, DomainTools, and Majestic Million, and other types of similar information. It also can leverage internal contextual sources such as CMDBs and behavioral baselines such as community of interest (COI) to prioritize by risk.
- **IronDefense offers a hunt module.** IronDefense allows customers to perform cyber hunts and fast search across all network flows collected by the platform. Customers have full PCAP access on flows collected by its sensors and can carve files from PCAP, the attributes of which can be matched with VirusTotal for further insights. Customers with IronDome have access to a Detection Correlation Dashboard (DCD) that visualizes how anomalies detected in their environment correlate to threats seen in the community and insights to how peer SOC teams rated and triaged the threat.
- **IronDefense does include several network performance monitoring techniques.** Designed specifically for security iterations, IronDefense can monitor the network for periodicity and evasive jitter for C2 beaconing, and to look for standard anomalous port, protocol, and rate-based anomalies; TLS handshake anomalies; and other behavioral outliers.

IronDefense offers multiple form factors for a customer's deployment. The IronDefense analytic engine is deployed in the cloud, but an on-premises option is available for customers that are unable to leverage external cloud infrastructure (or prefer not to). IronDefense sensors are deployed in the public cloud or on premises via SPAN or TAP ports as either a hardware or virtual appliance to collect network metadata and full PCAP for analysis. IronDefense can also ingest log data from cloud environments such as AWS or Microsoft Azure; infrastructure logs such as DNS, Proxy logs, and NetFlow; and other sources of telemetry data for analysis.

IronNet has a staggered approach to pricing for businesses of various sizes. For the midsize market (roughly 2,500–9,999 employees) and enterprises, the pricing is either per-employee or aggregate analytical throughput (not nominal network ingest speeds). In 2020, IronNet introduced an entry-level network log-centric solution for smaller companies. IronNet has had good success with U.S. infrastructure companies, financial service companies, and government clients, and the company is gathering momentum with clients in Asia/Pacific, Europe, and the Middle East.

MARKET CONTEXT

A singular aspect in all types of digital technologies in the 21st century is the idea of cooperation and competition from vendors in the same technology is a fluid condition. In cybersecurity, the reality is that no one vendor will win and emerge as a dominant security player. Therefore, security vendors have to embrace OpenAPI, common frameworks, and even the inclusion of open source platforms when asking enterprises for contracts. (That said, the tool sprawl in business environments is becoming concerning. In the most recent IDC FutureScape on cybersecurity, IDC predicted that by 2023, to reduce security complexity faced by limited staff, 55% of enterprise security investments will be on unified ecosystem and platform frameworks.)

At the end of the day, NITA vendors often compete for static security dollars. Furthermore, the competition occurs along the lines of excellence. If a SIEM becomes nimbler or develops better network intelligence or NDR, then it becomes a direct competitor to NITA. As discussed previously, some deception vendors are including an endpoint agent to cover both EDR-like detection and detection through deception. Perhaps device vulnerability management vendors such as Qualys or Tenable refine their detection platforms, giving them multiple use cases using agents and clouds. The successes in 2019 can be fleeting.

Significant Market Developments

In creating the content for this document, we included several key NITA technology developments in describing the offerings of vendors. If these served to be precise observations, these are the larger moving blocks of NITA cybersecurity.

Competitive Landscape

In this document, we have cited that the four sub-technology groups network intelligence, full packet capture and network performance monitoring, emulation and deep packet insights, and deception each has important vantage points and value in specific use cases.

In cybersecurity, there is a simultaneous accordion-like effect between platforms and services. EDR tools can be integrated in with network intelligence tools, and this would ostensibly be a win for both tool providers (network intelligence providing a holistic view of the network and EDR finding corruption and alterations on the endpoint). By the same token, a business may have limited cybersecurity resources and decide that an EDR provider wins static dollars against a network intelligence platform. SIEM vendors often use similar metadata collection that network intelligence and PCAP/NPM vendors do and may perceive that the SIEM is agile enough in handling metadata for incident detection and response, case management, workflow, and IT ticketing.

The next set of competitors is managed security providers (which address midmarket mostly), managed security service providers (which are for enterprises largely), managed detection and response (likely the most significant competitor to NITA), and professional services (although this might be for specialized industry verticals and would be an expensive option). MSSPs win when a company simply decides to hand over the keys and allows the MSSP to install the tools, design ingress/egress, manage firewalls, and contract/hire the security personnel. MSPs would be smaller regional players that may offer a security service or a centralized security platform. Of note, a company such as Verizon may offer a turnkey MSSP solution or offer various services including an NDR service. A second note too is that many of these NITA providers furnish tools that enhance the back end of MSSP and MSP platforms, which is the spirit of "coopetition" personified.

MDR is an interesting case that directly affects security point product providers but is a giant nuisance for NITA. MDR has two central strengths. The first strength is that the MDR offers a formal service-level agreement (SLA) to send an alert back the client's IT/SOC infrastructure within a specific time frame. The time frames given are from 15 minutes to one day, with an industry average of three hours. The second strength is that MDR services are often bought à la carte. A company could add firewall/EDR/anomaly detection and even remediation suggestions and or actions, depending on its appetite for security spending from the client.

However, there are two major considerations that work against MDR. The most important problem is the "shared responsibility" model. Self-evidently, a business is responsible for the physical security of its equipment and the host infrastructure, but after that shared responsibility gets cloudy. Network controls, application-level controls, IAM, endpoint protection, and data classification all need well-defined stakeholders. The client should assume full responsibility when responsibilities are not spelled out; but if there is a gap between the coverage of MDR and what the client expects, often it will be because the controls are not well defined. A problematic correlation exists as well — the more in-depth services that a client wants from a managed provider or MDR, the more control of the network that client cedes. Second, perhaps the most underrated part of a company owning its security posture is that it can customize its defense as it goes. Specific rules and roles are created based on inefficient workflows and gambits tried and failed but also on successful playbook implementation and user or industry-specific protections — these being difficult to create from the outside looking in.

We mentioned XDR briefly in the Market Share section. The architectures and the expectations of XDR are still being played out. IDC does see several XDR products and integrations emerging. Furthermore:

- The most common use case is EDR in conjunction with other sources of telemetry such as firewall logs, threat intelligence, and many intrusion detection and prevention systems. Palo Alto Cortex XDR is an example of the type of threat detection found in XDR (and perhaps the first vendor to formally use the term *XDR*).
- EDR plus SIEM plus automation and orchestration (SOAR, if you prefer) is a common architecture. This is appealing on several levels. First, whatever else is thought about SIEM, keeping and managing logs is necessary both for proving compliance and as a reservoir for search, especially when new malware signatures are found. SIEM platforms either natively have SOAR and case management functions or are widely integrated through APIs to initiate response.
- EDR is over IaaS. A recent agreement between Tanium and Google Cloud Platform gave sales managers for both companies the ability to sell across platforms. Also interesting is the platforms are tightly integrated for threat detection, metadata collection, and literally Google search for evidence of adversarial behaviors.
- Several vendors are advertising XDR as the assimilation of batch data, with logs, endpoint, and device flow data as an XDR architecture.
- NITA platforms act as an additional telemetry overlay to all said form factors.
- At the moment, it is up in the air whether external threat intelligence is value added to XDR or merely a feature.

Currently, IDC has decided against creating a formal total available market for XDR. The problem is that it can be argued that a perfect XDR platform is competitive in IaaS, SIEM, EDR, NITA, MDR, and even, threat intelligence deployments/contracts. We aren't trying to be cagey; a common XDR

architecture has not emerged and sublimated its competitors yet. As UBA became a "feature" and not a platform, certain aspects of XDR will be simply subsumed in the greater platform plays.

However, before we leave the topic altogether, there should be a word of caution for vendors offering "XDR" platforms. Understand that the customer *does not care* what you call yourself or what you advertise. If the customer decides that they want to use a certain EDR product, want to use its own SIEM, and would like these tools to function as an XDR platform, that same customer does not want three different pricing modules and three different dashboards. The customer expects a vendor to write or help with support API if the customer's architecture wants to include specific IT, security point products, identity, or CMDB to serve as a unified detection and response center. Ultimately, businesses purchasing cybersecurity products want to optimize their own people, processes, and technologies, and in so doing, they want a faster mean time to detect and mean time to respond to an adversarial conflict.

The Return of Deception

The concept of deception has always seemed inherently attractive in the context of network security. This is not meant to be a superfluous statement — once the adversary breaches the security perimeter, there is almost no proactive security action the network protector can make. As the attacker is learning about the configuration and business segmentations of the network, if the adversary stays quiet and does not trigger any rule- or role-based violations, the adversary could have free reign in the network There is no countermeasure that entices or changes the adversarial behavior short of deceptive registries, routing tables, directories, and yes, even files. (Note that the deception vendors scowl when analysts use the terms *lures, traps,* and *honeypots,* although we will need the antiquated technology shortly.)

If deception was this comely, then why has it failed to launch? (In this document, the largest deception vendor is Attivo Networks at $27.6 million in 2019; Fidelis Networks is larger, but parts of its revenue are realized in endpoint security.) Historically, there have been practical problems with deception:

- **It was (and is) hard to accurately profile an entire network.** A business network is an unstable and erratic environment. Devices drop on and off the network. Network conditions change due to OS and software upgrades. As many as 15–30% of devices on a network are unmanaged at any given moment. Deception requires static network paradigms for installation.
- **Malware became more adept at self-arming.** The reason why the older nomenclature of traps and lures draws elicit reaction from deception vendors is malware is becoming more sophisticated and more self-aware. Deception has to look real even up to the command line interface, or many strains of malware will divert.
- **The type of alerts coming to a tier 1 SOC analyst were difficult to decipher.** In the past, this may have been a problem in syntax, but running down an alert in a "made-up" environment may be no easier than running down an alert in the genuine network environment.
- **Pricing is or was ostensibly expensive.** Historically, deception was not designed for midsize enterprises. That said, like other technologies, cloud deployments, agents, and executables have reduced the pricing of deception.

However, it can be argued that the MITRE ATT&CK framework has helped deception vendors as much as any cybersecurity technology. The MITRE ATT&CK framework now has 14 major categories and over 300 sub-techniques listed. The Framework starts at Reconnaissance and Resource Development and ends at Exfiltration and Impact. What the MITRE ATT&CK framework does is roughly trace the (successful) stages that an attacker must go through to initiate a successful campaign against a network. However, if deception leaves a specific bait such as a knockoff registry, a phony password in

a password vault, a bogus exfiltration port on a routing table, the SOC team has a high-fidelity alert that it can take action on.

The field of deception was again helped on August 24, 2020, when MITRE introduced MITRE Shield. Shield is suggested active defense – the natural extension to ATT&CK. Shield is nascent, and it has eight active defense categories: Channel, Collect, Contain, Detect, Disrupt, Facilitate, Legitimize, and Test. There are 130 countermeasures suggested by Shield in active defense; 44 of these measures involved decoys, and other ideas such as pocket litter (false data), email manipulation, and admin access can be mimicked and monitored within a deception platform.

User Behavioral Analytics, a Feature not a Platform

The concepts of statistical baselines and UBA are nearly ubiquitous in cybersecurity that the conversation is nearly three of four years out of place. A couple of things are worth noting and are suggestive of where NITA vendors are going.

In the nascent days of UBA, circa 2012-2014, the biggest use case for UBA was that the analytics layer would find the adversary when perimeter defenses could not. This analytics as a feature and not a platform adds value. However, solutions offered by the first companies in UBA including Darktrace, Vectra, and Exabeam were almost solely mathematical functioning algorithms. The problem is that when these platforms were installed at a proof of concept, they would not find any anomalies because the algorithms had not been trained. A second possible problem is that in the first stages of training, the platform's suspicious behavior might be picked up as a possible anomaly the first time, not acted on the second time, and then recognized as "accepted behavior" from there on out. In time, the UBA vendors would add yet more algorithms to account for drift, the sum of squares, similarity, and divergence, but we can ask this: if the solution to simple algorithms was to add more algorithms, why can't the adversary add an algorithmic layer on top of the algorithms that normalize algorithms? More precisely, in the future, the adversary may be able to anticipate algorithm activity and create obfuscation against, and/or add so much flotsam to a system that it renders the alerting hierarchies as all but useless.

In the past few years, several UBA vendors were purchased to enhance varying cybersecurity platforms. RSA developed a relationship for back-end analytics with Fortscale and then bought the company to integrate on NetWitness platforms. Aruba purchased Niara to help with network performance monitoring and user behavior analytics for its network access control platform. Interset was acquired by Micro Focus and the fundamentals of that platform influence the ArcSight SIEM, Micro Focus Fortify, Micro Focus Unified Endpoint, and Micro Focus' cyber-resilience strategies. The precepts of UBA complement network performance monitoring platforms offered by companies such as VIAVI Solutions to move these platforms from a networking performance monitoring paradigm to provide security use cases.

What IDC did not anticipate is that UBA would be an important normalizing factor in cybersecurity in 2020. The isolation forced by COVID-19 was both physical and functional. Simple human factors such as "whiteboarding" an incident in a SOC or the daily meeting were altered. The number of end users accessing applications and new firewall telemetry and micro-VPNs required visibility. Some sort of out-of-the-box capabilities helped cover technical debt accrued through the new networking realities. The adaptability of NITA platforms that could find insights from batch data, applications, and devices and correlating threat intelligence resonates with enterprises.

METHODOLOGY

IDC has continuously tracked the NITA market over several years, including markets such as user behavioral analytics and PCAP tools. However, our first revenue estimate appeared in *Worldwide Cybersecurity Analytics, Intelligence, Response, and Orchestration Market Shares, 2018: Turning Alerts into Outcomes* (IDC #US44779319, December 2019), and this is our first dedicated study.

IDC asked for briefings, questionnaires, and product demonstration beginning in June 2020 and has been receiving vendor contributions throughout the process.

The IDC software market sizing and forecasts are presented in terms of commercial software revenue. IDC uses the term *commercial software* to distinguish commercially available software from custom software. Commercial software is programs or codesets of any type commercially available through sale, lease, rental, or as a service. Commercial software revenue typically includes fees for initial and continued right-to-use commercial software licenses. These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately. Upgrades may be included in the continuing right of use or may be priced separately. Commercial software must be available for competitive bidding. These use cases are counted by IDC as commercial software revenue.

Commercial software revenue *excludes* service revenue derived from training, consulting, and systems integration that is separate (or unbundled) from the right-to-use license but does include the implicit value of software included in a service that offers software functionality by a different pricing scheme. It is the total commercial software revenue that is further allocated to markets, geographic areas, and sometimes operating environments. For further details, see *IDC's Worldwide Software Taxonomy, 2020* (IDC #US45718419, January 2020).

IDC is tracking a primary market. This means that the revenue generated for one SKU can only be realized once (the revenue cannot be double counted in network intelligence and threat analytics and SIEM, for instance). The second note is that there are revenues from physical appliances that are not represented in the software tracker that are captured in these market revenue estimates.

As part of the cadence with this document, IDC sent revenue estimates to companies in this study for review and a chance to comment. Under no circumstance will IDC disclose the degree of transparency a vendor provided for a specific revenue estimate. Many companies may offer a precise revenue estimate or guide an analyst to 10-K/10-Q or related statements. Other companies are privately held or do not comment; others still provide ballpark estimates. In addition, the security team works with the larger tracker group and we reconcile revenue to add to a larger whole. Other tools at the disposal of the analyst are contracts won, press releases, and number of employees. Otherwise, it is unfair and unethical to compromise the confidentiality of the participating vendors.

The data presented in this study is IDC estimates only.

Note: All numbers in this document may not be exact due to rounding.

MARKET DEFINITION

Network intelligence and threat analytics (NITA) is a technology sector within the cybersecurity AIRO product group within the IDC Security and Trust set of services. The acronym AIRO (analytics,

intelligence, response, and orchestration) establishes the foundation for the types of technologies and platforms that are mapped within the service. In October 2018, IDC published an updated taxonomy of its cybersecurity and IT security products/services (of note, the group is now called Security and Trust). Currently, we are aligning discrete technologies to the taxonomy. The project is incomplete but evolving, and our clients should understand that the taxonomy is fluid as cybersecurity evolves.

Currently, cybersecurity AIRO has three constituent elements: analytics and intelligence, response, and orchestration. We now provide a description of the elements and the technologies that IDC presents in this document.

NITA roughly maps to the common industry acronym network detection and response (NDR). The reason for the expanded definition is IDC wanted to include all the ways that the network itself is used for detection. In our taxonomy, there are four discrete technologies that become the totality of NITA:

- **Network intelligence.** Network intelligence extracts metadata from packets and applies insights about the packet based on user behaviors (UBA) and network events and often cross-correlate with threat intelligence or attack simulation to find possible adversaries. These are often Layer 3 tools but can also be Layers 4–7. Network intelligence platforms can also combine external threat intelligence, known bad domains, malware families, and advanced persistent threat actors to metadata occurring (or occurred) on the network. The analytics in network intelligence aspirational reduce the number of threats and/or string alerts to create one version of truth. Last, because network intelligence enriches data, these platforms (in theory) facilitate search better than SIEM or IaaS.
- **Deception.** Deception has a legacy technology perception of setting decoys, lures, and honeypots, but these vendors also now focus on distributed or endpoint deception, where deceptions trip attackers attempting to move off the attack beachhead — credential harvesting, lateral and cloud movement, attack path reduction, and so forth. Worth noting about deception, the working assumption is that the alerts coming from a deception platform are high fidelity — if the recreated files, registries, or IP/MAC devices are approached, there is no reason for the authenticated user to be attempting access.
- **Full packet capture (PCAP) and network performance monitoring (/NPM) tools.** The first set of these tools would be platforms that perform full packet capture for analytics and forensic investigations. The con about using PCAP tools is that storage is expensive and full fidelity event replay is hard to perform over time. Finding IoCs much less the actual adversary in PCAP tools is difficult. However, the long card is that with the proper investigative techniques, the truth is ultimately in the packets. In addition, in many instances, only PCAP is admissible in criminal court. Network performance monitoring have high bandwidth capabilities and were designed to monitor high media events, such as video and IP telephony. Statistical analysis of jitter and potential bottlenecks help telecom operators with media. Ultimately, many of the NPM tool providers converted their platforms for network security.
- **Emulation and deep packet insights.** Test emulation are tools that run threat simulations with payloads on a network that is slightly different from attack simulation (attack simulation is not included in this category, and, as a product group, not currently included in the cybersecurity AIRO taxonomy). Emulation occurs when a live agent is placed on machines that measure how a device is performing when real malware is introduced on a network emulation layer. The deep packet inspection tools come from vendors that perform file analysis and derivatives of sandboxes to identify IoCs. The advantage of this technology is that a sandbox creates latencies while a file is being convicted, important not only in North-South traffic but also in moving traffic laterally within internal servers.

RELATED RESEARCH

- *Worldwide Device Vulnerability Management Forecast, 2020–2024: What Lies Beneath the Attack Surface* (IDC #US46286620, May 2020)
- *Worldwide Device Vulnerability Management Market Shares, 2019: Finding the Transitional Elements Between Device Assessment Scanning and Risk-Based Remediation* (IDC #US46284720, May 2020)
- *Analytics: The Foundation of the Future of Trust* (IDC #DR2020_T7_CK, March 2020)
- *Security Orchestration, Automation, and Response: Perceived and Added Value* (IDC #EUR145951120, February 2020)
- *Worldwide Cybersecurity Analytics, Intelligence, Response, and Orchestration Forecast, 2019–2023: Finding and Mitigating the Adversary* (IDC #US44778919, December 2019)
- *Worldwide Cybersecurity Analytics, Intelligence, Response, and Orchestration Market Shares, 2018: Turning Alerts into Outcomes* (IDC #US44779319, December 2019)

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.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com