opentext™

POSITION PAPER

7 security trends shaping today's threat detection technology

Evolving and increasingly sophisticated threats drive an urgent need for new security approaches

opentext™

Contents

opentext™

Executive summary

The need for new security approaches has never been more urgent as organizations face sophisticated and ever-evolving malicious actors. With new threats arising every day, it is critical to implement detection capabilities that evaluate potential threats from a wide variety of perspectives and are continuously evolving.

This paper covers seven top security trends that are shaping threat detection technologies and explores why they should be top of mind for all businesses.

opentext™

Trend No. 1: Data quality matters in security analytics

Comprehensive understanding of your network requires attention to all three aspects: breadth, depth and accuracy. Cybersecurity analytics used to investigate network-based incidents are similar to techniques employed to investigate physical incidents. In both cases, you need evidence or data on which to reach and support your conclusions, and you need to be able to trust that data to be accurate.

Networks are the virtual hallways of your digital business, and you need to actively and continuously monitor them for undesirable activity. It is too late to turn on the surveillance camera after the crime has been committed. Observing everywhere continuously satisfies the breadth requirement for evidence, but it must satisfy a depth requirement too. Network packet traffic provides a "perfect fidelity" primary source of everything that transpired on your network, but should be abstracted or summarized into more manageable network metadata.

Trend No. 2: Threats hiding among the alerts deluge

Security teams are drowning in alerts. A 2021 study polling 2,303 IT security and security operations center (SOC) decision makers across companies of all sizes and verticals revealed that 70 percent of respondents said their home lives are being emotionally affected by their work managing IT threat alerts. Fifty-one percent of respondents feel their team is being overwhelmed and fifty-five percent admit that they aren't confident in their ability to prioritize and respond.[1]

As a result, real threats often slip through unchallenged. Good threat detection must help SOCs to identify and focus on the most likely and most dangerous threats and corresponding alerts rather than contributing to the confusion. It should evaluate anomalies from a variety of perspectives to gauge their level of threat. It also needs to be flexible to enable security analysts to establish unique and nuanced alert thresholds that can be customized to each specific environment. This improves its ability to distinguish the critical alerts from the noise and focus threat hunting efforts in time-critical windows.

Trend No. 3: Ransomware pressures pricing

Every 11 seconds a business is hit with ransomware.

Most digital crime is focused on getting one thing: money. Stealing data to sell on the dark web was once seen as easy profit, but one criminal was selling to yet another criminal, monetization rates were low and time-to-money was long.

In today's landscape, holding respectable and flush companies' data hostage for ransom is proving to be quicker, easier to monetize and much more profitable. Most companies now maintain a healthy paranoia about their defense against and resilience to ransomware attacks. But as long as companies continue to pay ransoms, the threat will continue to grow.

In 2021, 37 percent of all businesses and organizations were hit by ransomware and recovering from a ransomware attack cost businesses $1.85 million on average.[2] With the other costs associated with ransomware prevention, infrastructure hygiene, insurance and sometimes remediation, threat detection must be sensitive to delivering the optimal balance of significant value for a reasonable price point.

1 Help Net Security, The human cost of understaffed SOCs. (2021)

2 Cloudwards, Ransomware Statistics, Trends and Facts for 2022 and Beyond. (2022)

opentext™

Trend No. 4: Malware that spreads laterally

In the ongoing arms race between security professionals and hackers, detection and eradication tools must evolve to meet the challenge of each new malware variant. The latest technique, lateral spread, simultaneously establishes survivability within the perimeter and infects more targets to exploit. The impact of laterally spreading malware is growing and will continue for the foreseeable future.

Today, variants can spread without any user interaction at all. Modern ransomware campaigns, like those that affected JBS and Colonial Pipeline, are inside the target network long before the actual ransomware is deployed. Typically, attackers are moving laterally, stealing data and credentials, deploying additional tools and only executing ransomware as the final stage of the attack.

To thwart laterally spreading malware, threat detection must be deployed both at the perimeter and throughout the internal network. It cannot rely on just one detection method, instead incorporating a myriad of methods and examining threats rapidly from different perspectives to recognize their techniques. Doing so ensures laterally spreading malware is stopped early in its spread to minimize the cost of recovery.

Trend No. 5: Zero trust philosophy

Security is increasingly adopting a "zero trust" philosophy, mandating that internal network traffic must be segmented and monitored.

Previously, IT security could build a perimeter around an organizational network where the only paths in and out could be tightly controlled, providing a place for deep inspection. Unfortunately, those days are long gone.

On the heels of the consumerization of business technology, Cloud, BYOD, IoT and other trends have only created more ways for threats to sneak in. As a result, security is increasingly adopting a "zero trust" philosophy, mandating that traffic inside its network must be segmented and monitored.

In the past, IT operations objected to instrumentation of internal networks because of their associated performance degradations. However, higher network speeds and techniques, such as shared memory packet inspection and file-carving, enable modern sensors to provide improved protection at much higher speeds without noticeable network impacts.

Trend No. 6: The rise of threat hunting

An emerging trend in cybersecurity today is threat hunting. Organizations start with the premise that they have been breached—true or not—and then look ("hunt") for evidence of the threat, its spread and/or damage it has inflicted.

Security analysts employ a combination of data gathering, analytics, experience and intuition to investigate inexplicable IT and network activity, atypical user behavior and anomalous data points. Threat detection systems have the capacity to monitor networks for anomalies and should be able to support threat hunting with the same network traffic and rich metadata they have already captured for anomaly detection.

Trend No. 7: Integration is paramount in security

New threat variants and attack vectors come so fast that enterprises are left with little choice other than to explore new tools to solve specific, emerging problems. As a result, the SOC can accumulate a portfolio of security tools. A recent survey of 1,200 US and UK enterprise security decision-makers found that the shift to cloud and remote working over the last two years has driven a 19 percent increase in the number of security tools organizations must manage—from 64 to 76.7.[3]

Since many security tools do not work in tandem with each other, integration and correlation of disparate data sources is done manually by the security team, often on a simple spreadsheet. As new tools are added, the problem expands exponentially.

Open standards and APIs support ease of integration amongst disparate tools and leads to a fluid and interoperable security fabric. They enable each tool to perform its own specialized function, and to share outputs to form an end-to-end kill chain.

Make sure that your threat detection system can receive inputs, such as rules and signatures, from open external sources, and that it can share its threat detection data with downstream containment and eradication tools as well.

3 Panaseer, Panaseer 2022 Security Leaders Peer Report. (2022)

opentext™

Security
OpenText Blogs

Threat Detection and Response
OpenText Solutions

Full-spectrum threat detection with OpenText™ Network Detection & Response

Staying on top of these trends is a tall order. More are certainly coming, and the old ones never go away. If you are like most security professionals, threat protection is just one of your many responsibilities. You need help.

OpenText NDR (formerly Bricata) provides a single-platform, full-spectrum threat detection solution that addresses these current security trends and continues to evolve along with the threats. The right combination of technologies is seamlessly integrated to deliver comprehensive enterprise threat protection in a form factor that is easy to use and manage, increases productivity (which speeds time to resolve) and minimizes total cost of ownership.

OpenText NDR has been proven to speed incident resolution by reliably detecting threats and providing the context necessary to get to the truth.

OpenText NDR keeps you ahead of the trends:

1. Captures full network packet traffic as its basis of truth and generates industry gold standard metadata summarizing every transmission.
2. Employs a range of different threat detection technologies, from signatures to artificial intelligence for zero-day malware, to deliver accurate threat alert priorities.
3. Provides highly competitive pricing for the unparalleled set of integrated capabilities, based on your aggregate network traffic volumes not how many devices are deployed.
4. Can be deployed both at your perimeter, to protect against malware ingress and data egress, and on your internal network, to protect against laterally moving malware.
5. Because your network perimeter is becoming less-defined daily, OpenText NDR becomes an active part of your network, continuously evaluating everything that transpires on it.
6. Captures rich network metadata that is centralized and fully indexed to create a powerful threat hunting environment with intuitive user interfaces, expert system workflows and visualization capabilities.
7. Adheres to open standards and open APIs to readily share the data it collects and generates with other cybersecurity tools. It also accepts rules, scripts and signatures from third-party threat intelligence sources.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

opentext.com/contact