Progress® Flowmon®

The Cybersecurity Threat Landscape in 2024

WHITEPAPER

Despite the best endeavors of many cybersecurity professionals to minimize threats, there will likely be no decrease in the threat levels faced by organizations of all sizes in 2024. As a result, cybersecurity teams are under immense pressure to reduce the risk to their organizations. They need to focus on identifying and mitigating the most significant threats that will likely occur during 2024 and beyond.

This white paper provides an overview of the cybersecurity landscape for 2024 and the areas that leadership teams should focus on to enhance their cybersecurity protections.

The Rise of AI-powered Attacks

Generative AI based on LLM (Large Language Model) technology is rapidly transforming the cybersecurity landscape, with both attackers and defenders utilizing its capabilities. Cybercriminals are using AI to automate attacks, develop more complex malware and avoid detection. However, using LLM and other techniques also provides the following:

- Tools for cybersecurity defenders.
- Helping detection of threats in real-time.
- Enabling better diagnosis of incidents and the rapid automation of responses.

Security leaders must prepare for the rapid evolution of Generative AI, as applications using it are only beginning their journey. There are many opportunities for increased productivity, reducing the skills gap and other benefits for cybersecurity. At the same time, business leaders also need to encourage safe and secure use of this emerging technology.

Ransomware, Malware, Supply Chain, Phishing, Crypto, IoT, Insider Risk

There are many threats targeting IT systems in 2024. We summarize the main ones below. Note that this is not an exhaustive list of areas a cybersecurity defense strategy must counter. Other unforeseen and emerging threats also need to be considered in any defense strategy.

The use of a modern Network Detection and Response (NDR) solution to detect anomalous network activity is a good foundation for a multilayered defense strategy. See the Conclusion section below for links to Flowmon NDR info and how to start a free trial that can start protecting your network within minutes.

Ransomware

Ransomware will continue to be a significant threat to organizations of all sizes in 2024 and beyond. Cybercriminal ransomware-as-a-service resources that are widely available for anyone to use have lowered the bar for entry to people looking to profit from this type of attack.

Individual ransomware attacks are also increasing in sophistication. During 2024, this trend will prompt organizations to strengthen their efforts and adopt more resilient cybersecurity strategies to help mitigate the impact if company defenses get breached.

Consolidated information from multiple industry sources shows:

- Ransomware played a part in 24% of all data breaches — as reported in the Verizon 2023 Data Breach Investigations Report (DBIR).
- A total of 66% of all organizations were impacted by ransomware in 2023, according to Sophos' The State of Ransomware Report.
- There have been over 130 different ransomware variants tracked since 2020, according to the VirusTotal Ransomware in a Global Context report. From these:
    - The most commonly seen was the GandCrab ransomware family, which was at 78% of the total.
    - Windows OS executable files or DLLs (Dynamic Link Libraries) were the vectors for delivering 95% of all ransomware.

Malware

Ransomware is the most common type of malware that organizations are most likely to encounter in 2024. Other examples of malware that could target organizations include:

- Wipers that work like ransomware but erase data rather than encrypt it for profit.
- Spyware that sits on systems and collects data.
- Keyloggers that record keyboard activity for attackers.

- Adware that displays unwanted ads that generate revenue for attackers.
- Trojans that mimic legitimate software to trick users into running it.
- Worms that exploit known vulnerabilities to spread between systems.
- Viruses are still prominent and become a large-scale problem if not mitigated.
- Bots and botnets that typically disrupt systems via denial-of-service attacks.

All these need to be monitored for and dealt with if detected.

Supply Chain Vulnerabilities

Upstream and downstream business partners in the supply chain can be a source of cyberattacks. This means that threats originating via linked IT systems need to be quantified and mitigated.

The risk of supply chain attacks will be high in 2024. These attacks aim to compromise a company's network by exploiting vulnerabilities in its third-party suppliers, software, or service providers. To mitigate this significant risk, organizations need to prioritize building stronger supply chain resilience. IT teams can achieve this by focusing on proactive vendor security assessments, rigorous software management, network monitoring and incident response planning.

Key circumstances driving this risk include:

- Increased Complexity - Supply chains are becoming increasingly complex, with multiple vendors and interconnected systems. This creates an expanded attack surface that's difficult to comprehensively monitor and secure.
- Software Vulnerabilities - Software dependencies often get deeply embedded in modern organizations. Unpatched or zero-day vulnerabilities in widely used software can ripple through an entire supply chain.
- Geopolitical Tensions - State-sponsored cyberattacks are rising, and they can disrupt critical infrastructure or businesses on a national scale.

- Lack of Visibility - Many organizations lack complete visibility into their supply chain's security posture, making it hard to identify and mitigate risks from third-party providers.

Supply Chain Attacks can have severe consequences:

- Data Breaches - Attackers can steal sensitive data, including intellectual property, customer information, or financial records.

- Operational Disruption - Ransomware attacks or targeted disruptions can shut down critical systems, causing significant financial losses and hindering business operations.

- Reputational Damage - Breaches caused by supply chain weaknesses erode customer and investor trust.

Unfortunately, the frequency and sophistication of supply chain attacks will likely increase in 2024.

Phishing and Other Social Engineering Attacks

Frequently, people are the weakest link in the security chain. This statement isn't to disparage anyone — we all make mistakes, but defenders need to incorporate this fact into cybersecurity planning. The sophistication of social engineering attacks, like phishing emails, is still a successful attack vector and a source for gathering data for future attacks.

These attacks are becoming more sophisticated as criminals use LLMs (as mentioned above) and deepfake AI video generation tools to compose more realistic emails, videos, dummy websites and other collateral to trick people into clicking malicious links or divulging data they shouldn't.

Business email compromise (BEC) and targeted spear-phishing attacks will continue to be common in 2024 as attackers target prominent individuals and their associates within organizations. We can also expect bad actors to use AI deepfake video and audio portrayals of real people to trick staff as part of phishing attacks. A Hong Kong company recently transferred the equivalent of $25.6M to cyber criminals after a scam featuring a digitally recreated version of the company's chief financial officer, along with other employees, who appeared in a video conference call instructing an employee to transfer funds. Scams like this and others built on emerging AI tools will become more common.

Crypto Scams

Crypto scams are types of social engineering-based attacks. In crypto scams, attackers send an innocuous message to a mobile phone or messaging service to lure the recipient into a conversation. For example, “Are you still free for lunch on Monday?” Then, they try to build a rapport with the recipient before asking them if they want to make some cash via crypto and luring them to a scam website that steals their money. Through the scam site, these attacks open the victim’s organization to other social engineering threats or malware. We can expect these scam attacks to become more sophisticated due to AI tools making them more believable.

IoT Vulnerabilities

Internet of Things (IoT) sensors and devices are expanding almost exponentially in the built environment and manufacturing. Some of these IoT devices have notoriously poor security. We’ve all heard of cases where multiple instances of a device get shipped with the same admin account and password. One that often doesn’t get changed during deployment.

This expansion of IoT devices increases the attack surface, which introduces easily exploitable vulnerabilities. If the IoT devices have access to other network systems, this can open a back door for anyone who knows the default account settings.

Insider Risk

Acknowledging that cybersecurity threats do not only come from external attackers is essential. Insider threats, which are cybersecurity risks originating from people within an organization, should not be overlooked. Individuals with access to IT systems as part of their job function are the source of most insider threats.

Insider risks from disgruntled employees or staff paid off by attackers are significant. From a cybercriminal’s perspective, why spend time looking for vulnerabilities when you can bribe an employee to take a malware-infected USB drive and plug it into a PC on the network? Protective measures like 24x7 NDR and zero-trust best practices to prevent malicious code spreading between systems are core to helping guard against this and other attack methods.

Cybersecurity Talent Shortages

As the number of cyberattacks continues to increase, organizations struggle to retain existing security professionals and hire new staff. This deficit of professional resources continues to pose challenges for organizations looking to bolster their defenses against attackers. Analysts expect there to be 3.5 million unfilled cybersecurity jobs in the market by 2025. Suffice it to say that skilled cybersecurity talent will still be hard to come by in 2024 and beyond.

The ISC2 Cybersecurity Workforce Study published in November 2023 reports that the growth for cybersecurity professionals broken down by global region was:

- **Asia-Pacific:** up 11.8% year-on-year to 960,000.
- **Middle East and Africa:** up 11.7% year-on-year to 402,000.
- **North America:** up 11.3% year-on-year to 1.5 million.
- **Europe:** up 7.2% year-on-year to 1.3 million.
- **Latin America:** up 4.5% year-on-year to almost 1.3 million.

Despite this growth, the ISC2 report also estimates significant shortfalls in the number of people available to fill cybersecurity jobs. The shortfalls by region they estimate are:

- **Asia-Pacific:** 2.7 million
- **North America:** 522,000.
- **Europe:** 348,000
- **Latin America:** 348,000
- **Middle East and Africa:** 112,000

The reasons behind the current cyber talent shortage are multi-faceted and varied — however, most causes originate from the expansion of digital transformation sweeping across industries. This has resulted in a shortfall of qualified security professionals. Many organizations struggle to upskill existing staff to meet rising security challenges and vacancies.

Though this shortage in cybersecurity talent is an issue shared by most organizations, businesses can mitigate their cyber risk with a limited staff count using appropriate tools and technologies, such as Flowmon NDR. Businesses that are proactively planning, using the right tools and equipping their current team members with the skills for success are best positioned to mitigate cyber threats, even in a job market where team members are hard to recruit.

Cost of Cyber Breaches

Cybersecurity Ventures predicts that the global cost of cybercrime will be over $9 trillion in 2024 and that this figure will increase by 15% to , with similar growth in the years beyond.

These are sobering figures, and a significant proportion of the overall cybercrime costs to businesses and other organizations will be due to the costs associated with dealing with data breaches. Ransomware recovery operations will also be a sizable chunk of the overall figure.

The last few years have demonstrated that cybercriminals are relentless opportunists who will exploit every opportunity to extort money from their victims or sell stolen data to others.

Data Security, Compliance and Regulatory Trends

Data security, compliance and regulatory trends will significantly impact how organizations think about and deliver cybersecurity defenses in 2024 and beyond. Ways that these areas will shape thinking include:

- An Evolving Regulatory Landscape.
  - **GDPR** - The EU General Data Protection Regulation (GDPR) has become a global benchmark that many organizations look to work within so they can work within or export to the EU. Plus, many nations are either adopting similar regulations or tightening their existing data privacy laws similar to GDPR and other emerging EU regulations. The California Consumer Privacy Act (CCPA) is another example that has

impacts beyond the originating US state.

- **Sector-Specific Regulations** - Industry-specific regulations from governments and within industry sectors are important drivers of cybersecurity response and strategy. Healthcare (HIPAA), finance (PCI DSS), critical infrastructure and other sectors face increasingly stringent compliance requirements specific to their industries.
- **Other regulations** - Many new regulations and standards are being discussed and developed across multiple global regions. For example, within the US Federal Trade Commission, the Food and Drug Administration, the Department of Transportation, the Department of Energy and the Cybersecurity and Infrastructure Security Agency. Similarly, the White House, Congress and the Securities and Exchange Commission (SEC) are focusing on rules for reporting cyber incidents. Across the globe, China has instituted new data localization measures, while India and the EU have expanded or added additional detail levels to their existing incident reporting requirements.

- **Zero-Trust Architecture** - When an organization implements a zero-trust architecture on its network, every connection is considered potentially hostile, irrespective of where it originates. A request to access an application that comes from within the network perimeter (such as from a PC in the corporate HQ) gets treated the same as one that originates on the Internet via a remote connection. Both need to satisfy the same level of cybersecurity before access is allowed. No connection is assumed to be safe based on where it originates. This level of cybersecurity moves beyond the traditional model of securing the perimeter. As a result, zero trust is also sometimes described as creating a software-defined perimeter (SDP).

- **Evolving Threat Landscape** - The constantly changing threat landscape will influence cybersecurity thinking and planning in 2024. Specific areas that will likely impact cybersecurity include:
  - **Ransomware 2.0 and Double/Triple Extortion** - Ransomware has evolved into a more complex threat and is sometimes referred to as Ransomware 2.0. The new threat not only involves data encryption but also data theft, leading to a double extortion scenario were attackers steal the data before encrypting it and then hold the copied data for ransom. In addition, they threaten to leak the data on the web, which can cause significant reputational damage. Triple extortion can come via a ransom demand to decrypt data, a fee to buy back the data and increasingly, the criminals directly contacting people and organizations whose contact details are in the stolen data to get them to pay to prevent public release.
  - **State-backed Attacks** - State-sponsored cyberattacks against nationally important industries pose a significant threat, requiring organizations to bolster their defenses against well-funded and highly skilled adversaries.

Conclusion

If history is any indication, third-party cyber threats in 2024 will continue to dominate the risk landscape as firms become increasingly connected through integrated software supply chains and vendor relationships. To reduce their attack surface and mitigate potential security exposures, organizations need to consider the impact that third parties, partners, vendors and even customers have on their overall cyber risk posture.

From a compliance perspective, laws and regulations will likely get more stringent in 2024 and beyond. In terms of talent, highly trained security professionals will continue to be coveted by organizations large and small across all industries.

How Flowmon NDR Can Help Your Defense

From DevSecOps to data science and cybersecurity, most IT disciplines deploy network traffic monitoring extensively to gain visibility and situational awareness about the network's state in real time. Effective infrastructure and network traffic monitoring and anomaly detection and response are critical for maintaining network continuity and continuous improvement across modern IT environments.

Flowmon can enable your network and security teams to achieve the shared goal of delivering a stable and healthy digital environment. As networks increase in complexity, as hybrid environments become common and threats become ever more sophisticated, Flowmon has the tools to help your business operate smoothly, safely and with greater agility by helping minimize modern threats.

Try Flowmon for Free

If you are evaluating NDR solutions or haven't thought about deploying one yet, you will benefit by trying the detection capabilities of Flowmon. We're confident you will find that when you try Flowmon, you'll discover it delivers enhanced protection, informative reporting and cost savings for your cybersecurity team.

But don't take our word for it. Your organization can evaluate our solutions by visiting the Flowmon product overview pages to read more or by reaching out to us to discuss your needs. You can also start a free trial to see for yourself how Flowmon starts protecting your networks within hours after deployment.

References

1. TechTarget Security: Ransomware trends, statistics and facts heading into 2024 - https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

2. Verizon: 2023 Data Breach Investigations Report - https://www.verizon.com/business/resources/reports/dbir/

3. Sophos: The State of Ransomware 2023 - https://www.sophos.com/en-us/whitepaper/state-of-ransomware

4. VirusTotal: Ransomware in a global context - https://assets.virustotal.com/reports/ransomware-in-a-global-context-2021

5. Are Technica: Deepfake scammer walks off with $25 million in first-of-its-kind AI heist - https://arstechnica.com/information-technology/2024/02/deepfake-scammer-walks-off-with-25-million-in-first-of-its-kind-ai-heist/

6. Cybersecurity Ventures: Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025 - https://cybersecurityventures.com/jobs/

7. ISC2: Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap - https://www.isc2.org/Insights/2023/11/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-Workforce-Gap

8. Cybersecurity Ventures: Cybercrime To Cost The World 8 Trillion Annually In 2023 - https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

9: Flowmon: Visualize Network Traffic, Identify Issues & Prevent Cyber Incidents - https://www.flowmon.com/