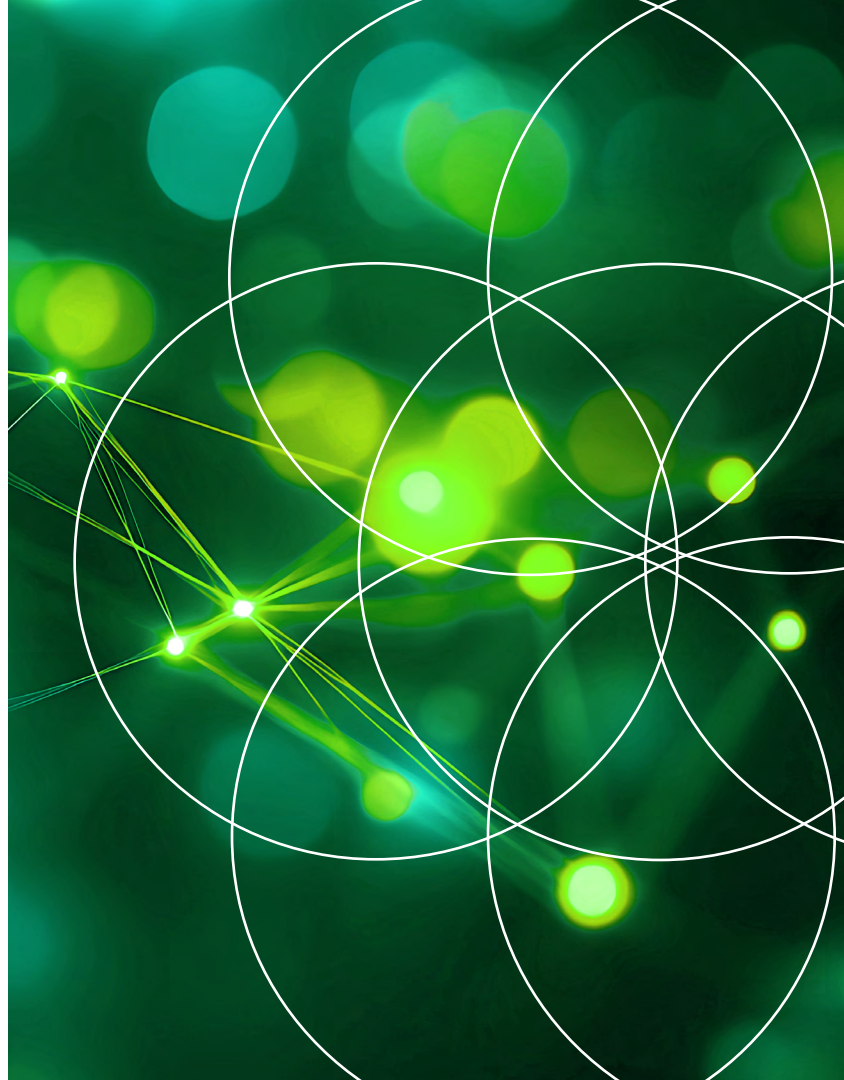


Embrace DNS Security And Overcome Hurdles Of Cloud Adoption

The Critical Role Of DNS In Securing Hybrid Cloud
Networks And Reducing Risk Amid Rising Cyberthreats

Get started →



The Adoption Of Hybrid And Public Cloud Is Increasing, Along With DNS Threats

In 2025, the adoption of hybrid and public cloud is expected to continue to grow as enterprises strive for agility, scalability, and operational efficiency. The cloud landscape is undergoing significant changes: AI is enhancing public cloud strategies and services while also boosting private cloud as organizations seek to balance innovation, compliance, and control.¹

As the cloud landscape evolves, so does cybersecurity. Security teams are confronting new risks, wider attack surfaces, strategic shifts, and increased network-related complexity as well as increased frequency of Domain Name System (DNS)-based attacks.

EfficientIP commissioned Forrester Consulting to explore the state of DNS security at large companies in North America and Europe. This study involved a survey of 218 senior decision-makers responsible for security strategy.

Key Findings



95% of organizations have experienced cyberattacks or vulnerabilities related to DNS in the last 12 months. Decision-makers recognize the financial, reputational, and legal impact of these incidents.



71% of security decision-makers say their orgs struggle with the complexity of hybrid cloud environments. They also feel a lack of control over DNS traffic, along with insufficient skills and tools.



Decision-makers identified several key initiatives to enhance cloud security and respond to threats, including DNS security, threat intelligence, cloud migration security, Zero Trust, and AI tech.

DNS Attacks: A Multifaceted Threat To Organizations

Network-related cyberattacks are alarmingly common — 95% of security decision-makers reported that their organizations experienced DNS-related incidents in the past year. Phishing (52%), ransomware (52%), and DDoS (50%) attacks dominate the threat landscape.

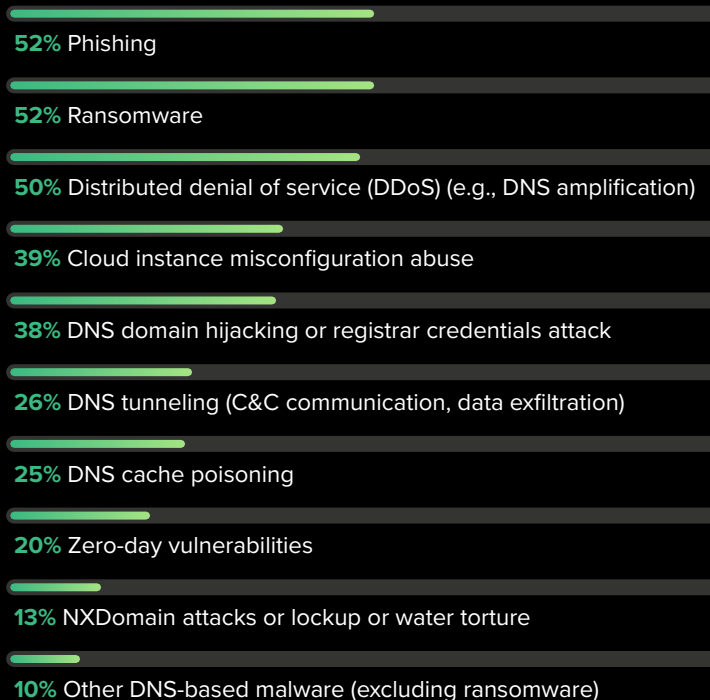
DNS attacks have far-reaching consequences: 62% of security leaders reported that their organizations faced disruptions to productivity and system availability, 61% faced financial impacts, and 59% suffered damage to brand reputation.

Over half of respondents experienced breaches of sensitive data, and one-third encountered legal repercussions due to inadequate data protection and management under regulations (e.g., GDPR, HIPAA).



95% of decision-makers reported that their organizations have experienced DNS-related incidents in the past year.

“Which of the following DNS attacks or vulnerabilities has your organization been subject to in the last 12 months?”



The Soaring Costs And Financial Fallout Of DNS Cyberattacks

DNS attacks and vulnerabilities expose organizations to severe financial consequences. According to 53% of security decision-makers in our survey, the average cost per attack falls between \$500,000 and \$5 million, including cost of mitigation, FTE resources spent to recover, and business damage.

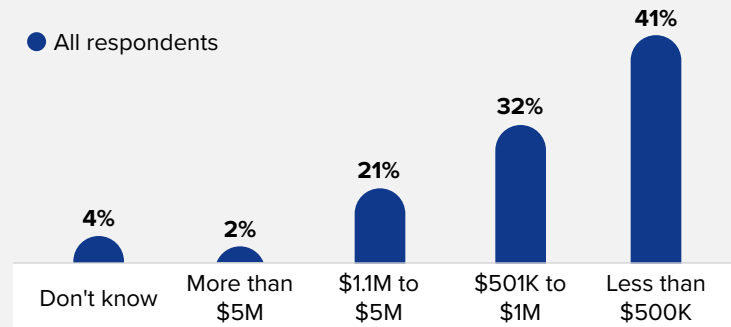
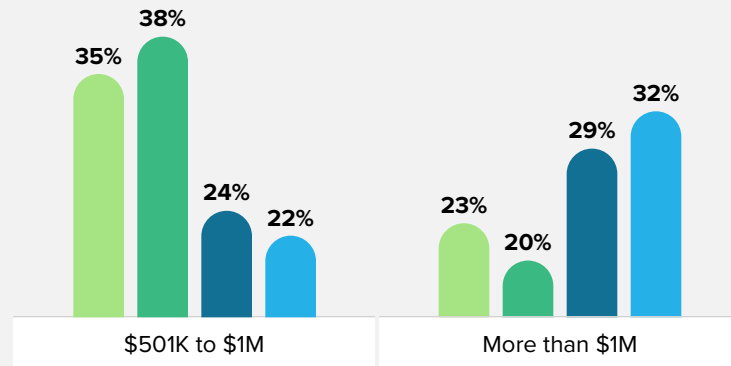
The financial impact is significant for midsized and large enterprises. Organizations with 500 to 4,999 employees are more likely to report average costs between \$501,000 and \$1 million. Larger companies with 5,000 to 19,999 employees are considerably more likely to incur losses exceeding \$1 million per incident.



The average cost of an attack, as reported by interviewed security leaders, was **\$1.1 million**.

Average Cost Of DNS Attacks

- 500 to 999 employees
- 1,000 to 4,999 employees
- 5,000 to 9,999 employees
- 10,000 to 19,999 employees

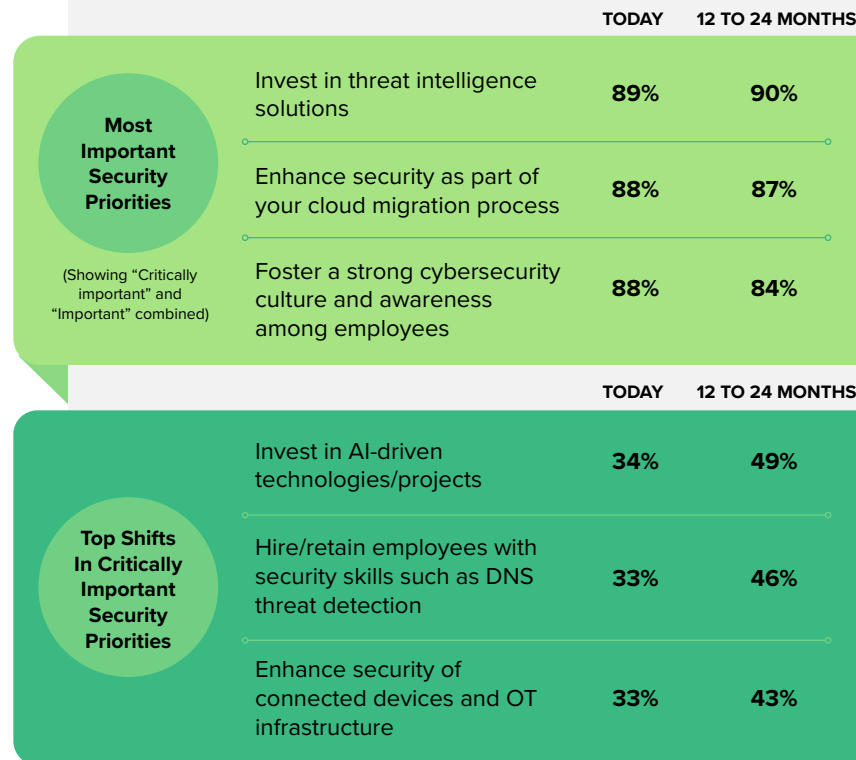


Strategic Security Priorities Are Evolving To Strengthen Resilience

As the cybersecurity landscape evolves, organizations are proactively aligning their strategies to address emerging threats and technologies. Several key focus areas have emerged as strategic pillars for resilience in the short, medium, and long term. Today's top five priorities for security leaders are investing in threat intelligence solutions (89% say it's critically important or important), enhancing cloud migration security (88%), fostering a cybersecurity culture (88%), improving threat detection and response (86%), and improving data privacy strategy (86%).

Looking ahead, security leaders are increasingly adopting advanced solutions such as AI-driven security technologies (49% say it's critically important) and acquiring specialized DNS expertise (46%). Also, securing IoT and operational technology infrastructure (43%) and implementing SASE (41%) are gaining prominence as digital ecosystems expand.

Strategic Cybersecurity Priorities For The Present And Beyond



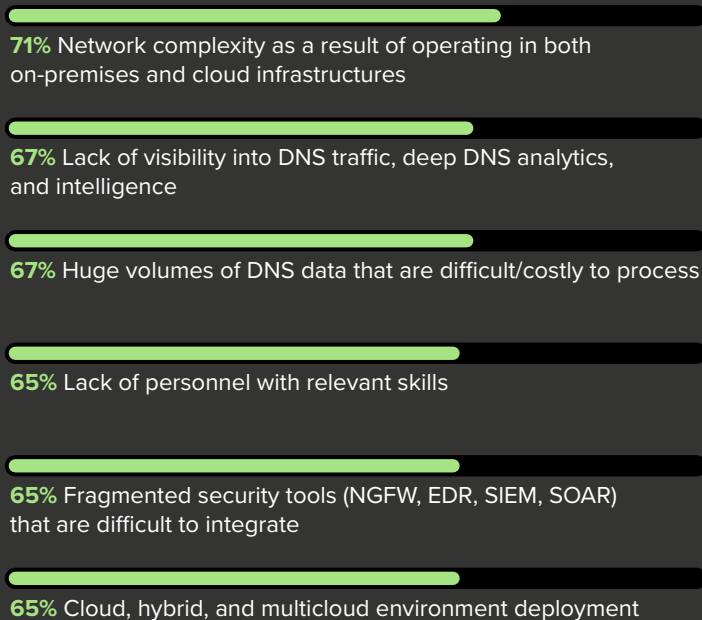
DNS Vulnerabilities Threaten Critical Infrastructure And Assets

Unsurprisingly, 71% of security leaders feel overwhelmed by the complexity of managing modern networks. Two-thirds of security leaders expressed concern over the lack of visibility into DNS traffic and DNS analytics/intelligence that could help them quickly detect misconfigurations, vulnerabilities, or DNS-based attacks. Such incidents can lead to severe consequences, such as system outages, degraded user experiences, and legal issues stemming from malware-driven data breaches. Moreover, 67% struggle to process massive volumes of DNS data, hindering their ability to gain critical insights necessary for timely anomaly detection and response.

Compounding these challenges is a lack of standardized processes and insufficient cloud-native expertise (65%), making it difficult to deploy hybrid and multicloud environments effectively. Security leaders also reported fragmented and poorly integrated tools (65%).

“How challenging are each of the following to your security teams to effectively defend and protect your network?”

(Showing “Highly challenging” and “Challenging”)



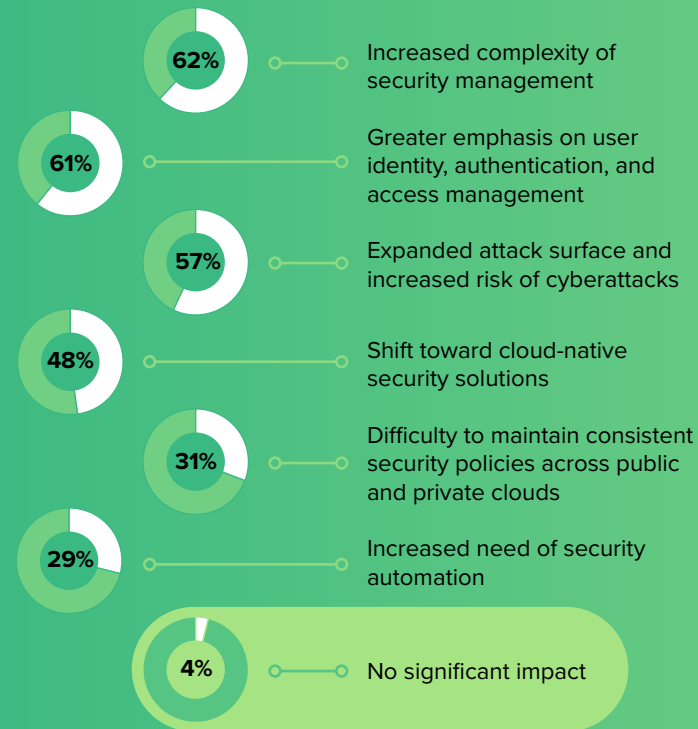
Traditional Security Approaches And Tools Are Unsuitable In A Cloud-Driven World

The acceleration of cloud adoption and anywhere access is reshaping cybersecurity, with 96% of security leaders reporting major strategy shifts. These are more than just technical adjustments — they demand the adoption of new tools and processes, including security automation, to foster a more integrated infrastructure and ensure visibility, compliance, and overall protection.

Over 60% of leaders indicated that the new, complex cloud environments outpaced traditional perimeter-based security models and tools. As a result, 61% reported greater emphasis on access control and management, accelerating their move toward Zero Trust Network Access. Over half observed an expanded attack surface, heightening the risk of misconfigurations, data breaches, and attacks across access points. DNS misconfigurations, such as exposed internal records, can disclose cloud infrastructure details and facilitate targeted attacks.

“How has increased cloud adoption affected your security strategy?”

(Select top three)



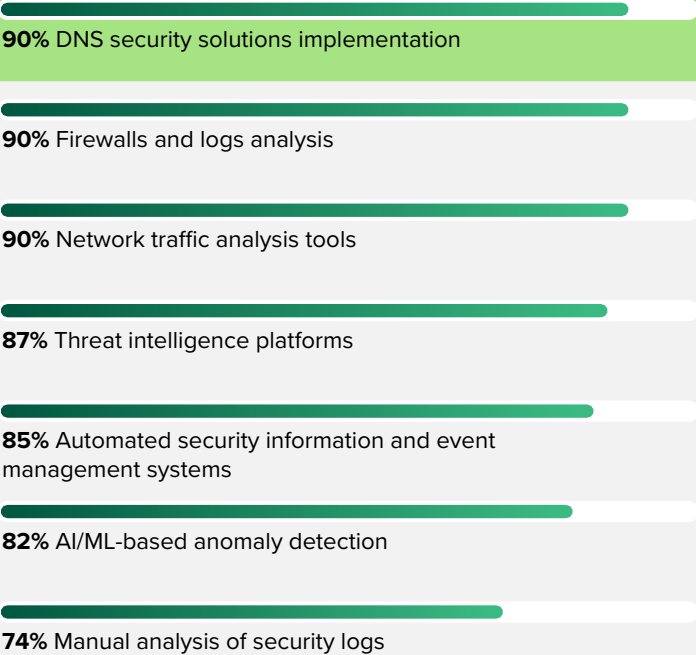
Security Leaders Make DNS Security Central To Their Security Strategy

Organizations increasingly recognize that DNS is not just a backend protocol but a critical frontline defense, with 90% of security leaders acknowledging its importance in monitoring for suspicious network activity. Its equal ranking with firewalls and network traffic analysis tools highlights its growing role in early threat detection, particularly in cloud and hybrid environments. The great emphasis on machine learning (ML)-based anomaly detection confirms the shift toward proactive intelligent monitoring.

Security teams are shifting from perimeter protection to more granular control of their networks. Over 60% of security leaders indicated that DNS security gave them more detailed visibility into network traffic, allowing more detailed flow inspection. Also, 59% indicated that DNS filtering supported policy enforcement against malicious domains, and 55% recognized DNS’s role in enhancing threat detection.

“How important is each of the following to your security team to monitor for suspicious network activity?”

(Showing “Critically important” and “Important”)



DNS Security: A Key Ally In Navigating The Complexity Of Cloud Adoption

As hybrid and multicloud environments grow more complex, DNS security becomes a key control point — offering visibility, enforcing access policies, and enabling threat detection. Over 50% of security leaders value DNS-centric threat intelligence for identifying threats, speeding up investigations, and improving forensic analysis.

Furthermore, firms operate in an increasingly data-centric world, with shifting threats and perimeters. Thus, 84% of security teams prioritize Zero Trust Architecture, which is built for boundaryless enterprises where users and devices operate across multiple clouds and locations.² ZTA also enhances data protection and regulatory compliance — top priorities for over 80% of decision-makers. Also, many expect automation to improve threat detection and response (67%), data protection (55%), and network policy management (46%), making processes faster, more consistent, and adaptive.

Top Initiatives To Improve Cloud Infrastructure Security

(Showing “Critically important” and “Important”)

91% Improve monitoring and analysis of DNS traffic

88% Enhance data protection and encryption

85% Perform regular DNS audits of DNS configuration to identify and mitigate vulnerabilities

85% Develop a cloud-specific incident response plan

84% Boost identity and access management by enforcing multifactor authentication or Zero Trust Architecture

81% Increase the number of DNS filtering rules

81% Increase the adoption of AI-powered threat detection technologies

80% Enhance network security through Zero Trust Network Access (ZTNA)

Conclusion

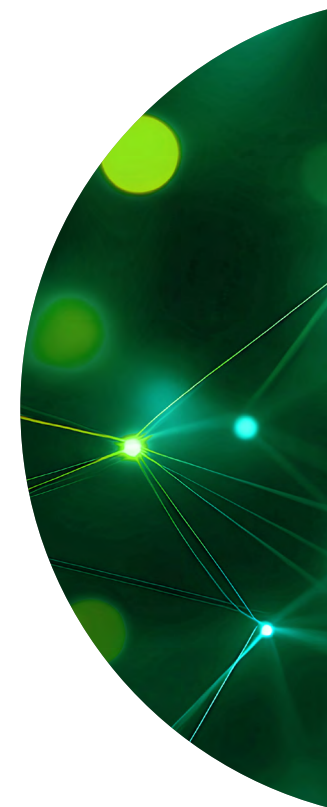
Adoption of hybrid and public cloud is expected to grow and evolve, along with the cybersecurity landscape. This comes with new threats, challenges, and network complexity for security leaders.

- **DNS attacks are taking their toll.** Organizations face numerous DNS attacks, resulting in severe consequences, including financial losses amounting to millions of dollars.
- **DNS security is becoming a frontline defense.** As network complexity grows, organizations are turning to DNS security to enhance visibility, threat detection, and policy enforcement, making it a critical layer in security cloud infrastructure.
- **Security strategies must adapt to ease cloud complexity.** Traditional security models fall short in cloud-native environments. To respond to evolving threats, orgs are shifting to new automated solutions and ZTA.

Endnotes

¹ Source: [Prediction 2025: Cloud Computing](#), Forrester Research, Inc., October 22, 2024.

² Source: [The Business Of Zero Trust Security](#), Forrester Research, Inc., July 11, 2023.



Resources

Related Forrester Research:

[Prediction 2025: Cloud Computing](#), Forrester Research, Inc., October 22, 2024.

[The State Of Cloud In Europe, 2024](#), Forrester Research, Inc., December 6, 2024.

[The State Of Cloud In The US, 2024](#), Forrester Research, Inc., November 15, 2024.

[The Business Of Zero Trust Security](#), Forrester Research, Inc., July 11, 2023.

[Zero Trust Everywhere Is The Security Model Of The Future](#), Forrester Research, Inc., September 5, 2024.

Project Team:

Tarun Avasthy,
Principal Market Impact Consultant

Corrado Loreto,
Market Impact Consultant

Miriam Oestreich,
Market Impact Consultant

Contributing Research:

Forrester's [Technology Architecture & Delivery](#) research group

Methodology

This Opportunity Snapshot was commissioned by EfficientIP. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 218 senior decision-makers responsible for security strategy at North American and European companies. The custom survey began and was completed in April 2025.

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective [research-based consulting](#) to help leaders deliver key outcomes. Fueled by our [customer-obsessed research](#), Forrester’s seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. [E-62853]

Demographics

COUNTRY	
United States	35%
Canada	16%
United Kingdom	16%
France	12%
Spain	11%
Germany	9%

NUMBER OF EMPLOYEES	
500 to 999	30%
1,000 to 4,999	28%
5,000 to 9,999	10%
10,000 to 19,000	18%
20,000+	13%

Note: Percentages may not total 100 due to rounding.

RESPONSIBILITY FOR SECURITY STRATEGY	
Final decision-maker	40%
Part of a team making decisions	32%
Decision influencer	28%

RESPONDENT LEVEL	
C-level executive	8%
IT-related VP	11%
IT-related director	35%
IT-related manager	29%
Cybersecurity analyst	7%
IT infrastructure architect	6%
Security engineer	2%
Other	2%

The background is a dark green gradient. Overlaid on this is a complex network of thin, light green lines connecting various nodes. Some nodes are small, bright green dots, while others are larger, glowing green circles. The network structure is organic and interconnected, with lines radiating from central points to peripheral ones. The overall aesthetic is high-tech and digital.

FORRESTER®