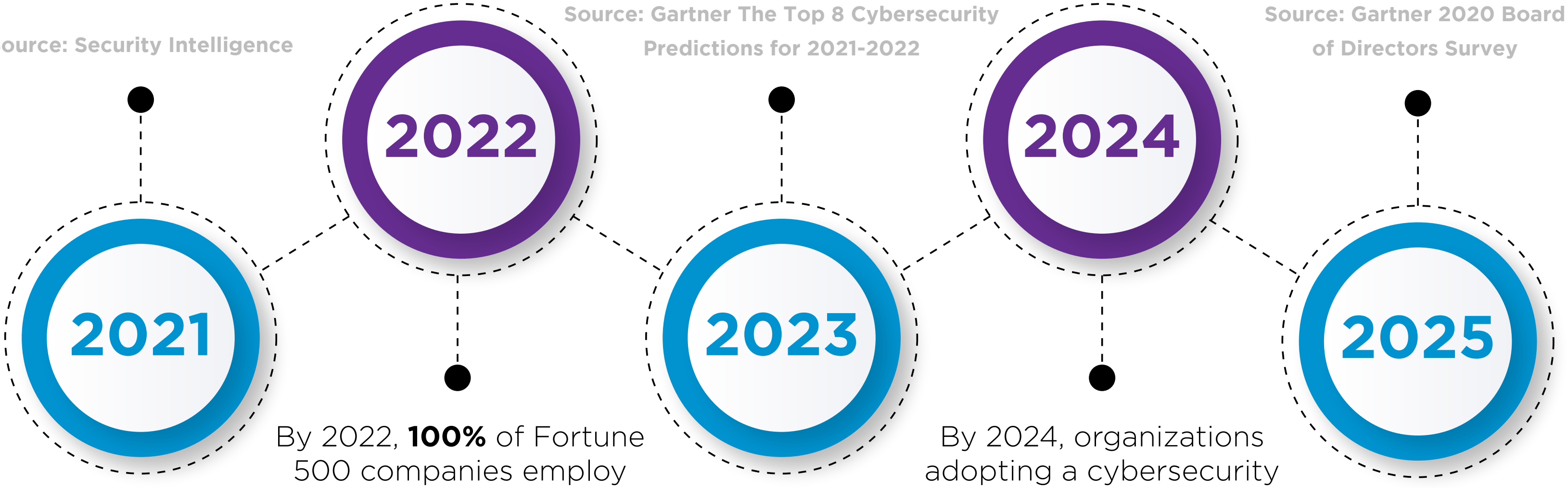
noesis
an Altia Company

TOP 8 CYBERSECURITY CAPABILITIES FOR IT LEADERS

The guidelines and investment priorities to secure a resilient cybersecurity roadmap.

Cybersecurity: You’ve been warned!



2021 was a banner year for cyber attacks. Compared to 2020, last year saw a **50%** increase in attacks per week on corporate networks.

Source: Security Intelligence

By 2022, **100%** of Fortune 500 companies employ a CISO or equivalent, compared to the **70%** in 2018.

Source: Cybercrime Magazine 2022 Cybersecurity Almanac

By 2023, **75%** of organizations will restructure risk and security governance to address the widespread adoption of advanced technologies, an increase from fewer than **15%** today.

Source: Gartner The Top 8 Cybersecurity Predictions for 2021-2022

By 2024, organizations adopting a cybersecurity mesh architecture will reduce the financial impact of security incidents by an average of **90%**.

Source: Gartner The Top 8 Cybersecurity Predictions for 2021-2022

By 2025, **40%** of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member, up from less than **10%** today.

Source: Gartner 2020 Board of Directors Survey

Cybersecurity outlook

The growing sophistication of cybercriminals, the exponential increase in their attacks, with higher complexity and diversity, and the evolution of attack techniques, pose new security challenges that traditional approaches are unable to address.

> *The current context poses a huge challenge to IT departments and has also been an impetus for a change not only in mentality, but also in prioritization and investment, when it comes to cybersecurity.*

Nuno Cândido

IT Operations, Cloud & Security
Associate Director
Noesis

> *It's time for organizations to refocus their strategy and reassess the critical aspects of the security architecture and empower themselves in a structured way with cutting-edge services and technologies to safeguard against increased cyber-exposure and insider threats.*

José Gomes

IT Operations, Cloud & Security
Associate Director
Noesis

Emotions CIO’s definitely don’t want to experience

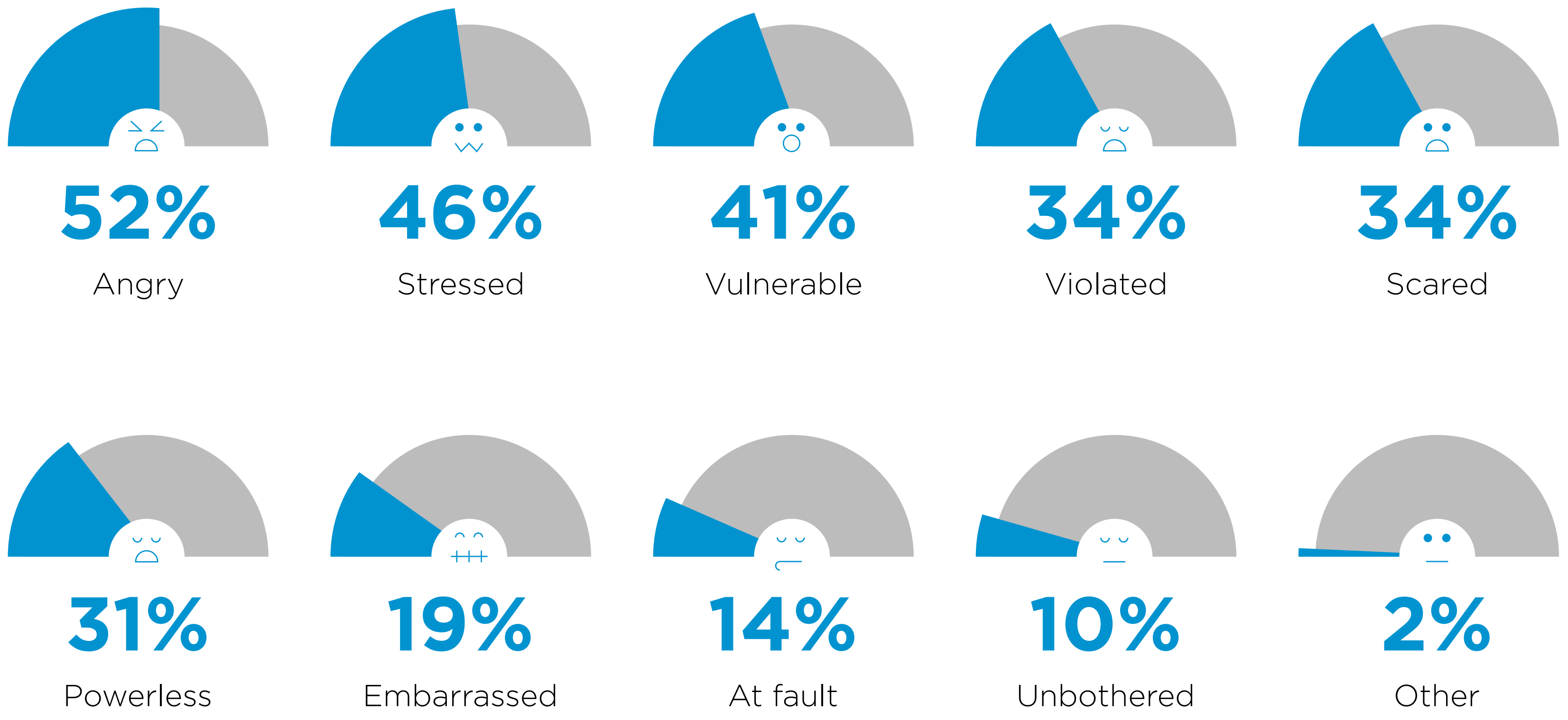
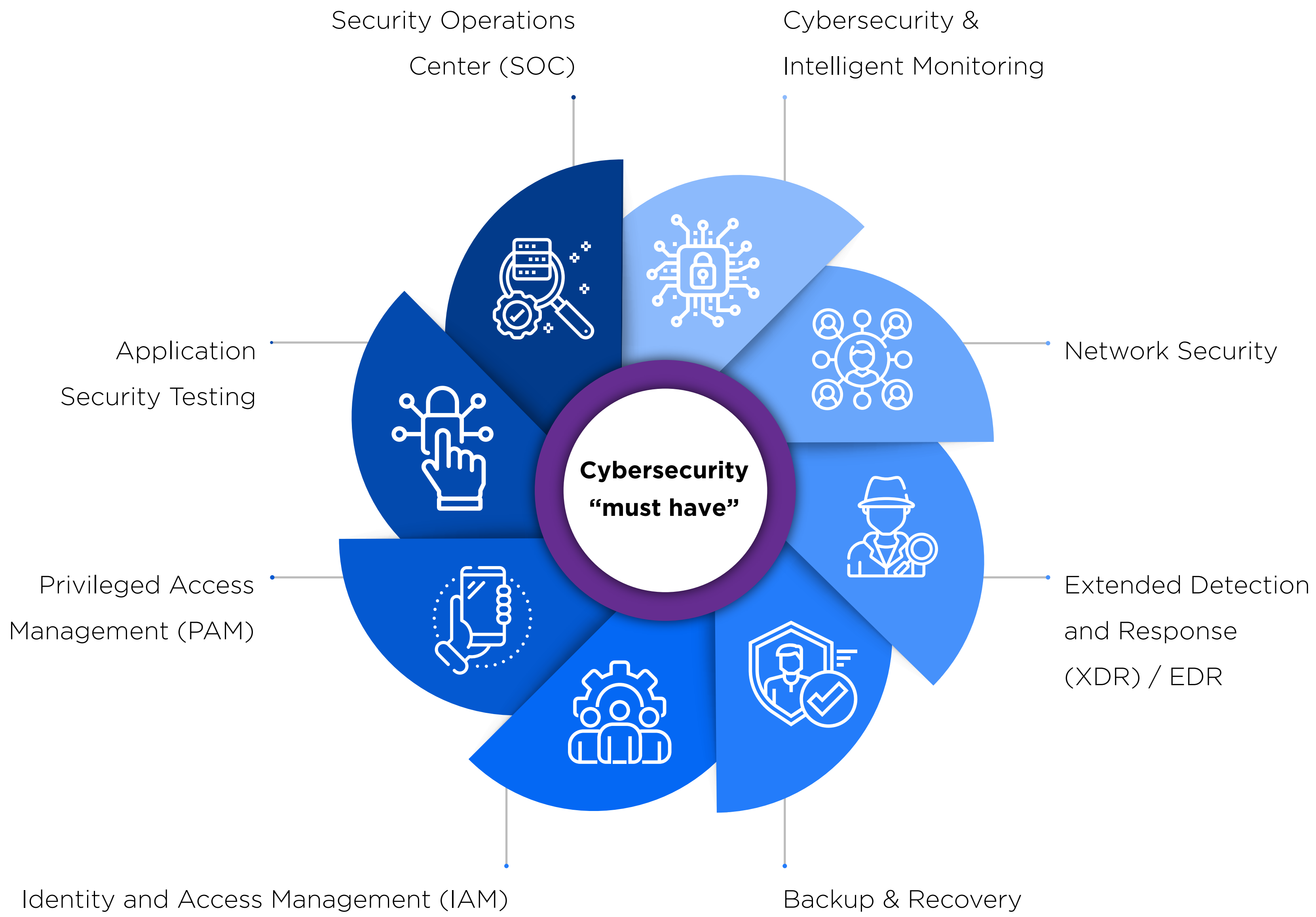


Figure 1 | Emotions Experienced by IT responsibles After Detecting Unauthorized Access to Accounts or Devices.

Source: “2021 Norton Cyber Safety Insights Report: Global Results”

Security by design



Security Operations Center (SOC)
Cybersecurity & Intelligent Monitoring
Application Security Testing
Network Security
Cybersecurity "must have"
Privileged Access Management (PAM)
Extended Detection and Response (XDR) / EDR
Identity and Access Management (IAM)
Backup & Recovery

Key priority areas

Intelligent Threat Detection and Response

- Self-learning AI swiftly stops cyber-attacks, including ransomware and phishing
- Detects, investigates, and responds to emerging threats instantly
- Safeguards cloud environments from unprecedented cyber threats

Key technologies

DARKTRACE

Network Security / Zero Trust

- Securing all physical and logical devices
- Applying Zero Trust principles
- Essential for countering network threats like worms, viruses, and hackers

Key technologies

paloalto NETWORKS zscaler FORTINET
netskope HPE aruba networking

Extended Detection and Response (XDR)

- It detects and responds to threats across endpoints, networks, and applications
- Unifies data from multiple security tools
- It improves visibility and simplifies threat management

Key technologies

paloalto NETWORKS CROWDSTRIKE
Microsoft MORPHISEC

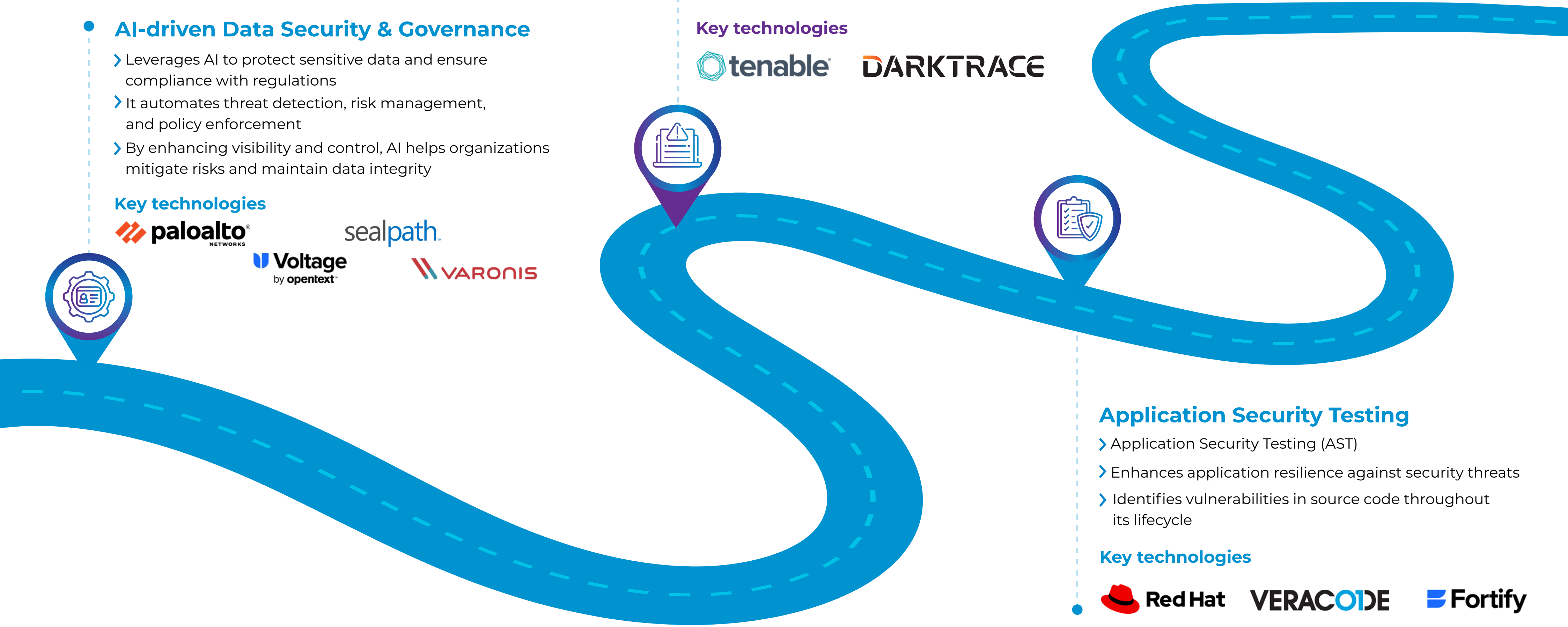
Identity Management

- Identity management ensures the right people access the right resources
- It verifies user identities and controls permissions
- Cover service, app, root, and priviledge accounts across the organization

Key technologies

okta Omada IBM
Microsoft Delinea

Key priority areas



AI-driven Data Security & Governance

- Leverages AI to protect sensitive data and ensure compliance with regulations
- It automates threat detection, risk management, and policy enforcement
- By enhancing visibility and control, AI helps organizations mitigate risks and maintain data integrity

Key technologies

paloalto NETWORKS · sealpath · Voltage by opentext · VARONIS

Vulnerability Management / Penetration Test

- It identifies and assesses security weaknesses
- It prioritizes risks and applies fixes to reduce exposure
- Mitigate inappropriate and risky access

Key technologies

tenable · DARKTRACE

Application Security Testing

- Application Security Testing (AST)
- Enhances application resilience against security threats
- Identifies vulnerabilities in source code throughout its lifecycle

Key technologies

Red Hat · VERACODE · Fortify

Key priority areas

Security Operations Center (SOC)

- SOC covers prevention, detection, investigation, and response to threats
- It offers continuous 24/7 monitoring for cyber threats
- The SOC ensures continuous protection and minimizes risks

Key technologies

securonix Microsoft

FORTINET ArcSight

Time to define Your roadmap

Starting this cybersecurity roadmap may seem challenging, especially when doing it alone.

Make sure you get proper guidance and counseling to guarantee you start off on the right foot and scale in the right way.

Our expertise tells us that many companies are reacting ad-hoc and end up investing in a distributed way, solving specific needs but do not guarantee real-time holistic protection of organizations' data, email, applications, assets, and networks, from sophisticated attacks.

Would you like to know what's the right move for your business?

Pro Tip

Do not rush, plan and prioritize security investments!

Contact us and we'll guide you throught this journey

Free Content

Government institution reduces threat analysis time by 92%!

Secure and control all privileged accounts across your enterprise

noesis

an Altia Company

www.noesis-corporation.com