noesis
an Altia Company

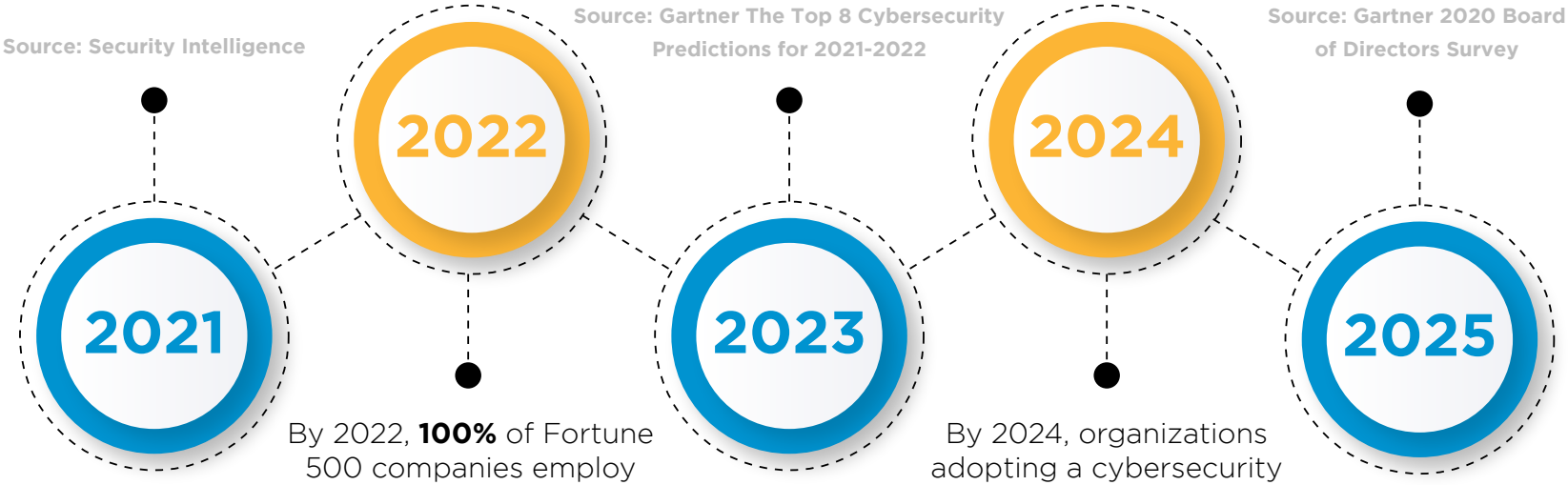
TOP 8 CYBERSECURITY CAPABILITIES FOR IT LEADERS

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

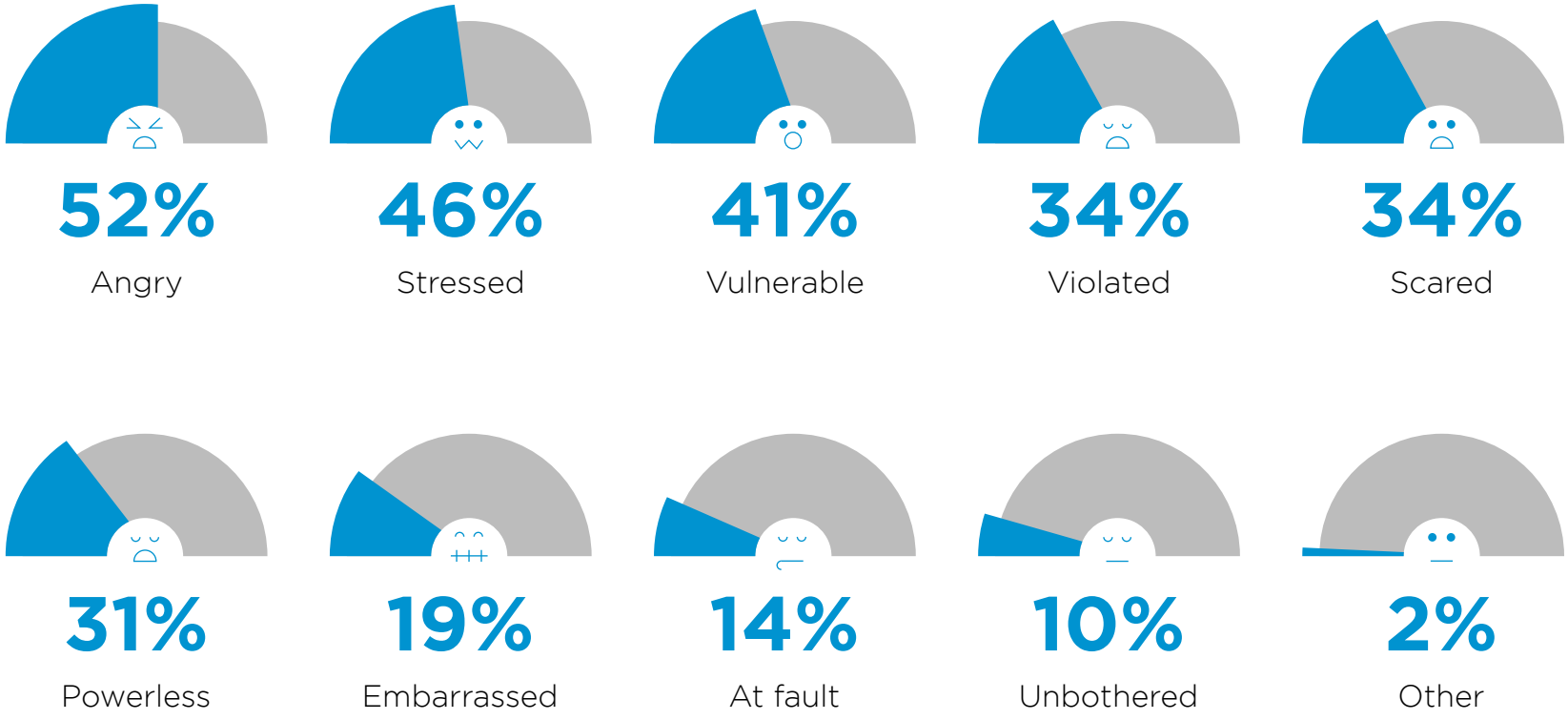
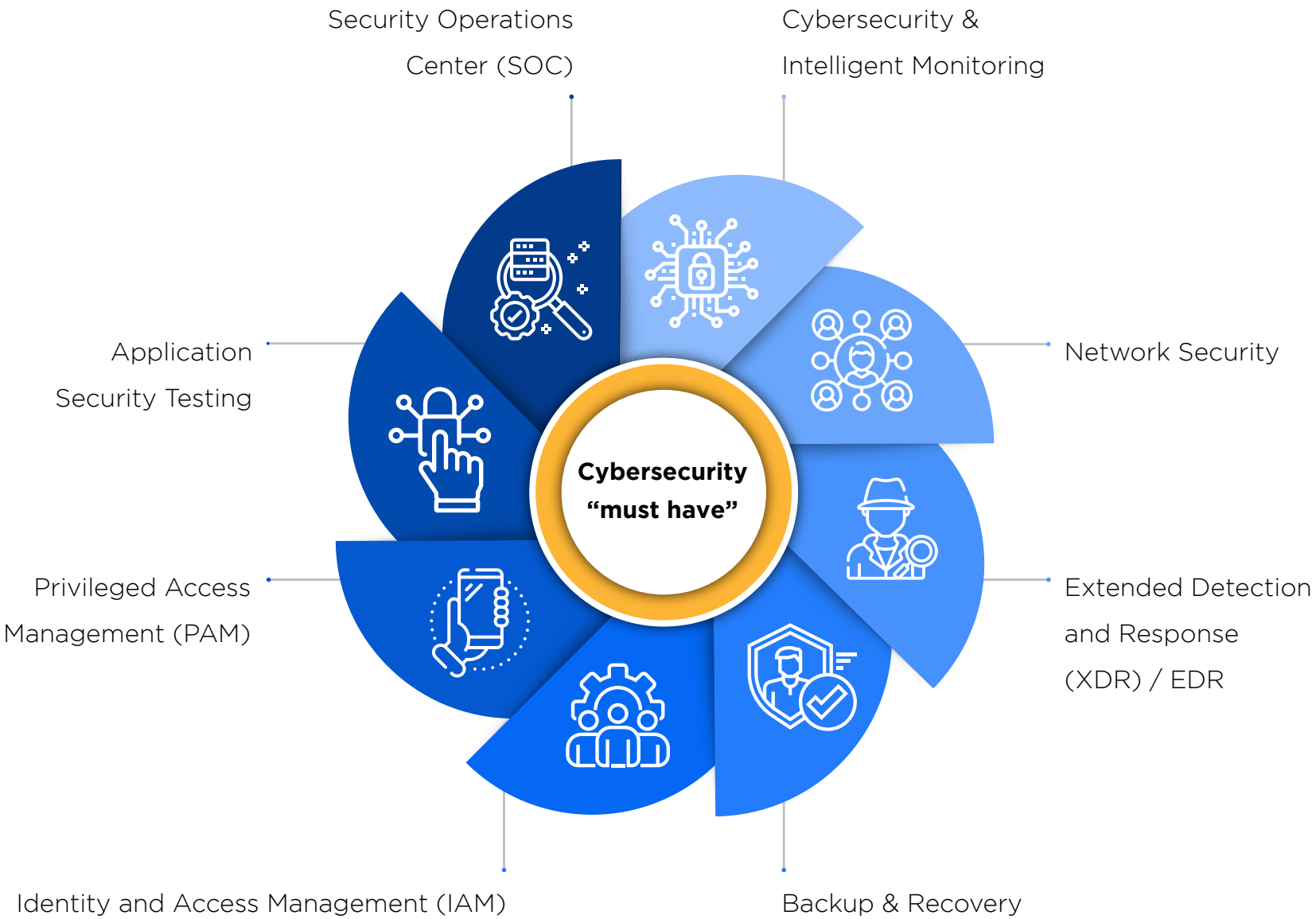


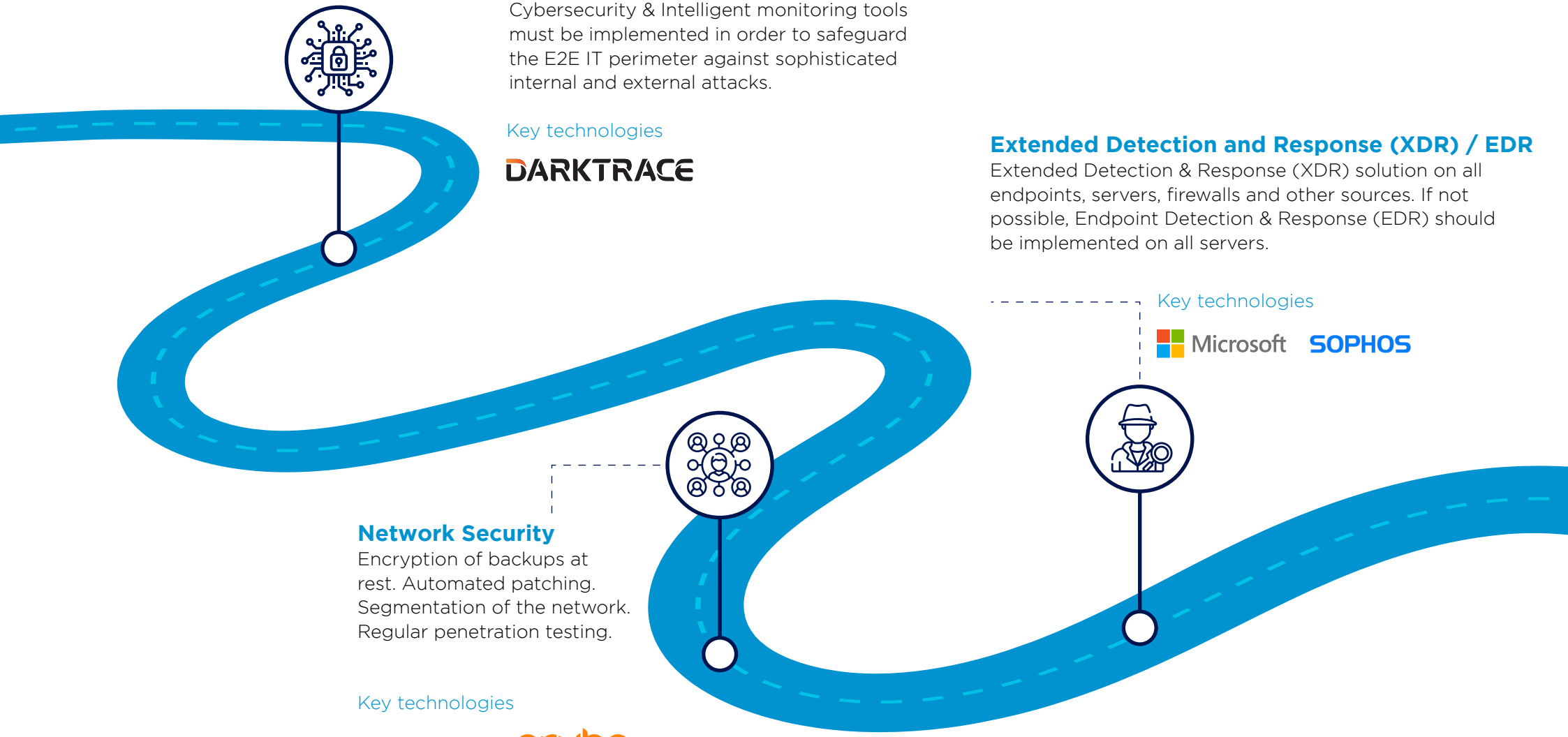
Figure 1 | Emotions Experienced by IT responsibles After Detecting Unauthorized Access to Accounts or Devices.

Source: "2021 Norton Cyber Safety Insights Report: Global Results"

Security by design



Key priority areas



Cybersecurity & Intelligent Monitoring

Cybersecurity & Intelligent monitoring tools must be implemented in order to safeguard the E2E IT perimeter against sophisticated internal and external attacks.

Key technologies

DARKTRACE

Extended Detection and Response (XDR) / EDR

Extended Detection & Response (XDR) solution on all endpoints, servers, firewalls and other sources. If not possible, Endpoint Detection & Response (EDR) should be implemented on all servers.

Key technologies

Microsoft SOPHOS

Network Security

Encryption of backups at rest. Automated patching. Segmentation of the network. Regular penetration testing.

Key technologies

paloalto NETWORKS

aruba
a Hewlett Packard Enterprise company

Key priority areas

Backup & Recovery

Backups are stored off-site and offline, completely separated from your production environment.

Key technologies

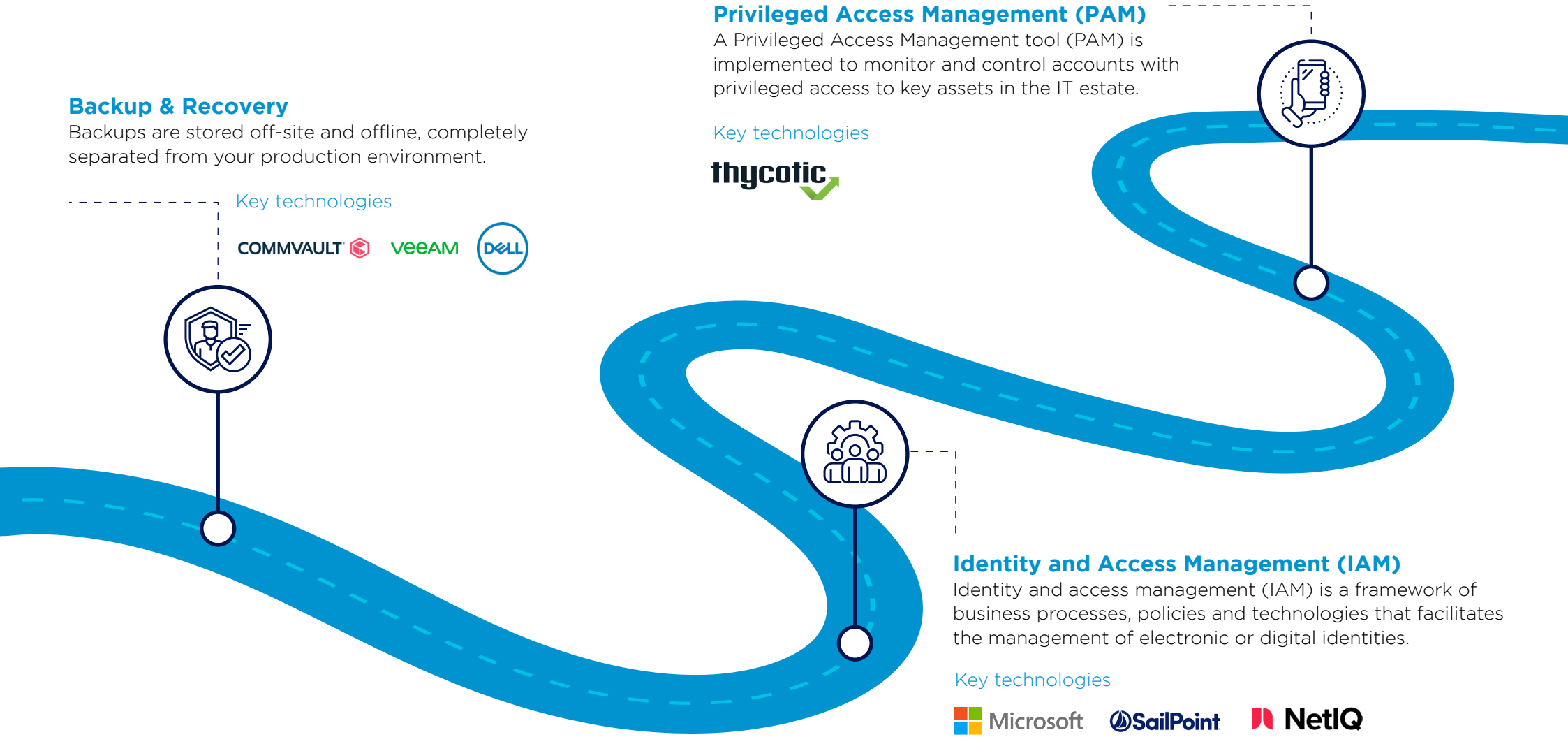
COMMVAULT VEEAM DELL

Privileged Access Management (PAM)

A Privileged Access Management tool (PAM) is implemented to monitor and control accounts with privileged access to key assets in the IT estate.

Key technologies

thycotic



Identity and Access Management (IAM)

Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities.

Key technologies

Microsoft SailPoint NetIQ

Key priority areas

Application Security Testing

Build on demand software resilience for modern development from an AppSec tool that delivers a holistic, inclusive, and extensible platform that supports the breadth of software portfolio.

Key technologies

Fortify

Security Operations Center (SOC)

Vulnerability scans to all websites and external facing points. Tool for log review (SIEM). Log sources must include firewall, AD, EDR, Domain Controllers and others critical resources.

Key technologies

SECURONIX Security Analytics. Delivered. Microsoft RAPID7 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?

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

Pro Tip

Do not rush, plan and prioritize security investments!