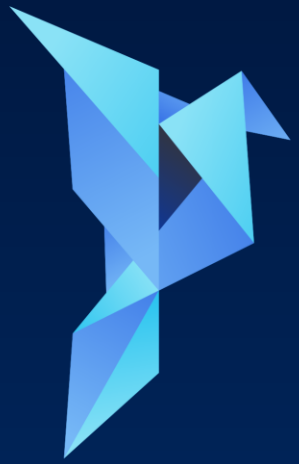


PACIFICA

A NOVENTIQ Company

Endpoints as prime targets for cyberattacks

Alan IBRAGIMOV – Cybersecurity Engineer

WHAT IS AN ENDPOINT?

CORPORATE LAPTOPS

MOBILE DEVICES

VIRTUAL SERVERS

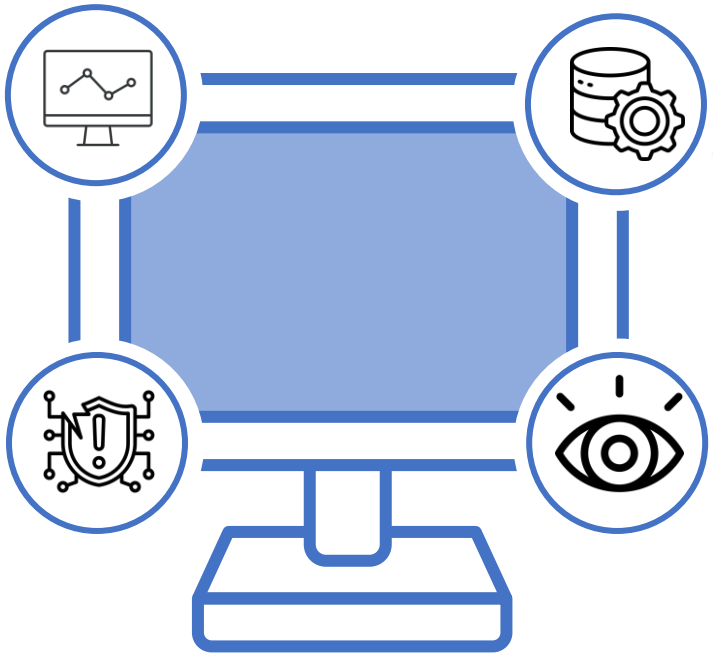
ENDPOINT AS PRIME TARGET FOR CYBERATTACK

Attack scale

- One compromised endpoint – access to the entire network
- Movement and spread of the attack across internal systems from an infected device

Weak protection and control

- Work outside of corporate perimeter (remotely, on business trips)
- Untimely updates and patches
- Lack of monitoring and centralized management



Unrestricted access to data

- Storing local copies of documents and emails
- Access to corporate services and databases
- Possibility of theft of credentials and access keys

Poor employee awareness

- Lack of basic cyber hygiene knowledge
- Inability to understand, which emails is phishing or not
- Ignoring of security alerts

PACIFICA
A NOVENTIQ Company

The most common endpoint threats

Phishing and vishing

E-mail

Phone calls

Malware

Viruses

Trojans

Keyloggers

Zero-day attacks

Malicious software not presented in signature databases

Ransomware

Encrypting ransomware

Locker ransomware

External devices

Infected USB-devices

External disks

PACIFICA
A NOVENTIQ Company

2021-2024 Statistics

Growth of cyber threats

- Enterprise endpoint attacks have **68%increase** from **2021 to 2024** (Verizon DBIR 2024)
- **80%**of successful attacks starts with **an endpoint compromise** (IBM 2024)

Record losses from incidents

- **The average** global cost of an incident at a large company – **$4,88 millions** (IBM Cost of a Data Breach 2024)
- Ransomware recovery costs an average **$2,73 millions** (Sophos 2024)
- Companies with remote workers **lose 20%**more from endpoint attacks(IBM 2024)

Evolution of the attackers

- Average time until Lateral Movement – **62 minutes** (CrowdStrike 2024)
- **Zero-day** attacks have **increased** by **50%**over the past two years (Mandiant 2024)

PACIFICA
A NOVENTIQ Company

HOW TO PROTECT YOUR ORGANIZATION?

TECHNICAL PROTECTION

- Using of antivirus systems to provide basic protection
- Implementation of EDR to collect telemetry and respond to complex threats
- Disks and data encryption
- Protection of mobile devices and data stored on them

ORGANIZATIONAL MEASURES

- Security policies for working both in the office and remotely
- Access rights restrictions based on the principle of "least privilege"
- Continuous monitoring of all endpoints and IT infrastructure components, such as laptops, mobile phones, servers and other devices
- Regular penetration testing and security audits

EMPLOYEE TRAINING AND AWARENESS

- Trainings of recognizing phishing and social engineering
- Phishing attack simulations
- Instructions for actions in case of suspected incidents

PACIFICA
A NOVENTIQ Company

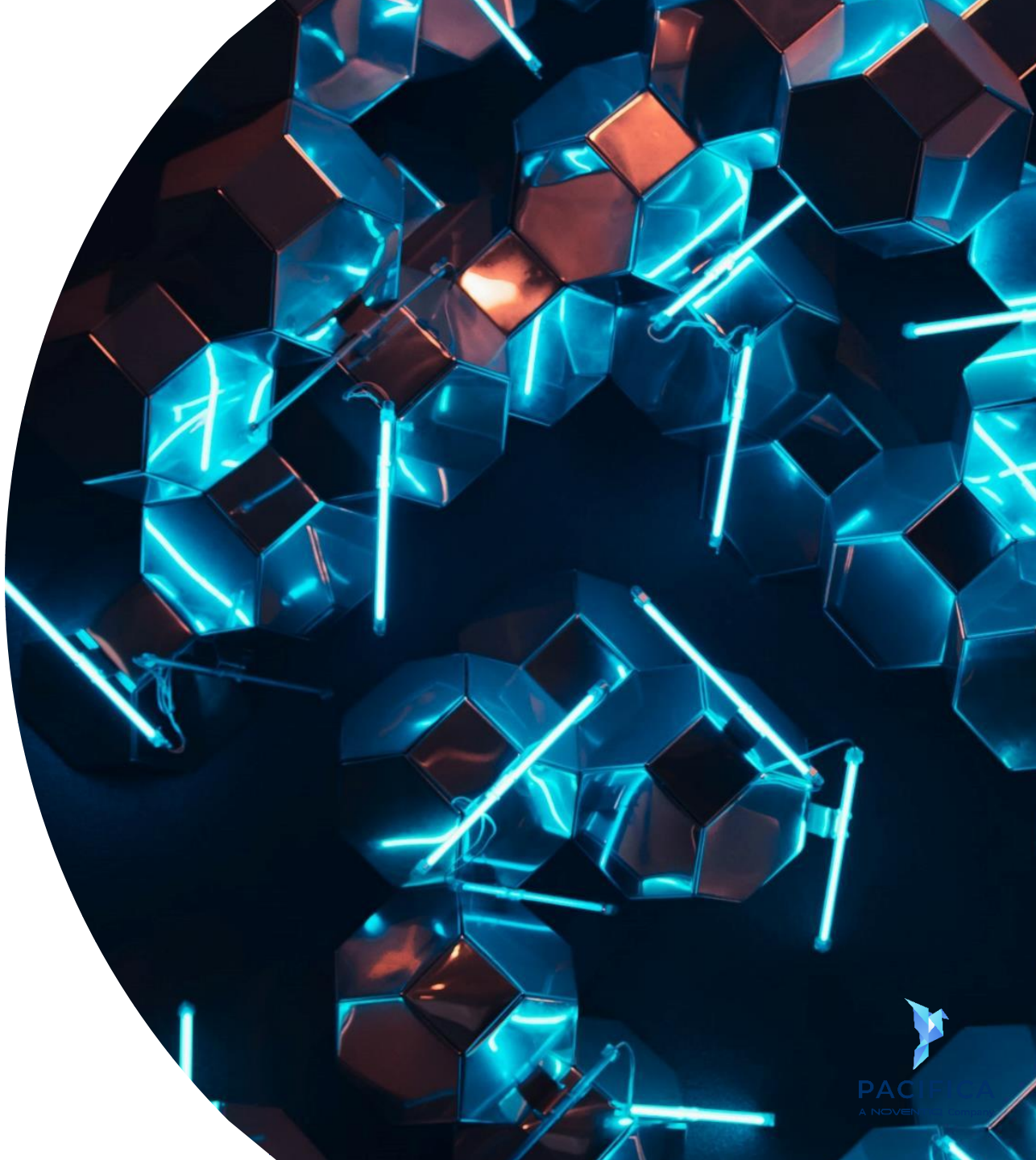
Antivirus – basic protection for endpoints

- **Detection** and **blocking** of known threats
- **Signature analysis** for viruses, trojans and spyware
- **Web and email protection:** filtering of malicious websites, attachments and URL's
- **Ransomware protection** – monitoring file changes and blocking encryption attepmts
- Automatic **signature updates**

PACIFICA
A NOVENTIQ Company

Endpoint Detection and Response (EDR)

- **Continuous monitoring of endpoints.** 24/7 telemetry collection and activity analysis on devices.
- **Detection of complex and previously unknown threats.** Behavioral analysis, search for IOCs (Indicators of Compromise), detection and prevention of zero-day attacks
- **Automatic and manual incident response.** Ability to isolate infected devices from the network, remotely eliminate threats and collect artifacts for further forensic analysis.
- **Attack recognition and analysis.** Building a detailed of events, forecasting potential incidents and gathering intelligence to strengthen protection



AV + EDR = Comprehensive Protection

Detection of known threats

Scanning and filtering

Signatures and heuristics

Detection of zero-day attacks

Instant response

Investigation and forensics

PACIFICA
A NOVENTIQ Company

XDR – Extended Detection and Response

Endpoints

Network

Mail

Cloud

Identity protection

Vulnerability management

- Unified view of the entire infrastructure
- Detection of attacks across the network and endpoints
- Complete event investigation

PACIFICA
A NOVENTIQ Company

Attack Chain and XDR Response

Connecting to an unsecured network

Attempt to access corporate email

Suspicious cloud access attempt

PACIFICA
A NOVENTIQ Company

Attack Chain and XDR Response

Endpoint compromise

Attempt to gain a foothold in the system

Use of credentials to access the cloud from the different country

Endpoint isolation

Blocking of compromised account

Attack was stopped before the attacker gains a foothold in the network

PACIFICA
A NOVENTIQ Company

MDM – Management and Protection of Mobile Devices

Mobile Device Management – centralized management of mobile devices with access control, security policies and compliance enforcement

Key Capabilities

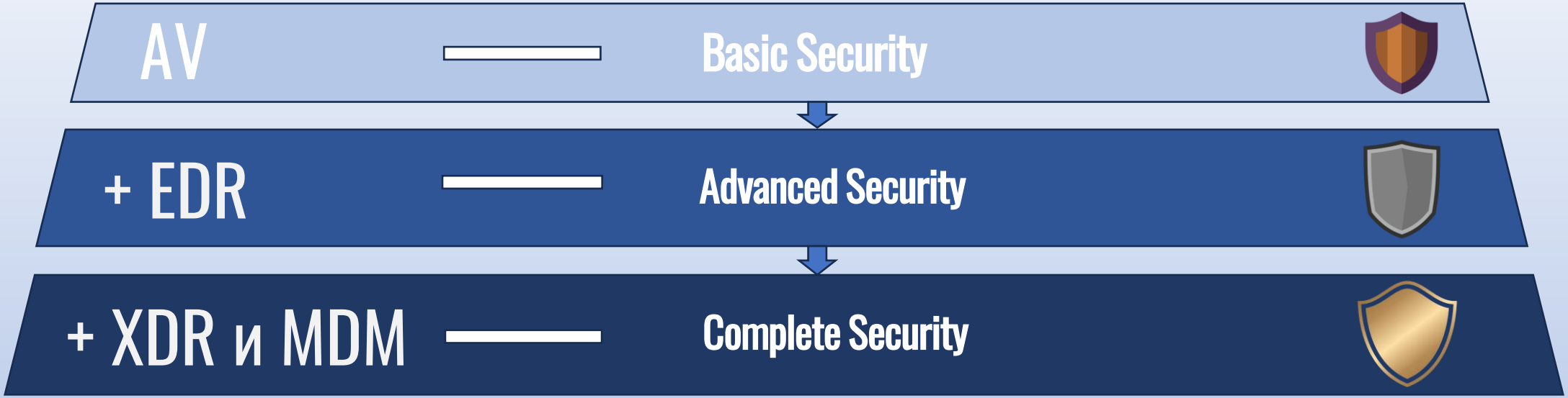
- Centralized management
- Data protection
- Access control
- Ensuring device compliance status

Why It's Needed

- Reducing the risk of data leaks when working outside the office
- Supporting secure BYOD (Bring Your Own Device) and remote work
- Rapid response to incidents involving mobile devices

PACIFICA
A NOVENTIQ Company

IGNORE SECURITY TODAY – PAY FOR IT TOMORROW



WHAT WE LEARNED TODAY?

- **Endpoints** are the main attack vector
- **Threats are growing**, attacks are becoming more **complex**, and the **cost** of incidents **is increasing**
- **Multi-level protection** significantly reduces risk and incident cost
- **Investing in security** always cheaper than **dealing with the consequences**

PACIFICA
A NOVENTIQ Company

PACIFICA
A NOVENTIQ Company

Thank you for your attention!

Almaty, Dostyk Avenue 210, «Koktem Grand» Business Center

phone: +7 (777) 812-03-31

e-mail: ai@pacifica.kz

www.pacifica.kz

PACIFICA – Peace of mind for your business


PACIFICA
A NOVENTIQ Company