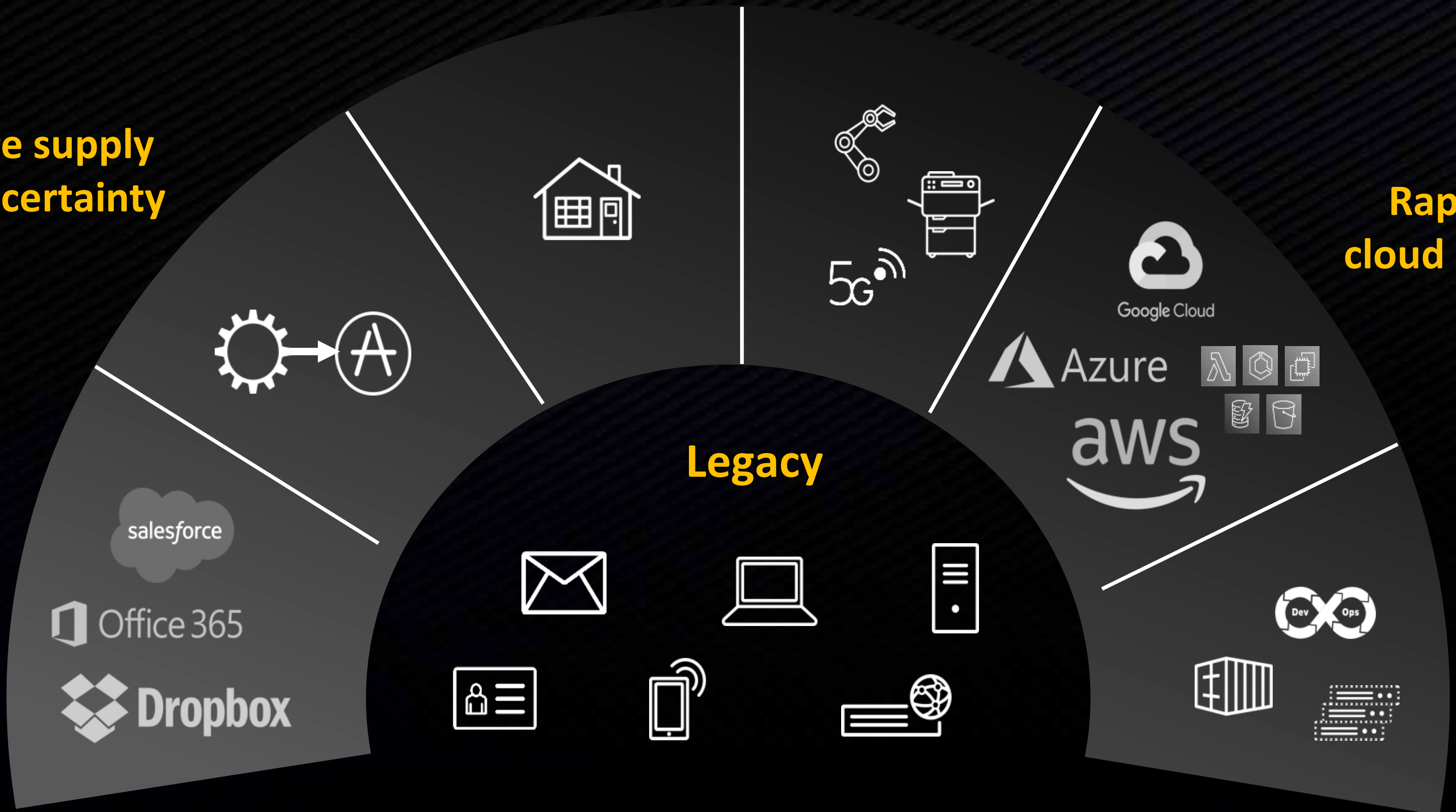
Trend Vision One ENDPOINT SECURITY

Garaj

Cloud Platform by Jazz

RISING IT INFRASTRUCTURE COMPLEXITY



Massive growth in SaaS applications

Software supply chain uncertainty

Work-from-home

IT / OT convergence & 5G

Rapid growth in cloud native services

Cloud native applications

Legacy

CYBERSECURITY BREACHES

Top 3 Industries and Segments

By detected ransomware attacks

9,034
Banking

5,073
Retail

2,6540
Transportation

- Industry
- Business segments

66,390
Enterprise

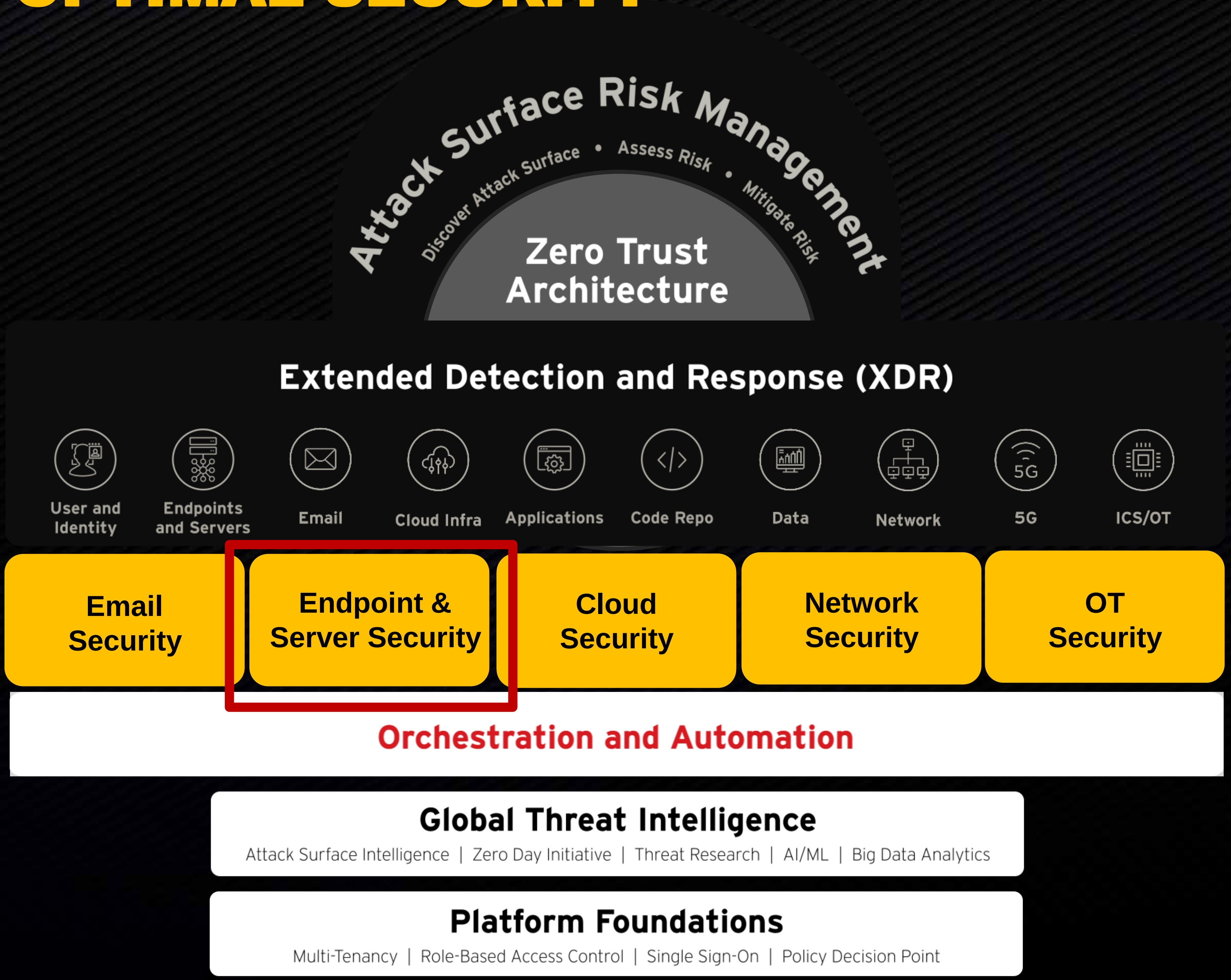
13,074
Consumer

8,379
SMBs

OFFERING OPTIMAL SECURITY

Garaj
Cloud Platform by Jazz

MANAGED SERVICES



Attack Surface Risk Management

Discover Attack Surface • Assess Risk • Mitigate Risk

Zero Trust Architecture

Extended Detection and Response (XDR)

User and Identity | Endpoints and Servers | Email | Cloud Infra | Applications | Code Repo | Data | Network | 5G | ICS/OT

Email Security | Endpoint & Server Security | Cloud Security | Network Security | OT Security

Orchestration and Automation

Global Threat Intelligence

Attack Surface Intelligence | Zero Day Initiative | Threat Research | AI/ML | Big Data Analytics

Platform Foundations

Multi-Tenancy | Role-Based Access Control | Single Sign-On | Policy Decision Point

ECOSYSTEM INTEGRATION

WHY ENDPOINT SECURITY?

Better Security Outcome

Superior prevention, detection & response for user endpoint, server, and cloud workload

Industry leading threat intelligence & timely vulnerabilities protection

Industry recognized leader

Less Complexity

Single pane of glass (inventory, detections, mitigation, policies)

Common RBAC, policy management, licensing & more across the platform

Connected IT/Security ops workflow

Accelerate your Technology consolidation journey

“75% of organizations are pursuing security technology consolidation” (Gartner)

Single platform - endpoint, email, network, cloud, OT

MDR service to extend your security team

COMPREHENSIVE THREAT PROTECTION

From layered protection to detection and response.

Prevention

- Virtual Patching - IPS
- Device Control
- Firewall
- App. Control
- Web Reputation

Real Time Detection

- Machine Learning
- Behavioural Analysis
- Malicious CLI
- Network Fingerprinting
- Antimalware & Known Threats

Automated Response

- Kill & Quarantine Process
- Restore Encrypted Files
- Suspicious object/ Intelligence sharing
- Quarantine Files

Investigation and Response

- Cross layered detection
- IOC (Indicator of Compromise) Sweeping
- MITRE Mapping
- Threat Intelligence
- Managed XDR*

BUILT & OPTIMIZED FOR SERVERS AND CLOUD WORKLOADS

Satisfying the unique needs of servers, cloud workloads, and runtime containers security, unlike other vendors using user endpoint capabilities for servers & workloads.

Network Security

- Intrusion Prevention
- Firewall
- Vulnerability Scanning

System Security

- Application Control
- Integrity Monitoring
- Log Inspection

Malware Prevention

- Anti-Malware
- Behavioral Analysis
- Machine Learning

Detection & Response (activity monitoring)

- Detect
- Respond
- Investigate

WHY XDR ON ENDPOINTS?

Most attacks interact with corporate endpoints during the breach lifecycle

Detect: Security analytics finds threats hidden amongst endpoint telemetry. IOC sweeping

Investigate: What happened within the endpoint? How did it propagate? What tactics/techniques are used

Respond Examples: Isolate, stop process, delete/ restore files

Going further with other XDR layers:

- Where did the threat originate?
- Where else is this threat in my network, workloads, email?

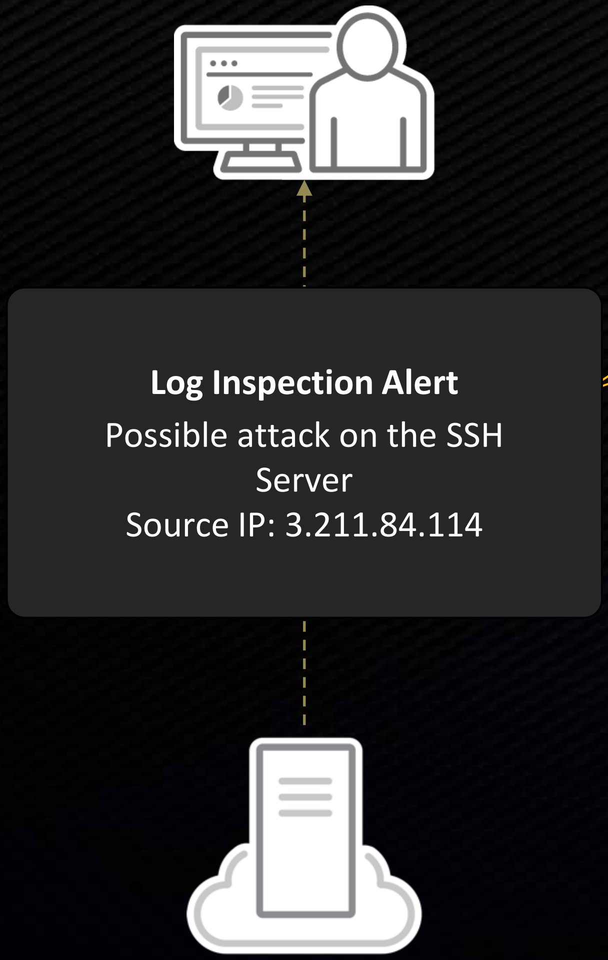
PROTECTING EXPLOIT OF OS & APP VULNERABILITIES

Shield from vulnerabilities until vendor patch is available.

Automatically shield newly discovered vulnerabilities within hours of their discovery.

Virtual Patch (IPS)

XDR FOR SERVERS AND CLOUD WORKLOADS



Log Inspection Alert

Possible attack on the SSH Server

Source IP: 3.211.84.114

Alerts don’t tell whole story

This is likely one step of many…

What’s the bigger picture?

Was the attacker successful?

Activity Data:

- User Account Activity
- Processes
- Executed Commands
- Network Connections
- Files Created/Accessed
- Registry Modifications

Detect: High-fidelity detections correlated from different security controls and activities to tell a whole story. IOC sweeping

Investigate: Full visibility of activities help answer; What happened within the workload? How did it propagate?

XDR BRINGS TANGIBLE RESULTS

Better Protection

Suffered **half as many successful attacks** over the last 12 months

Detecting Quicker

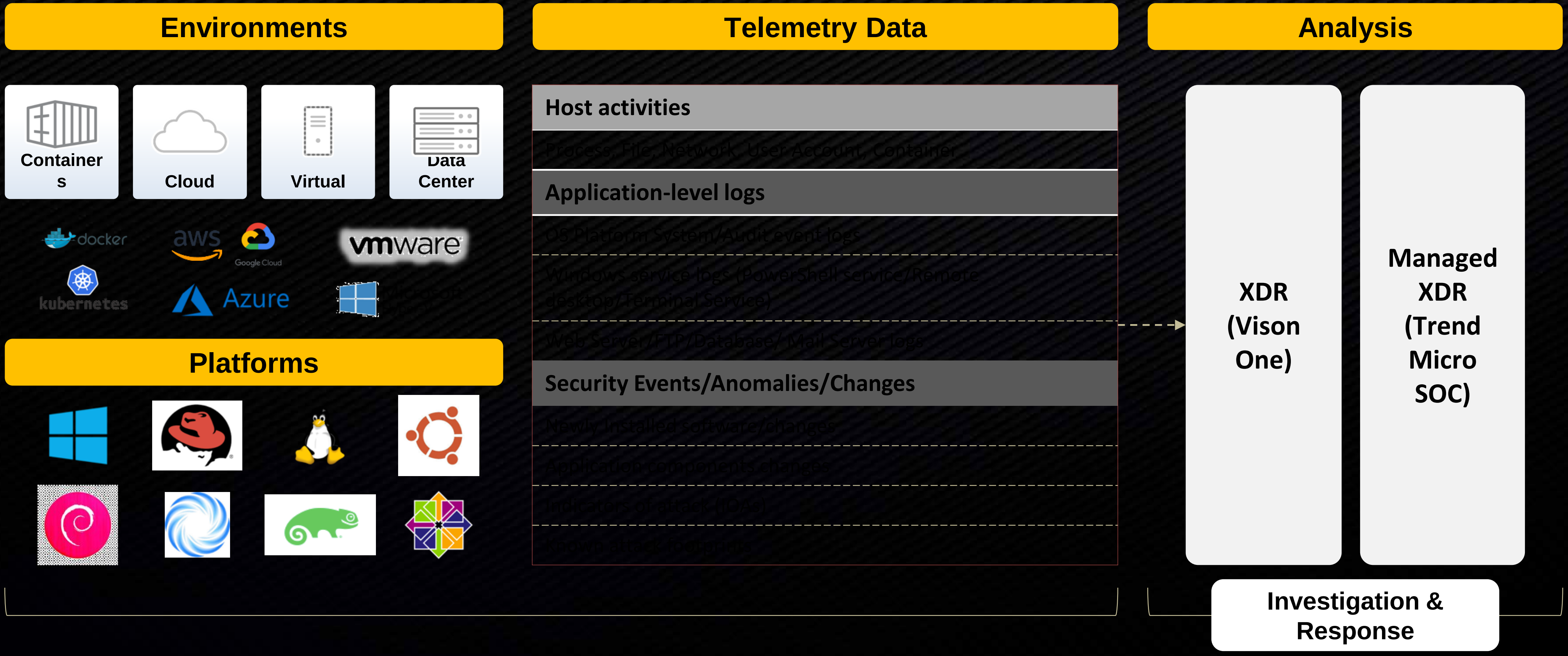
2.2X more likely to detect a data breach or successful attack in a **few days or less**

Responding Completely

60% less likely to report **attack re-propagation**

BROADER DETECTION FOR WORKLOADS

Garaj
Cloud Platform by Jazz



Environments

Container
s

Cloud

Virtual

Data
Center

Platforms

Telemetry Data

Host activities

Process, File, Network, User Account, Container

Application-level logs

OS Platform System/Audit event logs

Windows service logs (PowerShell service/Remote desktop/Terminal Service)

Web Server/FTP/Database/ Mail Server logs

Security Events/Anomalies/Changes

Newly Installed software/changes

Application components changes

Indicators of attack (IOAs)

Known attack footprints

Analysis

XDR
(Vison
One)

Managed
XDR
(Trend
Micro
SOC)

Investigation &
Response

ONE PLATFORM ONE CONSOLE

ENDPOINT SECURITY

Laptop

Desktop

Server

Virtual Server

Public/Private Cloud

WHAT IS IT?

Single pane of glass (inventory, detections, mitigation actions, manage policies)

Common Role-based access control, policy management, licensing & more

Connected workflows & automation

ONE PLATFORM ONE CONSOLE

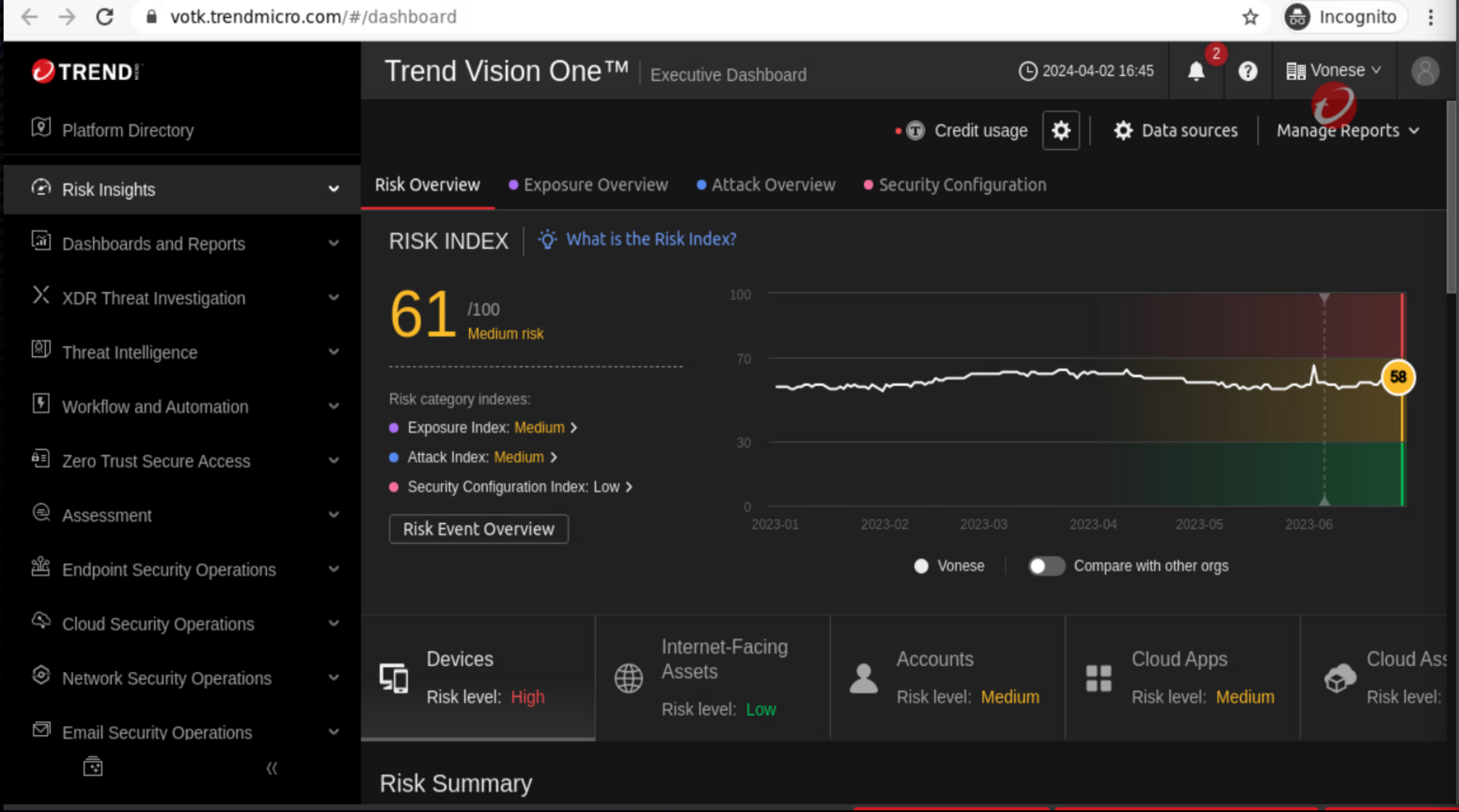
ENDPOINT SECURITY

- Laptop
- Desktop
- Server
- Virtual Server
- Public/Private Cloud

BENEFITS

- Central visibility, response, and management
- Reduce complexity; Increase efficiency
- Streamline your IT & Security Operations workflow

Trend Micro Vision One Console



Trend Vision One

1. Trend Vision One Introduction
2. Attack Surface Risk Management
3. XDR Threat Investigation
4. Free Assessment Tools
5. Managed XDR
6. Need Help?
7. Conclusion

TRENDMICRO LANDSCAPE IN BREIF BY TREND MICRO

64% Internet of Things Reputation Service declined.

Trend Micro Blocks 161 billion Incidents in 2023

35% annual increase in threats blocked under Trend's File Reputation Service (FRS).

In 2023, threats blocked by email and web reputation dropped annually by 47% and 2%, respectively.

2% Threats blocked by Trend's Mobile Application Reputation Service.

TARGETED AUDIENCE

Who to Sell?

Financial Sector

- Sensitive Data Protection
- Prevention of Financial Data Loss
- Phishing and Social Engineering prevention
- Malware and Ransomware Preventions
- Vulnerabilities Patching

IT Sector | Startups

- Application security
- Database Security
- Remote access – Security

Health Sector

- **Medical Devices security**
- **Security for Healthcare Apps**
- Malware and Ransomware Preventions

Garaj Customers

- **Secure VDC**
- **Application control**
- **Managed Deployment and Support**

Garaj

Cloud Platform by Jazz

Technical Support

✉ cloud.support@jazz.com.pk

☎ 0304 1110365 (24/7 helpline)

Billing & Invoicing

✉ bizcloudbilling@jazz.com.pk

To Learn More

✉ garaj-cloud@jazz.com.pk

🌐 garajcloud.com