InTTrust

Microsoft Solutions Partner

Rising Stronger:

Cyber Resilience without Compromise

Christos Papanikolaou | Solutions Sales Manager

InTTrust in brief

Established in 2006

Over 200 employees, including more than 170 engineers (over 400 IT Vendor certifications)

30Mi€ annual revenue | 9Mi€ services revenue (2024 prelim)

Microsoft Partner of the Year 2018

Microsoft Solutions Partner for:

- **Modern Work**
- **Data & AI**
- **Cloud & Hybrid Infrastructure**
- **Digital & App Innovation**

InTTrust


IBM
Platinum Partner
DARKTRACE
PLATINUM PARTNER
Microsoft
Solutions Partner
FORTINET
ENGAGE
FORTINET ADVANCED PARTNER
Integrator, Cloud
Commvault
PREMIER
SOLUTION PROVIDER
Red Hat
Premier
Business Partner
vmware
PARTNER
ENTERPRISE
SOLUTION PROVIDER
veeAM
Value-Added
Reseller
Silver
aws
ZABBIX
CERTIFIED PARTNER
Orchestry
Partner
Google
DELL Technologies
GOLD PARTNER
ORACLE
Partner
Hewlett Packard
Enterprise
Namirial
Frameable
OBRELA
PCCW
ManageEngine

Portfolio of Services

Dynamic Infrastructure Services

- Infrastructure for Multi/Hybrid Cloud Datacenters
- Multi-cloud consultancy, implementation, admin, operation, support
- SAP Hana Infra
- Network
- IT & Cloud Security
- Middleware
- Application Servers

Application Development Services

- Microservices
- Containers
- Low-code apps
- Modern Workplace Apps
- Cloud-Native Apps
- Data Analytics
- ML/AI
- Industry 4.0
- Application Integration

Managed Services

- Managed Hybrid-Multi Cloud 24x7
- Infra Monitoring, Operation, Support 24x7
- NOC Services
- DR Services
- Backup Services

DBA Services

- DB Operations
- DB upgrades, configuration, migration, performance tuning
- DB Consulting
- Data Migrations
- Data Management

Digital Transformation

Shift to Cloud Economy (+12T$ by 2030)

New “acronyms”

- IaaS (Infrastructure as a Service)
- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- DaaS (Desktop as a Service)
- BaaS (Backup as a Service)
- etc

New Frontiers

- AI
- Quantum computing

Cyber Crime Transformation

3rd largest economy (10T$)

New “acronyms”

- CaaS (CyberCrime as a Service)
- RaaS (Ransomware as a Service)
- PhaaS (Phising as a Service)
- DDoSaaS (DDoS as a Service)
- BaaS (Botnets as a Service)

New Frontiers

- AI (Deepfakes, Prompt Injections, Voice spoofing)
- Quantum computing (Encryption break)

CaaS merchant offering example:

Distributed denial of service (DDoS) on **a subscription model**.

Outsources the creation and maintenance of the botnet necessary to carry out attacks

Each DDoS subscription **customer receives an encrypted service** to enhance operational security and **one year of 24/7 support.**

The DDoS subscription **service offers different architectures and attack methods**, so **a purchaser simply selects a resource to attack** and the seller provides access to an array of compromised devices on their botnet to conduct the attack.

Cost for the DDoS subscription is a mere **$500 USD**.

1hr 12m

The median time it takes for an attacker to access your private data if you fall victim to a phishing email.[16]

1hr 42m

The median time for an attacker to begin moving laterally within your corporate network once a device is compromised.[17]

Source: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-cyber-resilience

Democratization of Cyber Crime

SMEs are a particular weak link

- Lack of situational awareness (Biggest myth: “We are too small….”)
- Lack of specialized resources and investments/budgets in Cyber Security
- Often outdated and legacy infrastructure, applications and protocols
- Rise of supply chain attacks (SME as a gateway for the “big fish”)
- Low hanging fruit for attackers – easy to compromise
- Results can be devastating (SME may not be able to recover at all or extreme financial impact)

Customer Case: Greenfield approach for (Cloud based) Cyber Recovery

Challenge

Severe Cyber Security incident heavily impacting multiple areas of the company operations

Ability to rapidly recover operations in a secure manner

Increase Cyber Security resilience (after recovery)

Solution

Rapid migration to Azure Infrastructure to restore data and services in a “clean state” manner (Isolated Recovery Environment)

Some of the Azure Services used:

- **Platform setup** (Azure Landing Zone) implementation
- Windows, Linux, MySQL, SQL Server migration, to Azure IaaS / PaaS
- **IBM P-Series on Azure** via **Skytap Service** Microsoft Azure Marketplace - 1st Skytap implementation in Greece
- Azure **Databox** (100TB data)

CyberSecurity stack deployment**:**

- **Defender XDR** (M365 E5 Security services)
- **Defender for Cloud** (P2) / **Defender for Identity**
- **Darktrace** NDR
- **Sentinel** SIEM/SOAR

Impact

Restore company operations **within 20 days**

Increase Cyber Resilience via DarkTrace NDR + Defender XDR + Defender for Cloud

Introduce Sentinel for SIEM/SOAR operations combined with **Obrela MDR platform**

Customer Case: Cloud based Greenfield approach for Cyber Recovery

Lessons Learned

Cyber Resiliency shall not be an afterthought – it is a critical company capability

SMEs are not immune – they are an easy target. **It's a matter of WHEN not IF**

Move to the Cloud **BEFORE** the incident… not as a Recovery method

Proactive & Holistic Threat Protection & BC/DR strategy powered by the Cloud

Immutable or even air gapped backups are of extreme importance
(if you need all your data….)

Leverage the power and economies of Cloud Computing to rise stronger
No compromises for your Cyber Resilience

InTTrust

Your InTrusted Partner for

- Transformation
- Growth
- Excellence

Thank you !!

EURO CERT CERTIFIED MANAGEMENT SYSTEM EN ISO 22301:2019 00.24.0198

CERT CERTIFIED QMS ISO 9001 QMSCERT Cert. No. 290113/3779

CERT CERTIFIED ISMS ISO 27001 QMSCERT Cert. No. 270218-3