

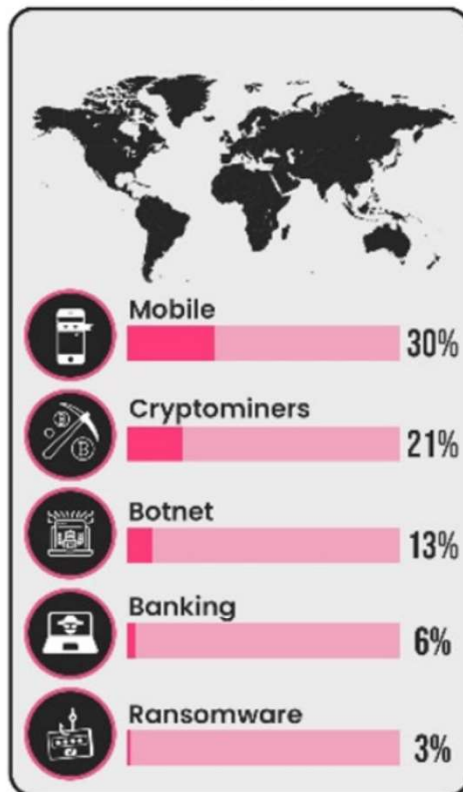


Sharing Implementasi Cyber Security di Perguruan Tinggi

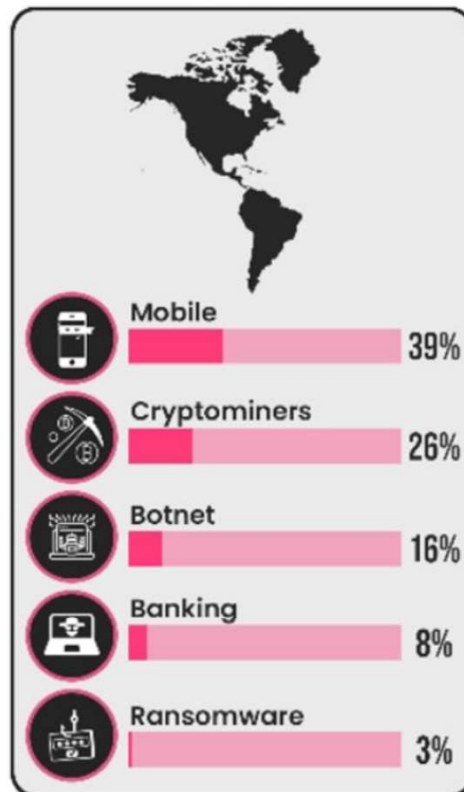
INSTITUT TEKNOLOGI BANDUNG

CYBER ATTACK CATEGORIES BY REGION

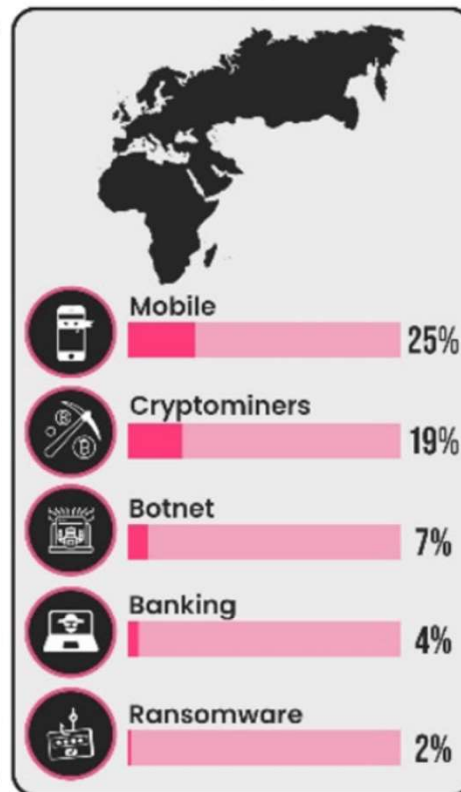
GLOBAL



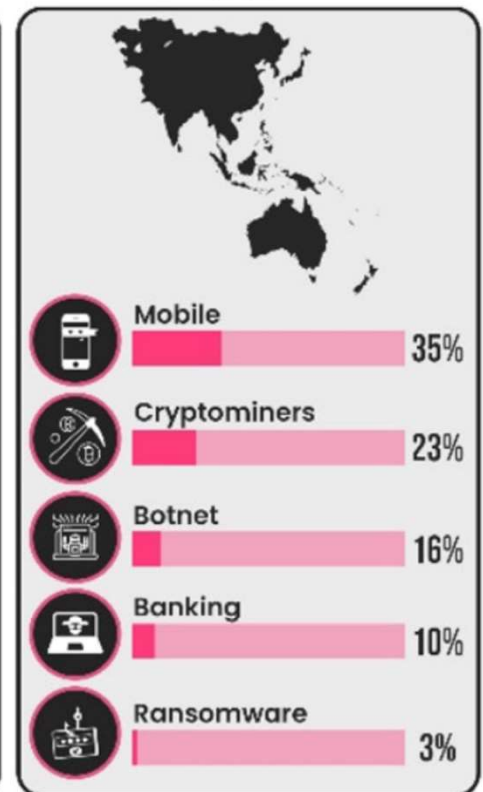
AMERICAS



EMEA











APAC



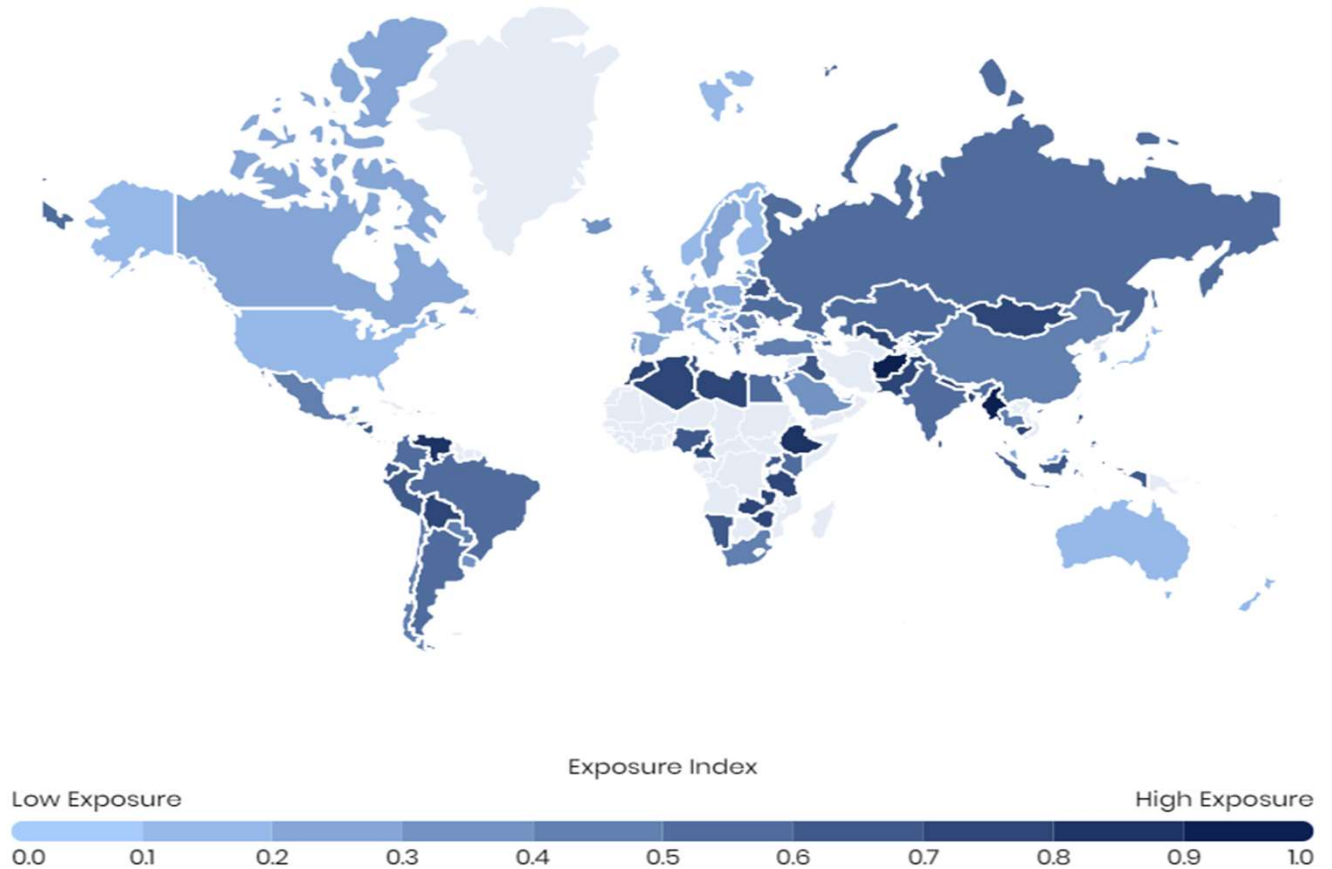
Global Cybersecurity Exposure Index 2020

From 0 to 1, the Cybersecurity Exposure Index (CEI) calculates the level of exposure to cybercrime by country. The higher the score, the higher the exposure.

Search

Country	Rank	Score
 Finland	1	0.110
 Denmark	2	0.117
 Luxembourg	3	0.124
 Australia	4	0.131
 Estonia	5	0.134
 Norway	5	0.134
 Japan	6	0.138
 United States	7	0.145
 Austria	8	0.162
 Switzerland	9	0.172

Share



made with 

FAKTA DAN DATA TENTANG CYBERSECURITY

5 NEED-TO-KNOW CYBERSECURITY STATS

The **threat landscape** is always evolving. Are you prepared to defend against **advanced attacks**?

2 IN 3 small & mid-sized organizations go **out of business** within 6 months of a cyber attack



of breaches start with an **email**



4000 RANSOMWARE ATTACKS occur on average every day



Security breaches have **increased** by 67% in the last 5 years.

Traditional anti-virus solutions are only 43% effective against today's **advanced threats**.



Contact us today. Sleep soundly tonight.

Infogressive
Cybersecurity Solved.

INTERESTING CYBER-SECURITY FACTS

By 2021, cybercrime damages will cost the world about **\$6 trillion** annually.

Small businesses are the targets for **43%** of all cyber-attacks.

A hacking takes place every **39 seconds** across the globe.



By 2021, unfulfilled cyber-security jobs all over the world will number **3.5 million**

only **38%** of organizations worldwide claim to be prepared to handle a sophisticated cyber-attack.



By 2021, cyber-crime is expected to be more than triple the number of unfulfilled cyber-security jobs.

By 2020, there will be **200 billion** connected devices, resulting in higher risk of cyber-attacks.



By 2022, the human attack surface is expected to reach **6 billion** people.

TRAINING DOYENS
accelerating HR Training

26468 E Walker Dr, Aurora, Colorado 80016-6104

Email: support@trainingdoyens.com | Toll Free: 1-888-300-8494 | Tel: +1-720-996-1616 | Fax: +1-888-909-1882

The Top 5 Cybersecurity Threats Facing Small Businesses in 2022

FUSION
MANAGED IT

The most dangerous threats to your business in 2022, based on potential data loss, downtime, and cost.



RANSOMWARE ATTACKS

- In 2021, 37% of all organizations were hit by ransomware
- A ransomware attack cost an average of \$1.85 million in 2021*



MOBILE SECURITY FLAWS

- At least 40% of mobile devices are vulnerable to cyberattacks
- 46% of organizations have had at least one employee download a malicious mobile application*



CLOUD VULNERABILITIES

- About 90% of data breaches target external cloud assets (servers)
- 30% of all businesses fail to apply adequate cloud security controls*



IoT WEAKNESSES

- 48% of businesses admit they are unable to detect IoT security breaches on their network*
- More than half of all IoT devices are vulnerable to medium or high-severity attacks*



INDUSTRY-TARGETED ATTACKS

- Cybercrime across all industries is up 600% due to the COVID-19 pandemic*
- The most targeted sectors worldwide by hackers in 2021 are healthcare, education/research, ISP/MSP, communications, and government/military*

Keep Your Business Protected

Protect your business against the latest threats with the help of our experts at Fusion Managed IT. We provide comprehensive cybersecurity solutions with best-in-class support to prevent attacks against your network and devices. Contact us today to learn how we can help your business stay protected.

Sources

- Cloudwards, "Ransomware Statistics, Trends and Facts for 2022 and Beyond"
- Checkpoint Mobile Security Report 2021
- Verizon 2021 Data Breach Investigations Report (DBIR)
- Cyber Talk, "Key cloud security statistics that will reshape your cloud perspectives"
- Gemalto, State of IoT Security (2019)
- 2020 Unit 42 IoT Threat Report
- PurpleSec, "2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends"
- Cyber Security Intelligence, "Corporate Cyber Attacks Up 50% Last Year" (2022)

FUSION
MANAGED IT

+1 (888) 475-9370

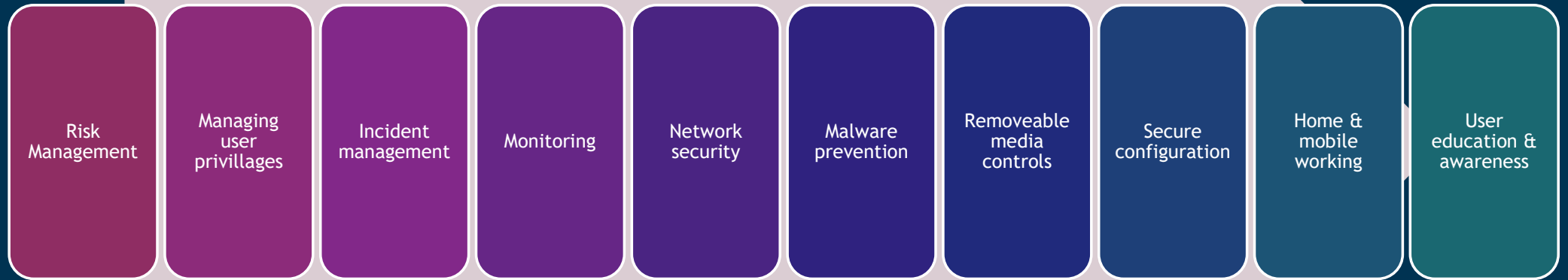
fusionmanagedit.com

info@fusionmanagedit.com

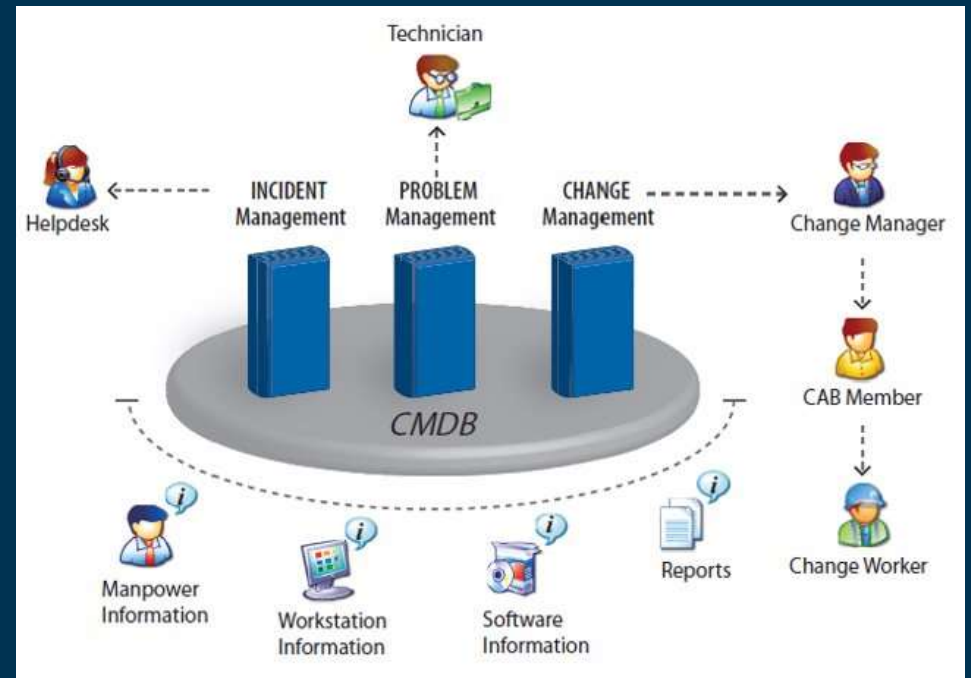
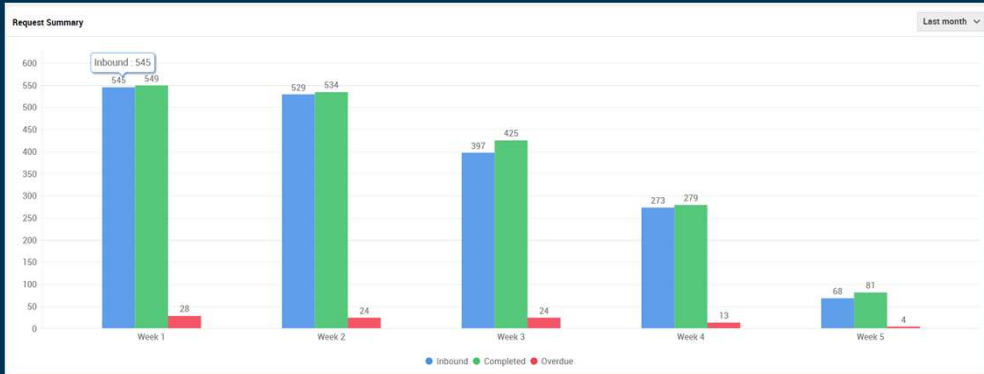
PERUBAHAN PARADIGMA TENTANG CYBERSECURITY

PARADIGMA LAMA		PARADIGMA BARU
Users are employees	➔	Employees, partners, customers, bots, things
Corporate managed devices	➔	BYOD & IoT
On-premises apps	➔	Explosion of cloud apps
Monolithic apps	➔	Composite apps & public restful APIs
Corporation network & firewall	➔	Perimeter-less
Local packet tracking & logs	➔	Explosion of signal

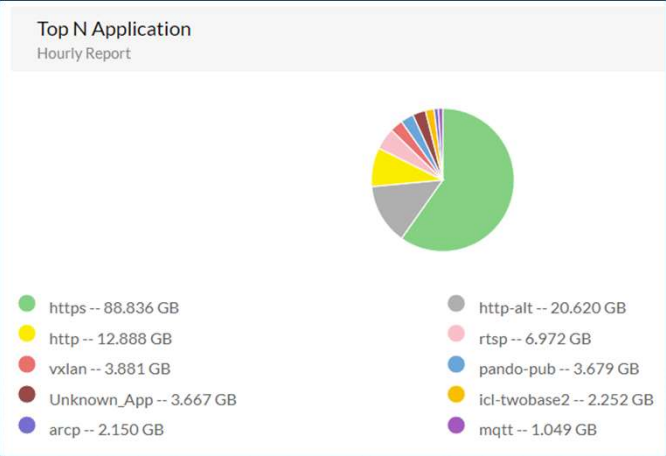
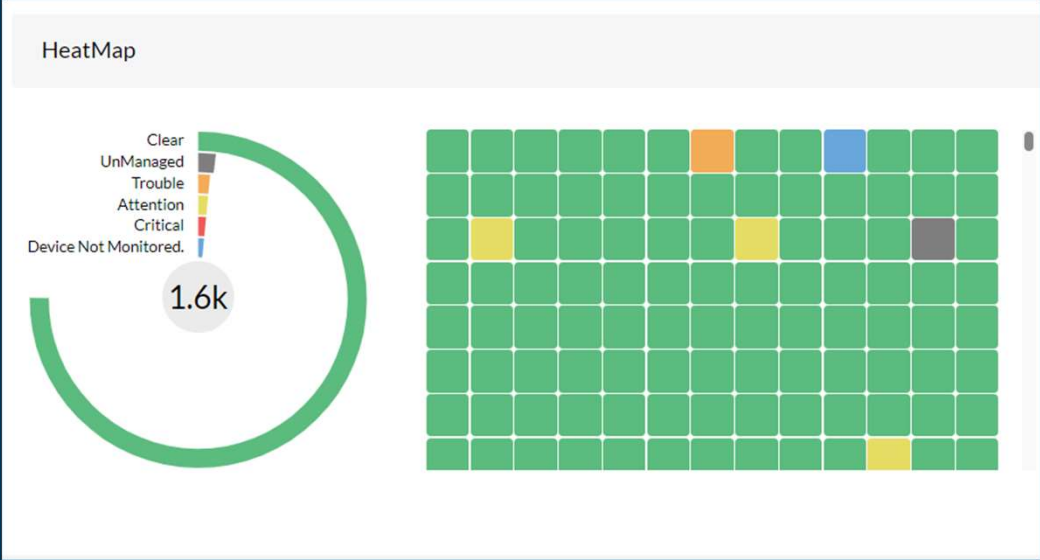
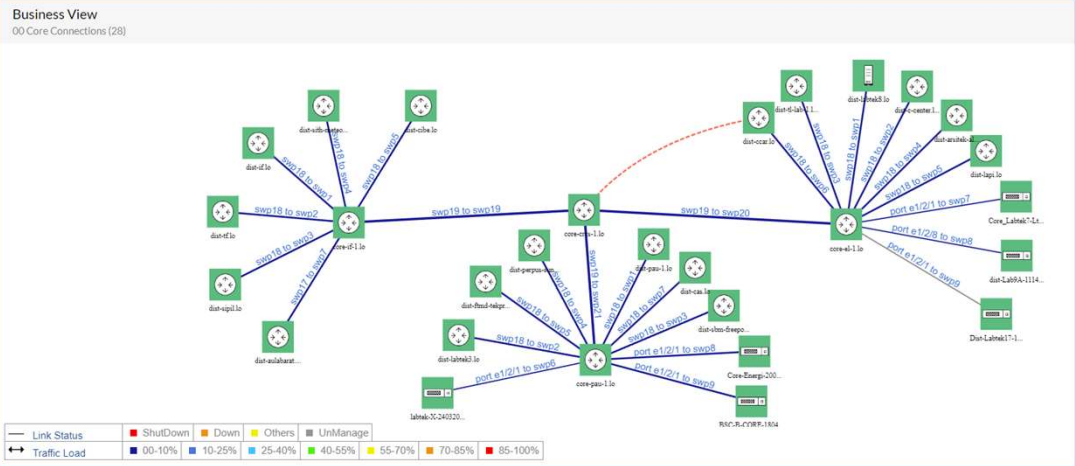
10 Steps to Cyber Security



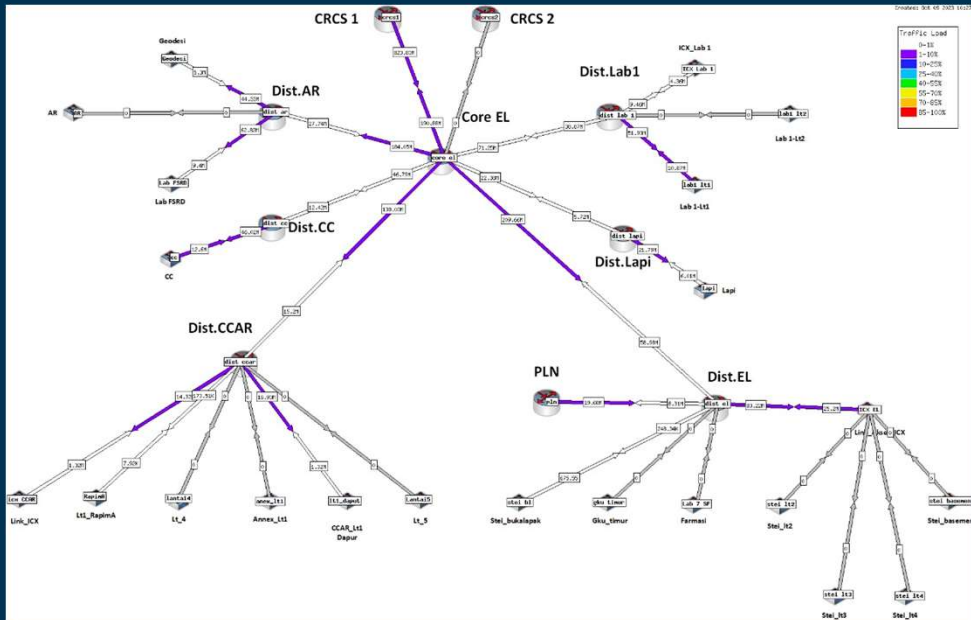
INCIDENT MANAGEMENT SERVICE DESK PLUS



DASHBOARD OPERATIONAL MONITORING



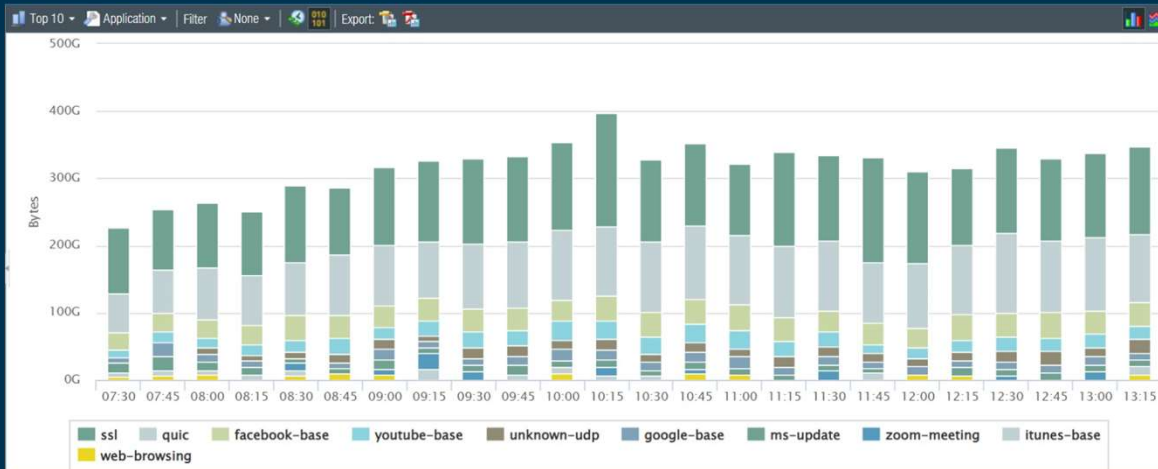
DASHBOARD NETWORK ACTIVITY



Device Summary

	Total	Up	Down	Ignore tag	Alert disabled	Disabled
Devices	476	355	107	2	11	4
Ports	19939	8293	9291	0	NA	2295
Services	27	22	1	0	NA	3

DASHBOARD MONITORING FIREWALL



Name	From Zone	To Zone	Source address	Source User	Destination address	Dynamic User Group	To Port	Application	Action	Severity
WordPress Login Brute Force Attack	Zone_Un...	Zone_Trust	192.18.130.225		167.205		80	web-browsing	reset-both	critical
Wordpress-BruteForce	Zone_Un...	Zone_Trust	146.235.200.145		167.205		80	web-browsing	reset-both	critical
Wordpress-BruteForce	Zone_Un...	Zone_Trust	146.235.200.145		167.205		80	web-browsing	reset-both	critical
WordPress Login Brute Force Attack	Zone_Un...	Zone_Trust	192.18.130.225		167.205		80	web-browsing	reset-both	critical
Wordpress-BruteForce	Zone_Un...	Zone_Trust	192.18.130.225		167.205		80	web-browsing	reset-both	critical
Wordpress-BruteForce	Zone_Un...	Zone_Trust	146.235.200.145		167.205		80	web-browsing	reset-both	critical
Wordpress-BruteForce	Zone_Un...	Zone_Trust	146.235.200.145		167.205		80	web-browsing	reset-both	critical
WordPress Login Brute Force Attack	Zone_Un...	Zone_Trust	192.18.130.225		167.205		80	web-browsing	reset-both	critical
WordPress Login Brute Force Attack	Zone_Un...	Zone_Trust	192.18.130.225		167.205		80	web-browsing	reset-both	critical
WordPress Login Brute Force Attack	Zone_Un...	Zone_Trust	192.18.130.225		167.205		80	web-browsing	reset-both	critical
XMRig Miner Command and Control	Zone_Trust	Zone_Un...	10.2.104.119		85.25.2		82	json-rpc	reset-both	critical

DASHBOARD 365 DEFENDER

The screenshot displays the Microsoft 365 Defender dashboard with the following sections:

- ITDR Deployment Health:** Shows deployment status for Defender for Cloud Apps, Defender for Identity, and Azure AD Identity Protection. A warning indicates that the environment is not updated against security-related threats.
- Connected SaaS apps:** Displays health status for SaaS apps, including healthy, alerts attention, and connection errors.
- Microsoft Secure Score:** Shows a score of 49.98% (866,241/1,328 points achieved) with a progress bar and a line chart showing trends over time.
- Device compliance:** Reports 24% noncompliance with a progress bar and a simulation section for a cross-product attack.
- Malware remediated:** Shows malware remediation statistics, including malware found and successfully remediated.
- Users at risk:** Reports 6615 users at risk, categorized by high, medium, and low risk.
- Insider Risk Management:** States that 25% of breaches are attributed to insider risks and offers simulation tools.
- Attack simulation training:** Reports that 100% of users have not experienced the simulation.
- Device health:** Shows 50 active devices, with 1 misconfigured and 27 inactive.
- Recently discovered devices:** A donut chart shows 1,266 devices discovered in the last 7 days, categorized by workstation and unknown.
- Active incidents:** Shows 1,956 active incidents with a line chart of most recent incidents and alerts.
- Discovered devices:** Reports a total of 15.1k discovered devices, broken down by device type (Unknown, Network Device, Audio and Video, Printer, Communication, Surveillance, Miscellaneous).
- Action center:** Lists 11 pending actions, including Malicious and Pending Approval.
- Threat analytics:** Shows 273 threats requiring action, including high-impact threats and highest exposure threats.
- Azure Sentinel integration:** Promotes end-to-end visibility with Azure Sentinel.

DASHBOARD COMPLIANCE MANAGER

Microsoft Purview
Automate compliance posture monitoring across your multicloud data estate with our updated assessments. [Learn more about multicloud support](#)
Create assessment

Compliance Manager settings
Data connectors
What's new?

View assessments
Filter

- Home
- Compliance Manager
- Data classification
 - Overview
 - Classifiers
 - Content explorer
 - Activity explorer
- Data connectors
- Policies
 - Roles & scopes
 - Trails
- Solutions
 - Catalog
 - App governance
 - Content search
 - Communication compliance
 - Data loss prevention
 - eDiscovery
 - Standard
 - Premium
 - Data lifecycle management
 - Microsoft 365 Exchange (legacy)
 - Information protection
 - Overview
 - Labels
 - Label policies
 - Auto-labeling
 - Information barriers
 - Insider risk management
 - Records management
 - Privacy risk management
 - Subject rights requests
 - Insider risk management
 - Records management
 - Privacy risk management
 - Subject rights requests
 - Information barriers
 - Records management
 - Privacy risk management
 - Subject rights requests
 - Information barriers
 - Insider risk management
 - Records management
 - Privacy risk management
 - Subject rights requests

Compliance Manager


Overview Improvement actions Solutions Assessments Regulations Alerts Alert policies

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. [Find guidance and documentation](#)

One or more of your assessments in based on a regulation template that has been updated. Review these assessments and decide if you want to update them with the new content.

Overall compliance score

Your compliance score: 63%



11742/18413 points achieved

Your points achieved: 163 / 6,234

Microsoft managed points achieved: 11,579 / 12,179

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Key improvement actions

Improvement action	Impact	Test status	Group	Action type
Create mail flow rules to encrypt messages	+27 points	= None	Default Group	Technical
Automatically apply Client Side Sensitivity Labels	+27 points	= None	Default Group	Technical
Conceal information with lock screen	+27 points	= None	Default Group	Technical
Implement rights management system for email	+27 points	= None	Default Group	Technical
Use IRM to protect online documents and storage	+27 points	= None	Default Group	Technical
Implement DMARC for outbound mail	+27 points	= None	Default Group	Technical
Set up Sender Policy Framework to prevent spoofing	+27 points	= None	Default Group	Technical
Use boundary protection devices for unclassified non-national security	+27 points	= None	Default Group	Technical
Apply sensitivity labels to protect ePHI	+27 points	= None	Default Group	Technical

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remaining actions
Audit	0/100 points	12
Azure	0/3 points	1
Azure Active Directory	118/331 points	27
Azure Information Protection	0/243 points	9
Azure Security Center	0/1 points	1
Communication compliance	0/42 points	6
Compliance Manager	18/2171 points	269
Data classification	0/30 points	2
Data loss prevention	0/129 points	5

Learn how your Compliance score is calculated

View all improvement actions

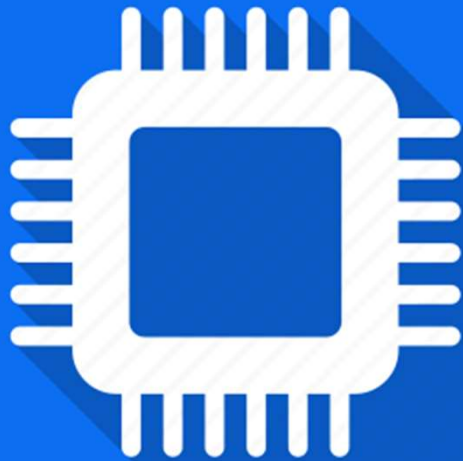
View all solutions

Compliance score breakdown

Category	Score	Points achieved	Description
Protect information	2%	22/108 points achieved	Enable and configure encryption, control access to information, and prevent data leakage and exfiltration
Govern information	0%	0/81 points achieved	Govern sensitive information and prevent its inadvertent disclosure
Control access	15%	116/769 points achieved	Configure authentication and password settings, user and sign-in risk policies, and review access reports
Manage devices	0%	0/901 points achieved	Use device configuration profiles, implement malicious code and spam protection, secure mobile devices, and block unwanted applications
Protect against threats	0%	0/770 points achieved	Prevent, detect, investigate, and respond to advanced threats
Discover and respond	0%	0/162 points achieved	Discover non-compliant applications, configure audit and alert policies, review and correlate audit records, and review alerts, activity, access, and detection reports
Manage internal risks	0%	0/42 points achieved	Identify and remediate critical insider risks
Manage compliance	80%	1097/1450 points achieved	Define your compliance scope, test control effectiveness, and manage your risk & compliance assessment

Disclaimer: Recommendations from Compliance Manager should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are subject to the terms and conditions in the [Online Services Terms](#). See also [Microsoft 365 license guidance](#)

NIST Cybersecurity Framework



- The NIST (US National Institute for Standard and Technology) Cybersecurity Framework is a set of guidelines for mitigating (manage and reduce) organizational cybersecurity risks
- Provides a common language for understanding, managing and expressing cybersecurity risk to internal & external stakeholders
- Can be used to help identify and prioritize actions for reducing cybersecurity risk and it is a tool for aligning policy, business and technological approaches to managing that risk

Preparation

Organizational
Communication

Development of
Control Baselines

Enterprise Architecture

Alignment with Risk
Management
Framework

Identify

Asset Management

Business Environment

Governance

Risk Assessment

Risk Management
Strategy

Supply Change Risk
Management

Detect

Identity Management &
Access Control

Awareness & Training

Data Security

Protective Technology

Information Protection
Processes &
Procedures

Maintenance

Respond

Respond Planning

Communications

Analysis

Mitigation

Improvements

Recover

Recovery Planning

Improvements

Communications

Pertanyaan Umum

- What applications or portals are you users accessing corporate data?*
- What apps contains business critical data?*
- Are users leaves, how do you know they don't have corporate data stored on their personal device?*
- Do users access email their personal cell phone?*
- Are there business-critical pieces of data that would leave you exposed if a personal device was compromised?*
- What would be the cost to company if this data was leaked?*
- Are we compliant if data is leaked to unmanaged applications like a user's personal cloud storage?*
- Do you want your users to be able to access corporate data securely from anywhere at any time?*
- Do employees have access to corporate apps after they leave the company? How do you know if they do?*

ITB Cybersecurity Policy



Optimizing Microsoft A3 License

Single Sign ON → Azure Active Directory

Microsoft Outlook Email

Mobile Device Management → INTUNE

Optimizing Windows Defender

The screenshot displays the Microsoft 365 Compliance Manager interface. The overall compliance score is 75%, with 1460/1937 points achieved. The dashboard is divided into several sections:

- Key improvement actions:** A table listing 12 actions, including "Protect Authentication Content", "Limit Connective Login Failures", and "Implement Account Lockout".
- Compliance score breakdown:** A grid of categories and their respective scores:

Categories	Assessments
Protect information	4% (1/27 points achieved)
Protect against threats	0% (0/100 points achieved)
Discover and respond	0% (0/100 points achieved)
Control access	0% (0/100 points achieved)
Manage devices	9% (8/90 points achieved)
Manage internal risks	0% (0/100 points achieved)
Manage compliance	88% (88/100 points achieved)

KEBIJAKAN KEAMANAN DAN AREA PENGELOLAAN SMKI

- ❑ Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik
- ❑ Peraturan Badan Siber dan Sandi Negara Nomor 10 tahun 2020 tentang Tim Tanggap Insiden Siber
- ❑ Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik
- ❑ Permendikbudristek Nomor 8 Tahun 2022 Tentang SPBE Kemendikbudristek
- ❑ Persesjen Kemendikbudristek Nomor 11 Tahun 2022 tentang Sistem Manajemen
- ❑ Keamanan Informasi pada SPBE Kemendikbudristek



Area Pengelolaan SMKI

Berdasarkan
Pesesjen
Kemendikbudristek
No.11 Tahun 2022

- a. Keamanan personil;
- b. Keamanan aset;
- c. Keamanan akses;
- d. Keamanankriptografi;
- e. Keamanan fisik dan lingkungan;
- f. Keamanan operasional;
- g. Keamanan komunikasi;
- h. Keamanan pengembangan dan pemeliharaan;
- i. Keamanan pihak ketiga;
- j. Manajemen insiden keamanan siber;**
- k. Manajemen keberlangsungan layanan SPBE Kementerian;
- l. Pengendalian kepatuhan; dan
- m. Audit keamanan SPBE Kementerian.

TASK EDU CISRT KEMENDIKBUD

Mencatat insiden keamanan informasi TIK Kemendikbud RI

Mendokumentasikan insiden keamanan informasi TIK Kemendikbud RI

Meneruskan insiden keamanan informasi TIK Kemendikbud RI kepada pihak external yang berkompeten

Memberikan telaah serta memberikan solusi atas insiden keamanan informasi TIK

CHALLENGE



TERIMA KASIH