cbts

AI-powered NaaS defends against modern cyber threats

Every business is at risk from a new generation of sophisticated cyber threats

Threat actors increasingly target individuals to gain unauthorized access to sensitive business data. When hidden behind valid credentials, malicious activity is hard to distinguish from legitimate use.

The damage from a data breach is not limited to individual employees. However, in 2024, the average cost of a data breach to its organization was $4.88 million.[2]

Without awareness and support, users put themselves and their organizations at risk every day by:

Careless browsing
Be aware

Do not:
- Use unsecured Wi-Fi connections

Do:
- Learn to recognize suspicious webpages
- Pay attention to security measures on pages and in your browser

Malicious e-mails
Be suspicious

Do not:
- Engage with unfamiliar messages. In 2023, 30% of cybersecurity incidents resulted from a successful phishing message—more than any other attack vector

Do:
- Verify all incoming emails even if they see valid. Attacks using valid credentials increased by 71% in 2022[1]

Weak passwords
Be smart

Do not:
- Use common, compromised, or simple passwords.
- Use the same password for multiple sites

Do:
- Use complex passwords with a mix of characters
- Change your passwords regularly
- Take advantage of a secure password manager

Types of data breaches

Internal incidents
Unintentional or malicious data loss from an inside source

- **Insider theft** occurs when an employee or third party exposes or steals sensitive information.

  In 2022: Malicious insiders caused 26% of cybersecurity incidents.

- **Accidental exposure** results from lost assets or mishandling of information.

  In 2022: 56% of cyberattacks were caused by employee or contractor negligence.[3]

External attacks
Strategic strikes from individuals or groups with technological expertise

- **Account compromise** occurs when threat actors use a valid business account for malicious activity.

  In 2023: Use of InfoStealers—a software that harvests data, including user credentials—increased by 266%.[4]

- **Ransomware** encrypts critical business data and demands money in exchange for the key.

  There is no guarantee paying the ransom will release encrypted files.

  In 2023: Enterprise ransomware incidents dropped 11.5%, highlighting the shift to account compromise.[1]

Fighting fire with fire

Cybercriminals are beginning to leverage AI tools to craft more convincing, thorough, and efficient attacks. AI-powered security platforms can harden your organization against this latest generation of threats. AI-driven network security can:

- Automatically flag suspicious behavior, even from valid accounts.
- Intelligently escalate security alerts to human experts.
- Analyze network activity trends and identify outliers.
- Adapt to the latest threat intelligence.
- Assess security configurations for vulnerabilities and recommend improvements.
- Learn from security incidents and improve remediation.
- Detect and respond to intrusions in real time.

Modern threats require specialist support

Cybersecurity is becoming a specialized field. Many companies—particularly small- and medium-sized businesses, for whom attacks are increasing—have neither the personnel nor expertise to mount a mature defense against modern cyber threats. For these businesses, engaging a trusted cybersecurity partner is critical.

77%	of companies experienced at least one cybersecurity incident in 2022-2023
18%	of companies reported that a cybersecurity skills shortage caused their incidents
75%	of companies see cybersecurity skills shortages as a serious issue
41%	of companies plan to hire third-party cybersecurity experts to prevent future breaches[4]

Why CBTS?

Network as a Service (NaaS) solutions from CBTS offer enterprises of every size comprehensive, up-to-the-minute protection from the latest cybersecurity threats. CBTS NaaS delivers the latest in AI-powered network monitoring and threat intelligence without the time and expense of on-premises upgrades, backed by the collective expertise of industry-leading security professionals.

Partner with CBTS to free your technology team to focus on the essential day-to-day responsibilities of running a contemporary business. **Contact CBTS today to learn more.**

Sources:

1. X-Force Threat Intelligence Index 2024 | IBM
2. Cost of a Data Breach Report 2024 | IBM
3. Cost of Insider Threats Global Report 2022 | ProofPoint
4. Human Factor 360° Report 2023 | Kaspersky