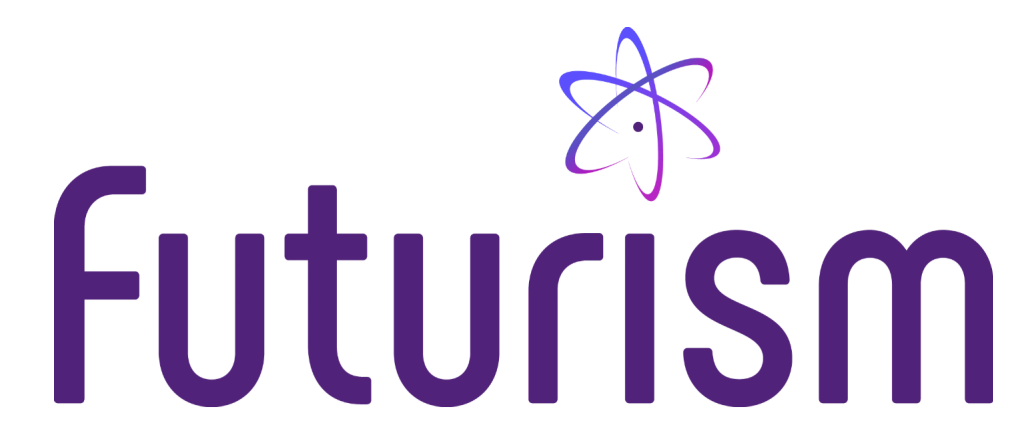


Futurism Managed Security Services



Powered by IBM Watson Advanced Threat Intelligence

We have the security skills to cover you 24/7/365

With threat actors using sophisticated and multi-prong cyber tactics to get at your data, cybersecurity is more important than ever.

→ Some alarming cybersecurity facts:

- 48% of hospital executives reported shutdowns as a result of external attacks or Ransomware attacks!
- Midsize hospitals reported an average shutdown of 10 hours at a cost of \$45,700 per hour due to cyberattacks
- Nearly half of hospital IT teams lack adequate security staffing
- 64% of hospitals were found to be unprotected against Ransomware and other vulnerabilities

Time to act now!

Futurism's Managed Security Service offerings are aimed at simplifying the lives of IT/security teams & admins, managers and CTOs alike. Our security experts leverage a Zero-Trust Security architecture and work like an extended arm of your IT and security team helping to secure your business and data round-the-clock.

Be it tackling new threat actors or addressing the problem of skill shortage, we do it for you so you don't have to hire additional security staff or spend on expensive security tech or products.

✓ Why Futurism's Managed Security Services?

- ✓ Full stack of security defense-in-depth levels available
- ✓ Zero-Trust Security Framework for improved security strategy & maturity
- ✓ Service based on best-of-breed security products/technology (IBM)
- ✓ Monthly service fee - no product or capital costs
- ✓ Security automation
- ✓ 24/7/365 coverage & support
- ✓ Certified security experts & Global presence
- ✓ IBM Global Business Partner with 18+ years of expertise
- ✓ Flexible SLAs & engagement models
- ✓ Quarterly business reviews

Mitigate attack surface for a range of cyber threats

Backed by market-leading threat intelligence technology (IBM Advanced Threat Intelligence), our Cybersecurity Services offer protection against a range of advanced threats/vulnerabilities and help reduce the attack surface significantly.

✓ Email Security

- ✓ Detects phishing attempts/Ransomware/malware
- ✓ Phishing tests for employee awareness
- ✓ Zero-Day threat protection

✓ Web Security

- ✓ Enforce acceptable use policies
- ✓ Block attempts to click on websites containing malware
- ✓ Remote Filtering and SSL Inspection

✓ Database Security (Data-Protect)

- ✓ Managed database protection (IBM Guardium)
- ✓ Data Discovery & Compliance
- ✓ Intelligent data activity monitoring & protection
- ✓ Advance and active data threat analytics
- ✓ Data Exfiltration
- ✓ Round-the-clock threat response

✓ Identity & Access Management (Secure-Access)

- ✓ Intelligent hybrid IAM (IBM Verify Access)
- ✓ Zero-Trust approach
- ✓ Strong multi-factor authentication
- ✓ Identity federation
- ✓ Risk based authentication powered by AI

✓ Endpoint Security - EndPoint Secure (IBM MaaS360 with Watson)

- ✓ Unified endpoint management (UEM) & mobile device management (MDM)
- ✓ Device encryption & mobile security index
- ✓ BYOD endpoint security & remote access
- ✓ Enforce application policies (what can be downloaded)
- ✓ Enforce patch applications
- ✓ Real-time reporting & analytics (IBM MaaS360)

Advanced Threat Protection – Eagle Eye (IBM QRadar)

Get ahead of advanced and sophisticated threat actors with our Advanced Threat Protection Services powered by IBM Advanced Threat Intelligence.

Our security experts leverage IBM QRadar and intelligence feeds from X-Force & IBM Watson AI to provide up-to-the-minute protection from novel threats including new strands of Ransomware and multi-prong attacks.

Insider Threat Detection

✓ Privileged user monitoring

- ✓ Preconfigured alerts and notifications for DoS attacks and hijacked accounts
- ✓ Behavioral analytics

✓ Trusted Host and Entity Compromise

- ✓ Determine risk score of an entity (e.g. disgruntled employee)
- ✓ Track Network Activity
- ✓ Remote Access Activity (Credential theft, password sharing)
- ✓ Identity (credential violations, account takeover, privilege escalations)

✓ Abnormal Authentication Behavior

- ✓ Real-time alerts for brute force attacks, password guessing, and unauthorized access

✓ Cloud Discovery

- ✓ Track abnormal cloud usage & workload
- ✓ Centralized security monitoring
- ✓ Identify misconfigurations
- ✓ Intelligent user monitoring capabilities

✓ Protection against Phishing attacks

- ✓ Identify malicious code/content – including hidden ones
- ✓ Detect and extract suspicious e-mail contents & attachments

✓ Protect Mission Critical Business Assets

- ✓ Gain visibility and understanding of network topology & attack paths
- ✓ Protect critical assets such as financial, EMR, EHR, COVID databases, etc.
- ✓ Monitor logs and source for unauthorized attempts

✓ Endpoint Protection including EDR (Endpoint Detection & Response)

- ✓ Scan and detect Ransomware and malware across all endpoints including mobile & IoT devices
- ✓ Quarantine and remediate infected devices, machines, servers, etc.
- ✓ Advanced risk & threat analysis with IBM QRadar

✓ Automatic Investigation with IBM Watson AI

- ✓ Automated security analysis & escalation of offenses with IBM QRadar & Watson AI
- ✓ Monitor unstructured data & large amounts of data in shorter periods of time
- ✓ Identify more attack patterns using IBM QRadar and Watson AI
- ✓ Concentrate on higher priority threats



Don't take the bait! Get help now

Get in touch with our security expert today!

Learn more about our Managed Security Services here