
Security
Offering

Table of Contents

MS Defender for Business

- Advanced endpoint protection
- Significant advances and investment from Microsoft
- Native integration with the Microsoft Cloud
- Becoming the industry standard
- Including in your current licensing


Microsoft Defender
for Business
Elevate your security
Threat & Vulnerability Management
Attack Surface Reduction
Next Generation Protection
Endpoint Detection & Response
Auto Investigation & Remediation
Simplified Onboarding and Administration
APIs and Integration

DarkWeb Monitoring

Cyberattack danger is ramping up for organisations in every sector as the world grows more technology-dependent and interconnected. Shifting circumstances due to tumultuous world events are giving the bad guys golden opportunities to profit from cybercrime…

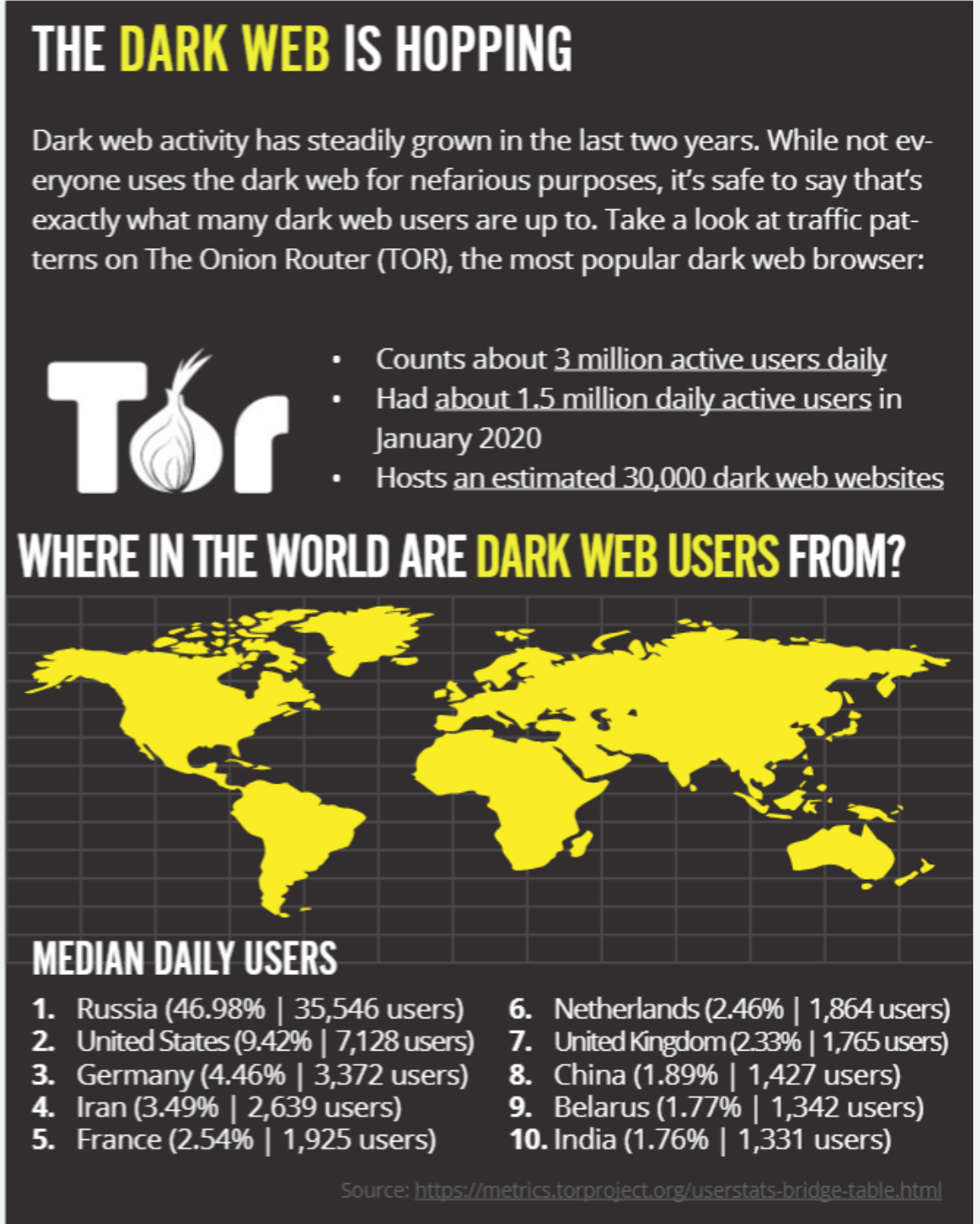
and they aren’t hesitating to act.

itGlobal Technology 102/815 Pacific Hwy, Chatswood NSW 2067

The Reality

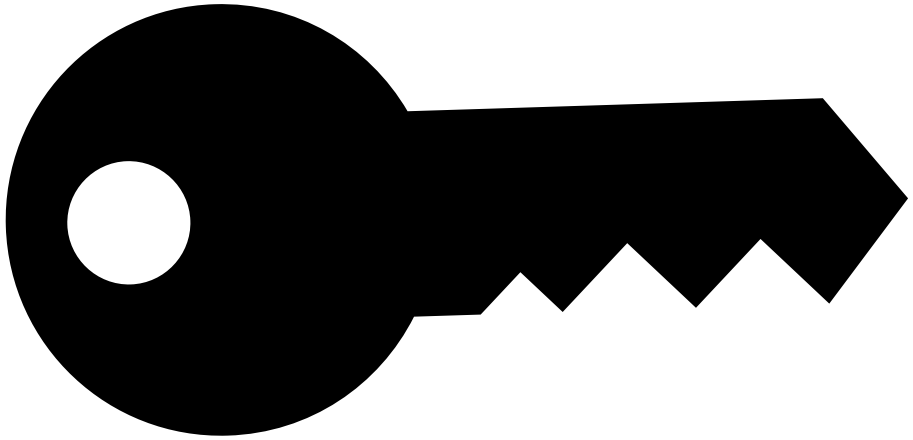
User credentials are the key

- 15 billion logins are on the dark web.
- The average organization has 17 exposed login details.
- 133,927 C-level Fortune 1000 executives' credentials are accessible on the dark web.
- Corporate login details with plaintext passwords on the dark web increased by 429% since 2020.



What is Dark Web

- Dark web monitoring involves searching, tracking, and verifying specific information on the dark web. It utilizes a combination of human analysts and specialized software to analyse harvested data from dark web locations where information is traded.



Features

- Dark Web Monitoring
- Compromised Credential Detection
- Data Leak Detection
- Identity Theft Protection
- Proactive Alerts
- Comprehensive Reporting


Security
Training

Insider risk

Every business that handles data or operates digital systems is at risk of an insider incident that impacts their security – and that risk is growing.

Why is Training so Important?

Almost 90% of all security incidents are a result of human error.

Phishing emails aim to steal login credentials, perpetrate financial fraud or launch even more dangerous assaults like ransomware and account takeover.

Untrained employees are a ticking time bomb.

- Only an estimated 30% of internet users know what ransomware or malware is.
- 97% of employees cannot spot a sophisticated phishing email.
- Only 16% of employees can recognize cyberthreats without security awareness training.
- An estimated 55% of organizations say privileged users are their greatest insider threat risk.
- More than 2 out of 3 insider threat incidents are caused by negligence.
- More than 80% of data breaches involve a human element.
- Over 65% of accidental insider threats come from phishing attacks.

What can you do?

USER TRAINING & EDUCATION

TRAIN employees to spot phishing attempts that may slip through email security

SOLUTION:

Provisioning a security awareness training and phishing simulation solution that educates and protects every employee.

1. Educate and empower employees to spot and stop phishing threats
2. Use training campaigns
3. Satisfy requirements for cyber liability insurance
4. Maintain compliance with industry regulations

Features

ENGAGING CONTENT

Choose from a rich set of plug-and-play phishing simulation kits and animated video lessons accompanied by short quizzes — and ensure that training reaches every employee no matter how tech-averse they are.

SEAMLESS AUTOMATION & REPORTING

Easily schedule training and phishing campaigns up to a year in advance. Reports show training results for the entire organization as well as individual employees and get delivered automatically to designated recipients.

CUSTOMIZABLE MATERIALS

Customize phishing emails, sending email addresses and attachments to your needs to mimic threats specific to your organization and increase training effectiveness.

ALWAYS-CURRENT TRAINING ASSETS

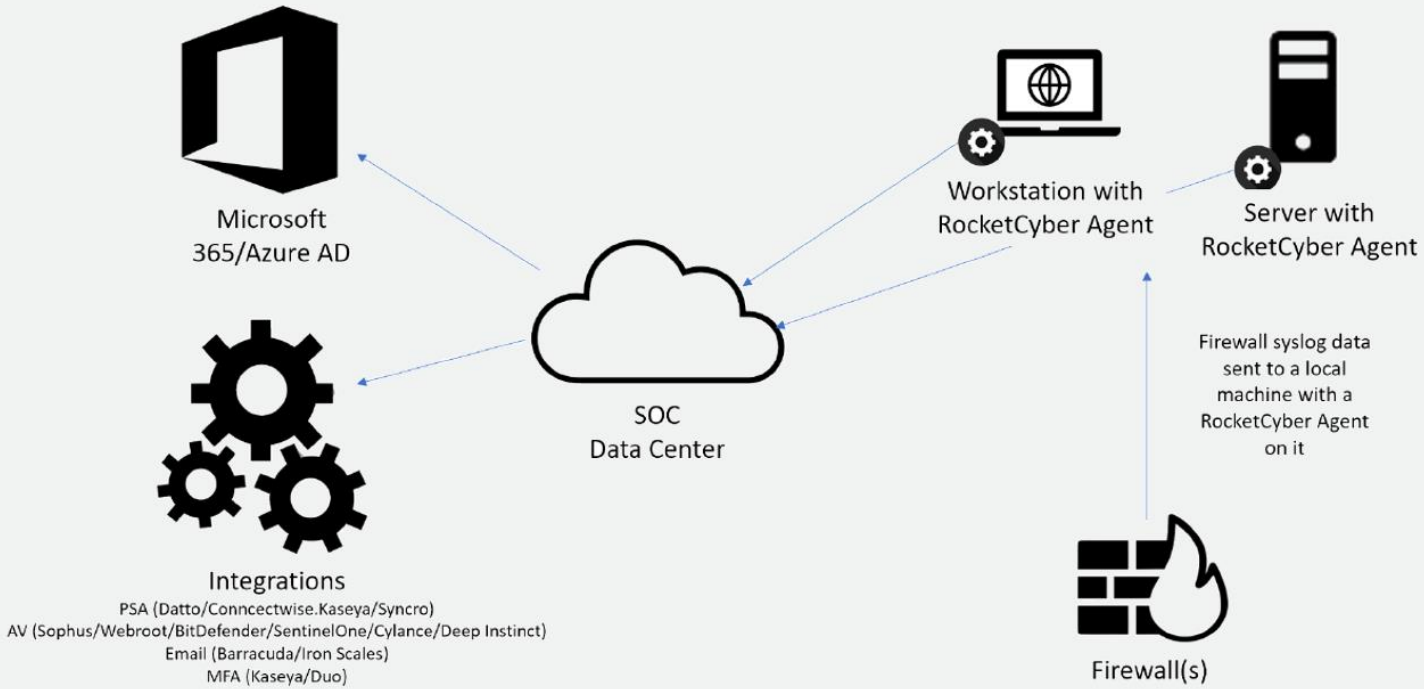
Fresh phishing kits and videos are released monthly to reflect the current threat landscape and keep your employees on the lookout for trouble.

Managed Security Operations Centre (SOC)

"Today's cybercriminals have adopted automation, which has enabled them to cost-effectively and aggressively target the SMB market. Our advanced security operations services enable us to protect you more effectively and efficiently by providing 24x7 security monitoring and incident response."

itGlobal Technology 102/815 Pacific Hwy, Chatswood NSW 2067

How does it work?



ENDPOINT SECURITY

Windows & macOS event log monitoring, advanced breach detection, malicious files and processes, threat hunting, intrusion detection, 3rd party NGAV integrations and more.

NETWORK SECURITY

Firewall and edge device log monitoring integrated with real-time threat reputation, DNS information and malicious connection alerting.

CLOUD SECURITY

Secure the cloud with Microsoft 365 security event log monitoring, Azure AD monitoring, Microsoft 365 malicious logins and overall Secure Score.

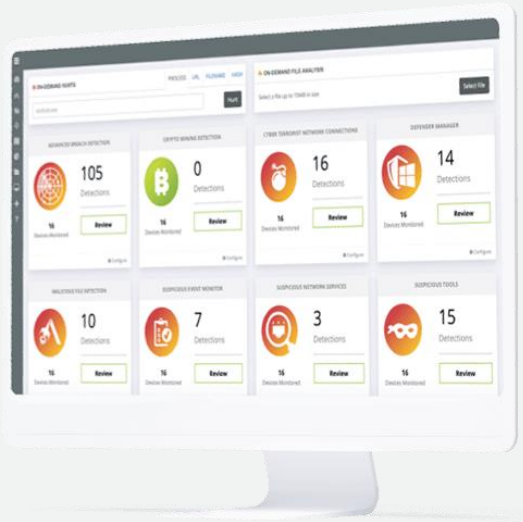
Looking after your environment in all 3 attack vectors

24x7 Cyber Security Powered by Experts

Our elite team of security veterans hunt, triage and work with your team when actionable threats are discovered.

itGlobal Technology 102/815 Pacific Hwy, Chatswood NSW 2067

Features

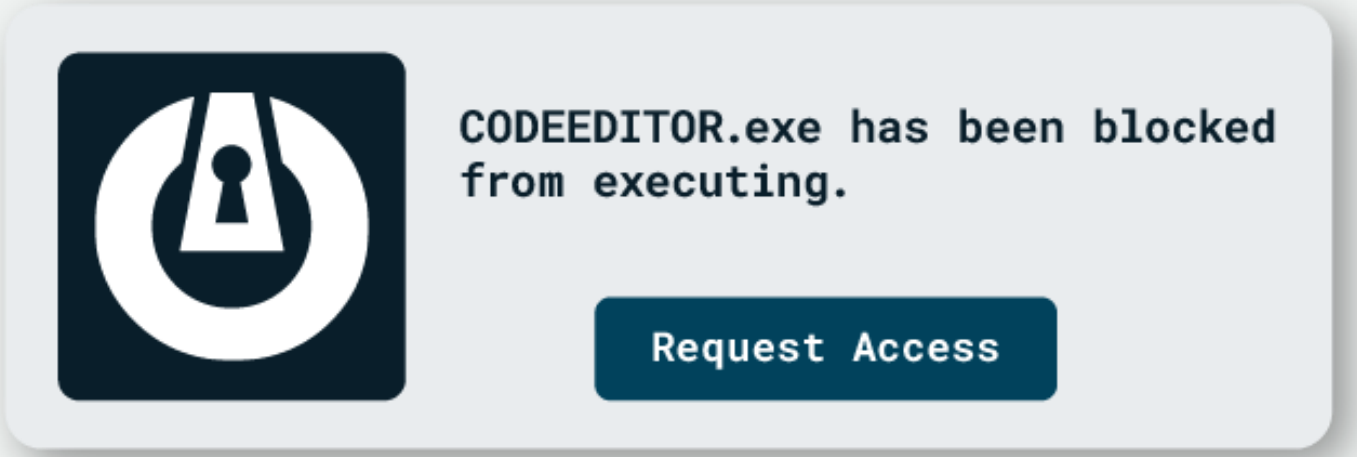


1. Seamless Log Monitoring
2. Threat Intelligence & Hunting
3. Breach Detection
4. Intrusion Monitoring
5. NextGen Malware

Application Hardening

What is Application Hardening

- Application Hardening is an advanced security solution designed to protect your endpoints
- Employs strict application control by allowing only trusted applications to run
- Safeguards against unauthorised applications



Features

- Application Control
- Ringfencing
- Storage Control
- Elevation Control