FEATURED PRODUCT

EXIGENT

Fortify Managed Detection & Response

Safeguard your data, network, and endpoints with Fortify Complete.

Comprehensive Cybersecurity for Your Business

Fortify Complete offers an all-encompassing cybersecurity solution to protect your organization from ransomware, malware, and other sophisticated cyber threats. Our advanced detection and response capabilities safeguard your endpoints, network, and cloud services, ensuring your business remains secure around the clock. Guided onboarding ensures a bespoke solution for your environment instead of a cookie-cutter solution.

Layer Live SOC into Protection

Enjoy the peace of mind that comes with a live 24/7 Security Operations Center (SOC) responding to critical alerts and watching for opportunities to improve your cybersecurity posture.

Minimize risk

Early detection

24/7 cybersecurity expertise

Fortify Complete

✓ **24/7 Security Operations Center (SOC)**

- Protect your business 24/7 with real-time response from cybersecurity experts

✓ **Active Response**

- Balance business continuity and risk management with automated, flexible response options tailored to your needs

✓ **Endpoint Detection and Response**

- Block ransomware and malware on your MacOS, Windows, and Linux devices
- Detect suspicious attack behavior in real-time

✓ **Network Detection and Response**

- Identify suspicious traffic and connections
- Protect devices not protected by endpoint agents or cloud

✓ **Suspicious Email Analysis Service (SEAS)**

- Receive notifications within minutes if any concerns are detected

✓ **Cloud Detection and Response**

- Stop unauthorized access and compromise within your cloud-based email and application accounts
- Protect services including Microsoft 365, Google Workspace, Dropbox, Box.com, AWS, Azure, Salesforce, ZenDesk, and Okta

✓ **24/7 Vulnerability Scanning**

- Detect potential threats such as outdated patches, misconfigurations, externally exposed assets, and shadow IT

✓ **Enjoy safe web browsing with DNS Firewall**

- Monitor and block connections to malicious websites

✓ **Dark Web monitoring**

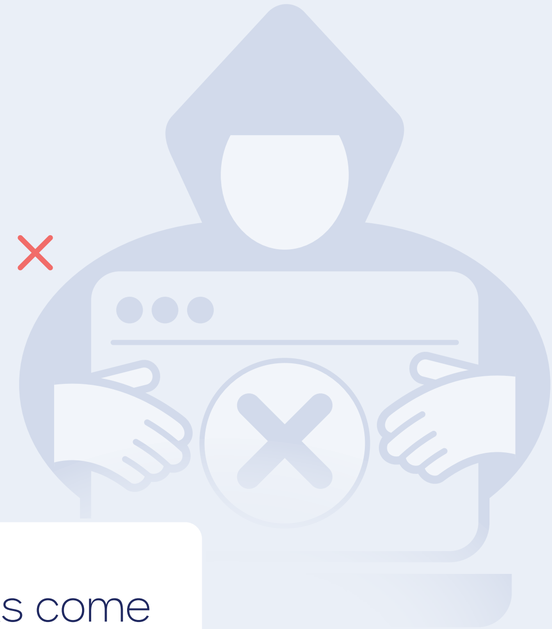
- Alerts when organizational data found available on the Dark Web

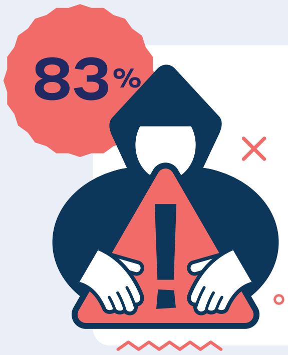
✓ **Log Retention**

- Store critical log data to improve compliance with frameworks

CONTACT US: 877-EXIGENT EXIGENT.NET

Why is Managed Detection & Response CRITICAL?





83% of alerts come from cloud apps with compromised credentials

68% of organizations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure

Attacks on endpoints are some of the most prevalent, with **81%** of businesses experiencing an attack involving some form of malware

*In cases where customer hardware or existing environments conflict with preferred software solutions, we can offer suitable alternatives.