Zivver Email Threat Protection

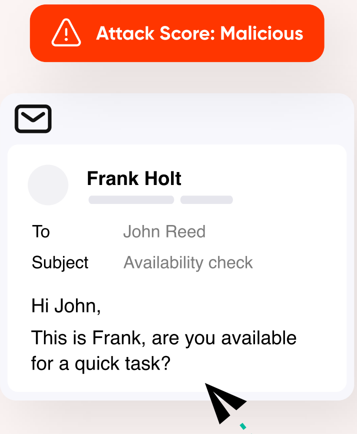
Elevate Your Email Security Beyond Microsoft 365

01

Microsoft 365 & Zivver: Why you need greater protection

Microsoft provides basic email security to protect against common threats like viruses and spam. However, with an emphasis on deliverability over comprehensive protection, significant gaps remain that advanced attackers can exploit. These gaps leave your organization vulnerable to sophisticated threats like phishing, Business Email Compromise (BEC), and ransomware.

Zivver complements Microsoft 365 by addressing these blind spots. Acting as a second pair of eyes, Zivver is purpose-built to protect against advanced, evolving threats using AI-powered detection, customizable threat prevention, and explainable intelligence.



Attack Score: Malicious

Frank Holt

To John Reed

Subject Availability check

Hi John,

This is Frank, are you available for a quick task?

02

The Gaps in Microsoft 365's Email Protection: Why Microsoft 365 alone isn't enough

While Microsoft offers baseline defenses for known malicious content, its security often falls short due to:

- Complexity in Configuration: Effective security requires deep expertise, making it difficult for non-experts to optimize defenses.
- Tier-Based Protection: Advanced features are locked behind costly, high-tier licenses, making comprehensive security less accessible.
- Lack of Transparency: Microsoft's "black box" approach provides limited insights into why emails are flagged or passed, leaving organizations unable to refine or trust their systems fully.
- Security by Obscurity: Relying on checkbox solutions without visibility or control over operations is risky in today's landscape.

These limitations create vulnerabilities,leaving organizations exposed to increasingly sophisticated threats.

03

Zivver Email Threat Protection: Closing the Gaps

Zivver enhances Microsoft 365 security with advanced, explainable, and customizable threat detection.

1. Advanced Threat Detection

Key features that make Zivver unique include:

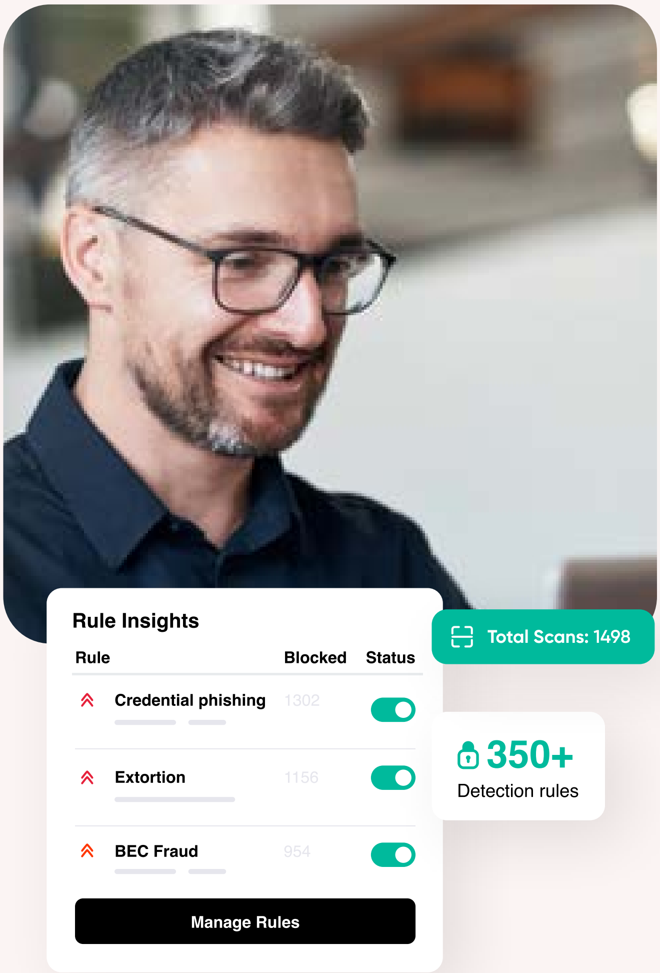
- ✓ Sandboxing: Analyze and isolate suspicious files in a controlled environment.
- ✓ URL Analysis: Prevent phishing links from reaching users.
- ✓ Multi-Database Virus Scanning: Cross-check threats against 12 malware databases.
- ✓ Click Protection: Safeguard against malicious links post-delivery.
- ✓ Sender Profiling: Detect suspicious deviations in sender behavior.
- ✓ Natural Language Processing: Identify social engineering attempts in email content.

Threat	✓ How Zivver stops it
Business Email Compromise	✓ Identifies and blocks impersonation attempts, even without malicious links or attachments.
Credential Phishing	✓ Alerts users to fake login pages, preventing credential theft.
Callback Phishing	✓ Neutralizes scams that bypass email filters by luring victims into calling fraudulent numbers.
Malware/ Ransomware	✓ Neutralizes hidden threats in attachments or links before they infiltrate systems.
VIP Impersonation	✓ Blocks highly targeted phishing attempts aimed at executives or high-value employees.

2. Explainable AI

Problem: Microsoft blocks emails without explaining why, limiting organizations' ability to investigate and refine detection rules.

Solution: Zivver's Explainable AI provides full transparency, offering insights into flagged emails-from a high-level summary for CISOs to in-depth technical details for engineers. This clarity builds trust and enables proactive threat management.



Rule Insights

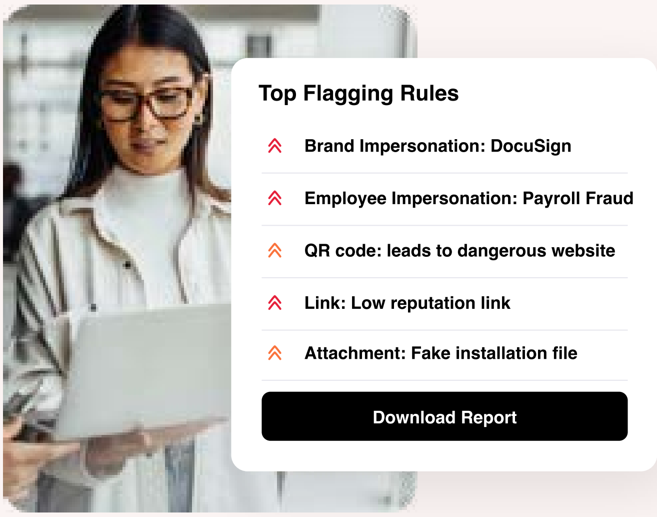
Rule	Blocked	Status
Credential phishing	1302	●
Extortion	1156	●
BEC Fraud	954	●

3. Customizable Threat Detection

Problem: No solution stops 100% of threats. Microsoft provides limited options for organizations to adapt to unique risks, leaving IT teams overwhelmed with alerts and operational disruptions.

Solution: Zivver allows for granular customization:

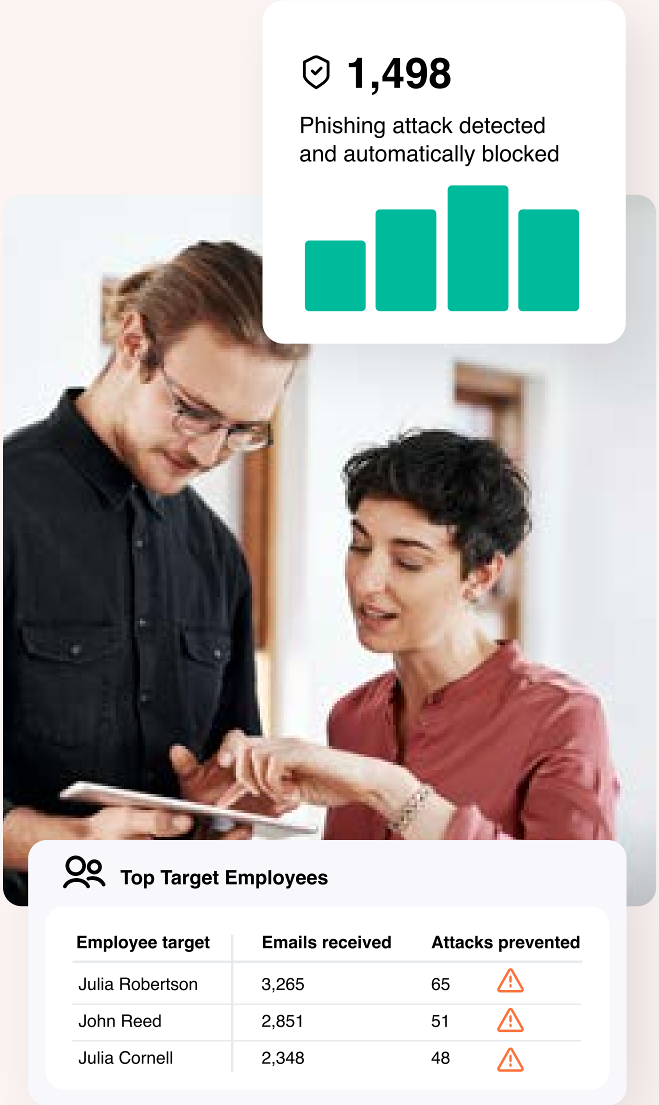
- **Custom Rules:** Tailor detection to fit your specific risks
- **Pre-Built Rules:** Leverage over 350 expert-curated rules for instant protection.
- **Behavioral AI:** Continuously learn and adapt based on your organization's email patterns.



Top Flagging Rules

- Brand Impersonation: DocuSign
- Employee Impersonation: Payroll Fraud
- QR code: leads to dangerous website
- Link: Low reputation link
- Attachment: Fake installation file

Download Report



1,498

Phishing attack detected and automatically blocked

Top Target Employees

Employee target	Emails received	Attacks prevented
Julia Robertson	3,265	65 ⚠
John Reed	2,851	51 ⚠
Julia Cornell	2,348	48 ⚠

4. Automated Triage and Workflow Integration

Problem: Without automation, IT teams face alert fatigue and missed threats, increasing organizational risk.

Solution: Zivver automates manual processes to enhance efficiency and accuracy:

- **Automated Triage:** Focus on high-risk threats, eliminating manual sorting.
- **Threat Hunting Tools:** Equip teams to quickly identify and neutralize risks.
- **Workflow Automation:** Streamline reporting and response tasks.

04

Your Questions - Answered

We're confident in our Microsoft 365 security.

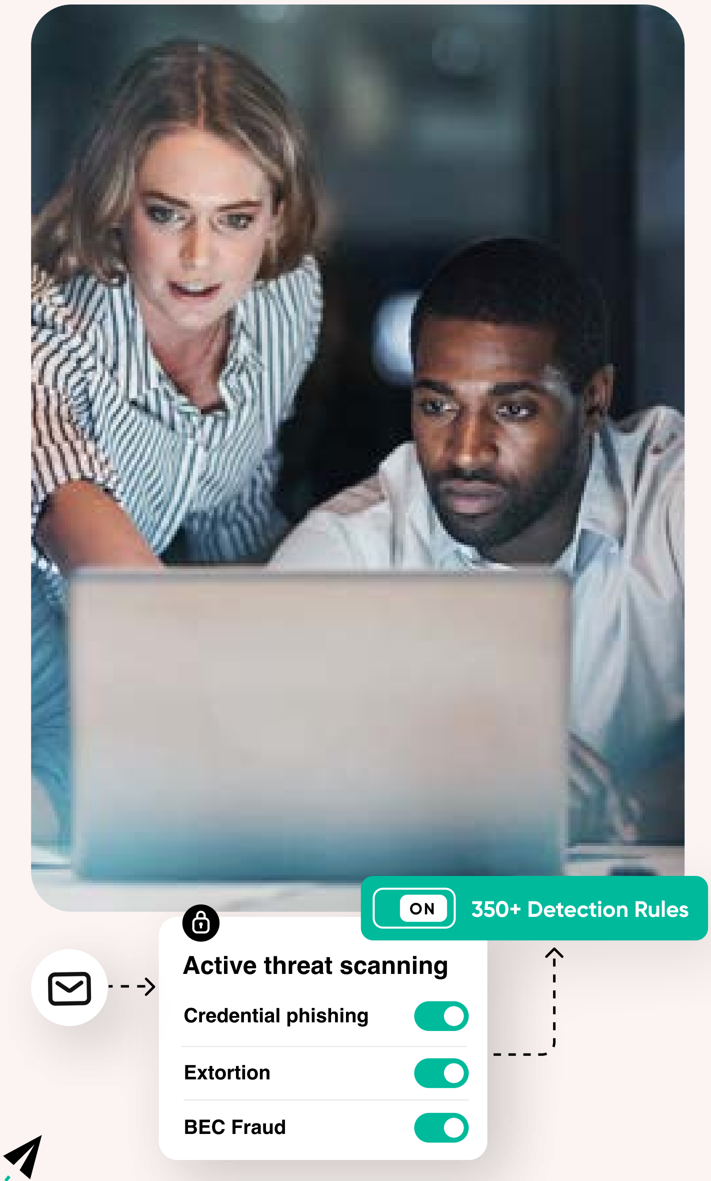
Defender for Office 365 struggles with sophisticated attacks like BEC, callback phishing, and VIP impersonation. These threats often bypass traditional defenses by avoiding malicious links or attachments. Zivver closes these gaps, offering advanced detection and layered protection for comprehensive security.

Why should we add Zivver to our existing setup?

Attackers evolve faster than standard solutions. Zivver identifies advanced threats like payload-less phishing and credential harvesting that others miss. Features like Explainable AI and automated triage reduce IT workload and provide actionable insights, ensuring proactive defense.

We can't afford downtime for deployment.

Zivver deploys in under 30 minutes with no disruption to operations. As a fully cloud-based solution, it integrates seamlessly with Microsoft 365, delivering immediate protection with expert support throughout the process.



ON 350+ Detection Rules

Active threat scanning

Credential phishing ●

Extortion ●

BEC Fraud ●

05

Executive Summary

Microsoft 365 provides basic email security, but its focus on deliverability leaves critical gaps against advanced threats like phishing, BEC, and ransomware. Zivver addresses these blind spots with AI-powered detection, explainable insights, and customizable protection. Acting as a second layer of defense, Zivver enhances security, reduces IT burden, and empowers organizations to tackle the evolving cyber landscape with confidence.