CNEXT SECURITY SERVICES · MONTHLY REPORT · MONTHLY

Microsoft Defender monthly report

CUSTOMER
Muster AG, Bern (fictional)

REPORTING MONTH
October 2026

SCOPE
Defender for Office 365, Endpoint, Identity and Cloud Apps; 184 users, 203 devices

CONTACT AT CNEXT
Named in the real report

1'412	11	1	74 %
phishing and malware mails stopped before…	incidents reviewed	account blocked, the same evening	Secure Score, previous month 71%

When you receive this document: In the first week of every month, in operation.

Summary

In October Defender stopped 1,412 phishing and malware mails before they reached a mailbox. Of eleven incidents, seven were remediated automatically and we settled four with your IT. On Friday 17 October someone abroad signed in with the account of an accounting employee. We blocked the account at 19:42, reset the password and removed a new forwarding rule in the mailbox. No mail left the company.

Incidents we settled with your IT

DATE	INCIDENT AND MEASURE	SEVERITY	STATUS
3 Oct	Invoice with a macro sent to logistics, quarantined, sender blocked	**Medium**	Closed
17 Oct	Sign-in from abroad with an accounting account; account blocked, password reset, forwarding rule removed	**High**	Closed
24 Oct	Unknown program on a field sales laptop; isolated, identified as a supplier's remote support tool, released after checking	**Medium**	Closed
30 Oct	Upload of 2.3 GB to a private cloud storage; discussed with the head of department	**Low**	Settled

Open items

- Two laptops have not checked in with Defender for over 30 days; your IT is checking whether they are still in use.
- Recommendation: passkeys for the eight accounts with admin rights by the end of December.

Next steps

We go through the report with your IT in half an hour. Next report in the first week of November.

Every name, system and number in this document is invented. Your report contains your environment on the day of the check.