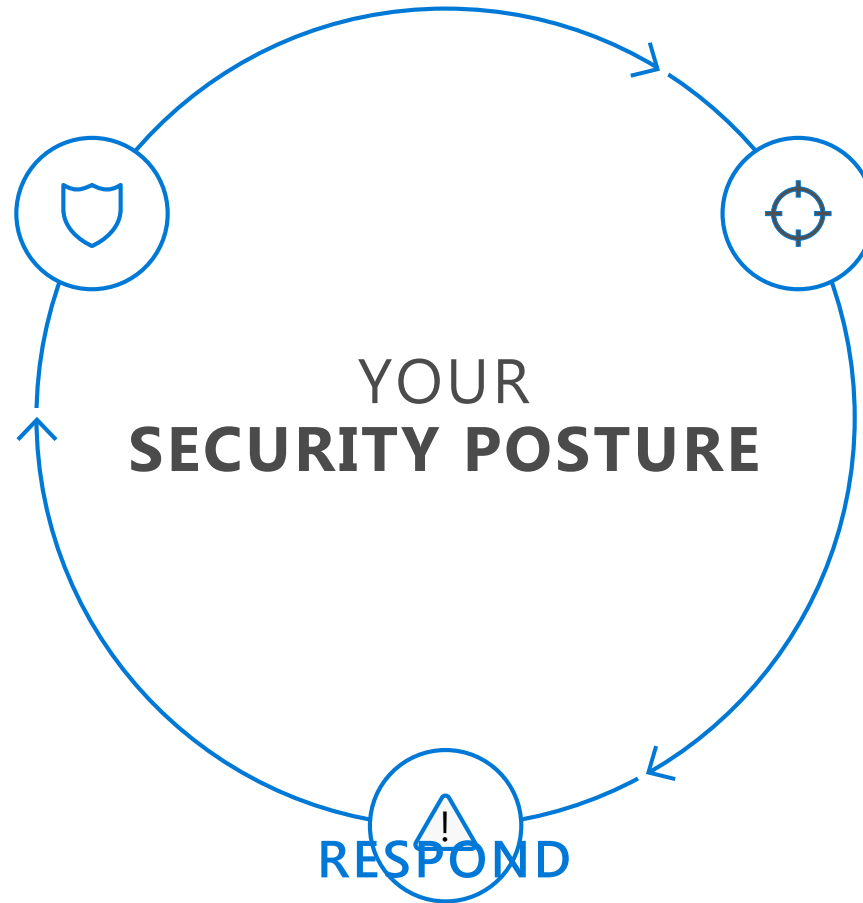


Security for the modern Hybrid Enterprise

Ralf Gomeringer
Threat Management TSP

PROTECT

across all endpoints, from sensors to the datacenter



closing the gap between discovery and action

DETECT

using targeted signals, behavioral monitoring, and machine learning

Cybersecurity Trends

- Identity is the new security perimeter
- Data is new currency
- Threat hunting is the new norm for IR

Secure Modern Enterprise

Monitoring & Reporting

**Identity & Access
Management**

Endpoint & Devices

**Application & Data
Management**

**Network &
Infrastructure**

Test, Audit & Compliance

Identity & Access Management

Data Protection / DLP

UEBA / ID Analytics

CASB

Identity Driven Security

Security Management

Endpoint & Devices

Data Protection / DLP

Advanced EPP / HIPS

Endpoint Detection & Response

Anti-Malware

E-Mail Protection

Identity Driven Security

Security Management

Application & Data Management

Data Protection / DLP

CASB

Identity Driven Security

Security Management

Network & Infrastructure

Data Protection / DLP

UEBA / ID Analytics

CASB

Advanced EPP / HIPS

Endpoint Detection & Response

Anti-Malware

E-Mail Protection

Identity Driven Security

Security Management

Data Protection / DLP

Office 365 DLP
Azure Information
Protection (AIP)
Windows Information
Protection (WIP)
Intune MAM

UEBA / ID Analytics

Azure AD Identity
Protection (IDP)
Advanced Threat Analytic
(ATA)
Azure Advanced Threat
Protection

CASB

Microsoft Cloud App
Security (MCAS)

Advanced EPP / HIPS

Windows Defender Exploit
Guard ASR
Windows Defender
Application Control
Windows Defender
Application Guard

Endpoint Detection & Response

Windows Defender
Advanced Threat
Protection (WDATP)

Anti-Malware

Windows Defender
Antivirus (WDAV)

E-Mail Protection

Office 365 Exchange
Online Protection (EOP)
Office 365 Advanced
Threat Protection (ATP)
Office 365 Threat
Intelligence

Identity Driven Security

Azure Multi Factor
Authentication
Azure AD Conditional
Access
Azure AD Privileged
Identity Management

Security Management

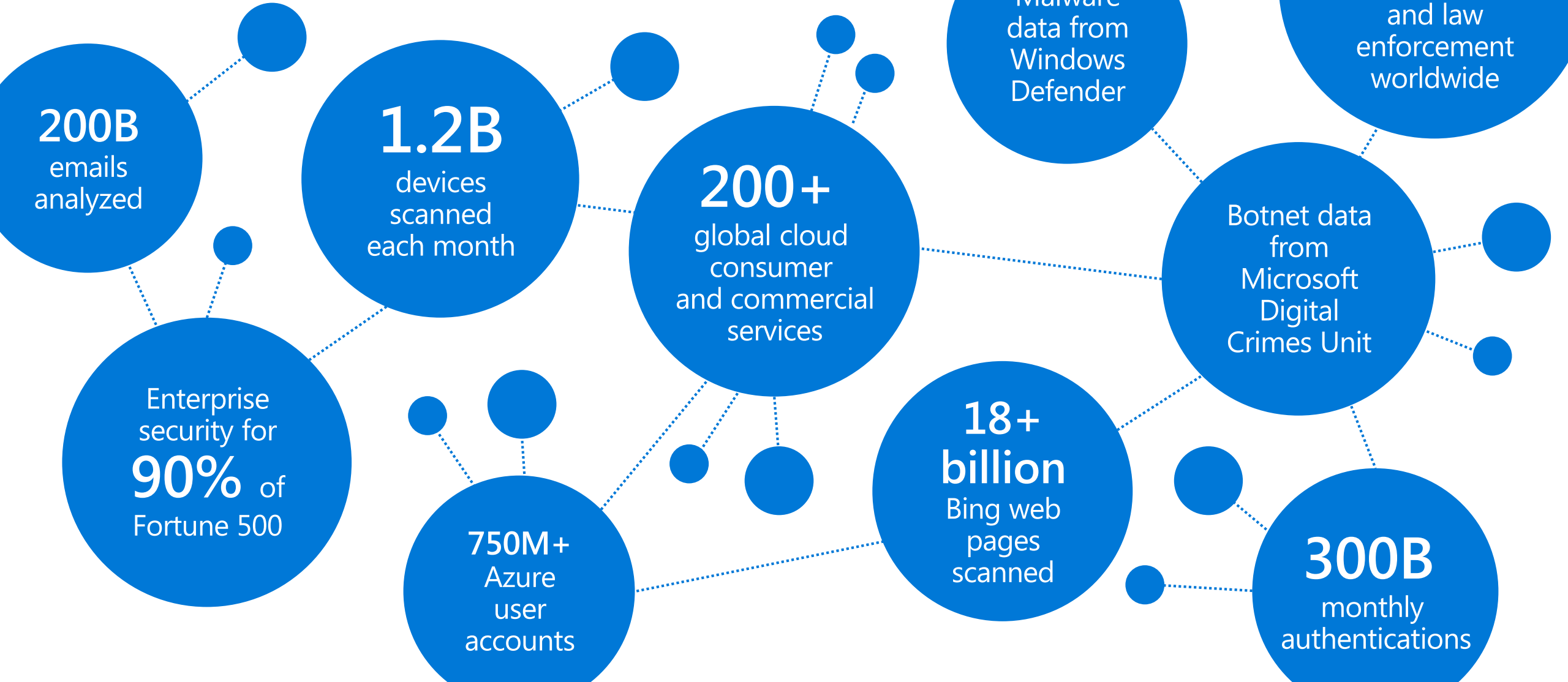
Microsoft Intune
Microsoft System Center
Configuration Manager
Azure Operations
Management Suite
Azure Security Center

Acronyms for reference

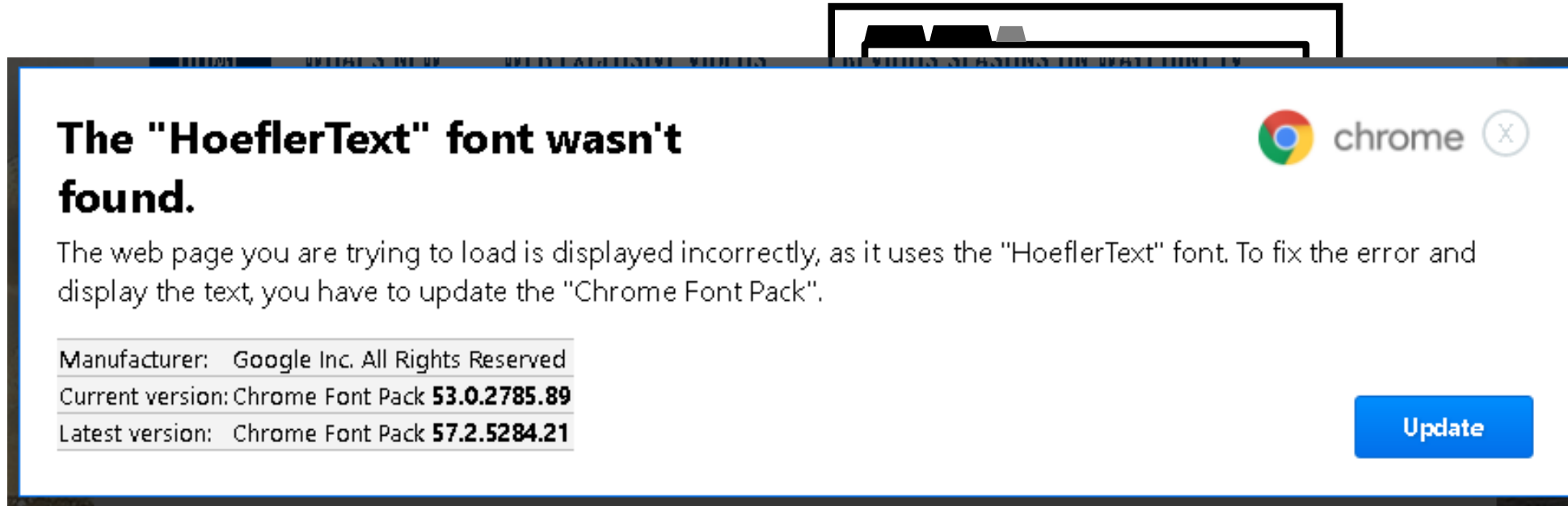
- [AIP: Azure Information Protection](#)
- [ATA: Advanced Threat Analytics](#)
- [AppLocker \(Windows 10\)](#)
- [AzATP: Azure Advanced Threat Protection](#)
- [CA: Conditional Access](#)
- [Client Hardening \(Reference to Sec. Baselines\)](#)
- [IDP: Identity Protection](#)
- [LAPS: Local Administrator Password Solution](#)
- [MCAS: Microsoft Cloud App Security](#)
- [MFA: Multi Factor Authentication \(Azure AD\)](#)
- [O365ATP: Office 365 Advanced Threat Protection](#)
- [O365DLP: Office 365 Data Loss Prevention](#)
- [O365 TI: Office 365 Threat Intelligence](#)
- [PAW: Privileged Access Workstation](#)
- [PIM: Privileged Identity Management](#)
- [WD: Windows Defender \(EPP\)](#)
 - [SmartScreen](#)
 - [WDATP: Windows Defender Advanced Threat Protection](#)
 - [WDAV: Windows Defender AntiVirus](#)
 - [WDAC: Windows Defender Application Control](#)
 - [WDCG: Windows Defender Credential Guard](#)
 - [WDDG: Windows Defender Device Guard](#)
- [WDEG: Windows Defender Exploit Guard](#)
 - [WDEG ASR: Attack Surface Reduction](#)
 - [WDEG EP: Exploit Protection](#)
 - [WDEG NP: Network Protection](#)
 - [WDEG CFA: Controlled Folder Access](#)
- [WHfB: Windows Hello for Business](#)
- [WIP: Windows Information Protection](#)

Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



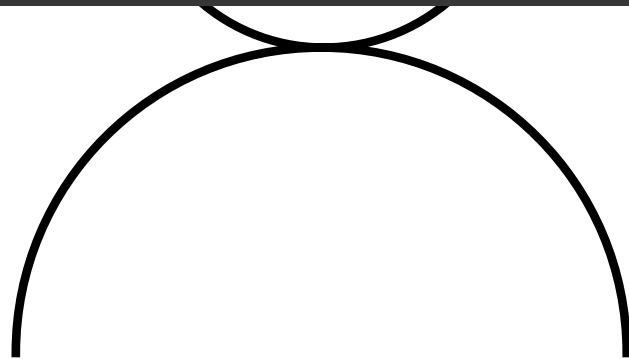
The story of Bob



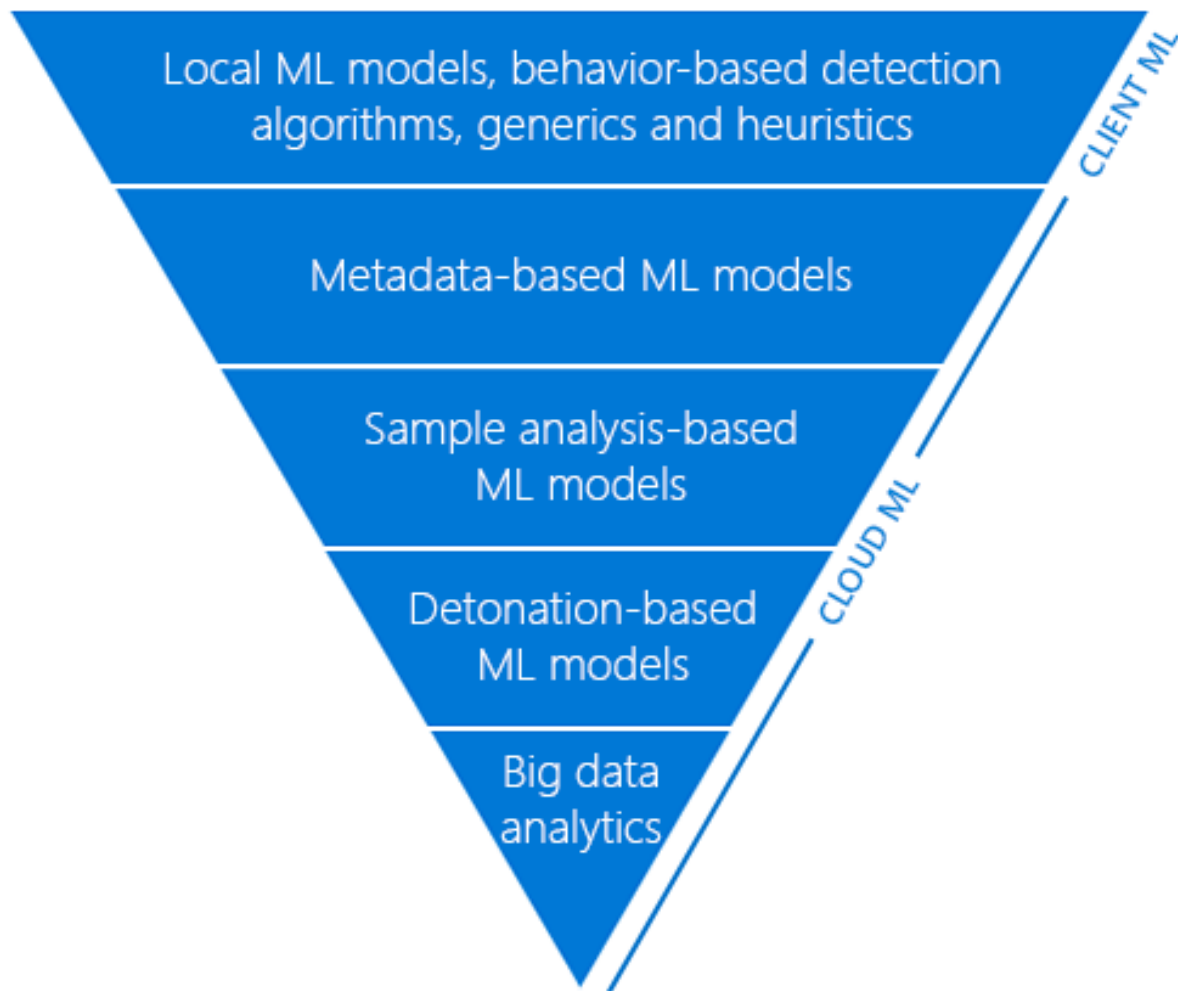
The screenshot shows a Chrome browser error message. At the top right, there is the Chrome logo and the word 'chrome' with a close button (X). The main heading reads 'The "HoeflerText" font wasn't found.' Below this, a paragraph explains that the web page is displayed incorrectly because it uses the 'HoeflerText' font, which is not in the Chrome Font Pack, and that the user must update the font pack. On the left side, there is a table with font information. On the right side, there is a blue 'Update' button.

| | |
|------------------|--------------------------------------|
| Manufacturer: | Google Inc. All Rights Reserved |
| Current version: | Chrome Font Pack 53.0.2785.89 |
| Latest version: | Chrome Font Pack 57.2.5284.21 |

[Update](#)



The WDAV detection funnel



Protection in milliseconds

Most common malware are blocked by high-precision detection in Windows Defender AV

Protection in milliseconds

ML-powered cloud rules evaluate suspicious files based on metadata sent by the Windows Defender AV client during query

Protection in seconds

A copy of the suspicious file is uploaded for inspection by multi-class ML classifiers

Protection in minutes

The suspicious file is executed in a sandbox for dynamic analysis by multi-class ML classifiers

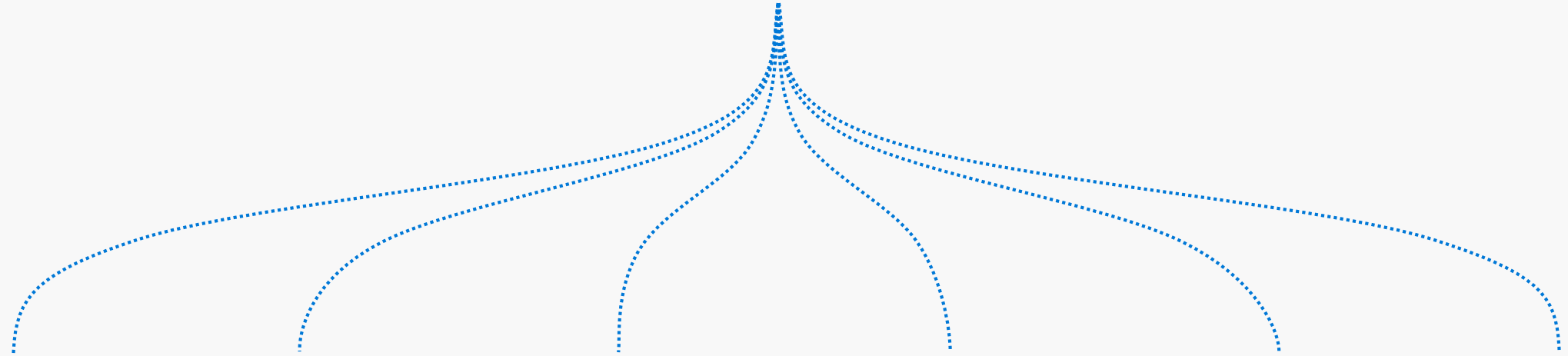
Protection in hours

ML models and expert rules correlated signals from a vast network of sensors to automatically classify threats



Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations



NEXT GENERATION PROTECTION

Protect against all types of emerging threats



ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks



AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale



SECURITY POSTURE

Track and improve your organization security posture



ADVANCED HUNTING

Advanced threat hunting

Management and APIs

Automation and Response

The introduction of automation in WDATP enables security operations team to quickly and effectively deal with the increasing load of security incidents by automating the investigation and remediation process

With Hexadite AIRS, WDATP will be the only endpoint security solution in the market using AI technology to automatically investigate incidents mimicking the same actions a skilled human analyst will take

The screenshot displays the Windows Defender Security Center interface. The main alert is titled "Process privilege escalation due to kernel exploit (17386)" with a status of "Investigation Completed - Fully Remediated". The alert severity is "High" and the category is "Privilege Escalation". The detection source is "Windows Defender ATP" and the data source is "WDATP Graph-API". The remediation tools used are "Windows Firewall" and "Windows Defender Antivirus".

The "Investigation details" section on the left provides the following information:

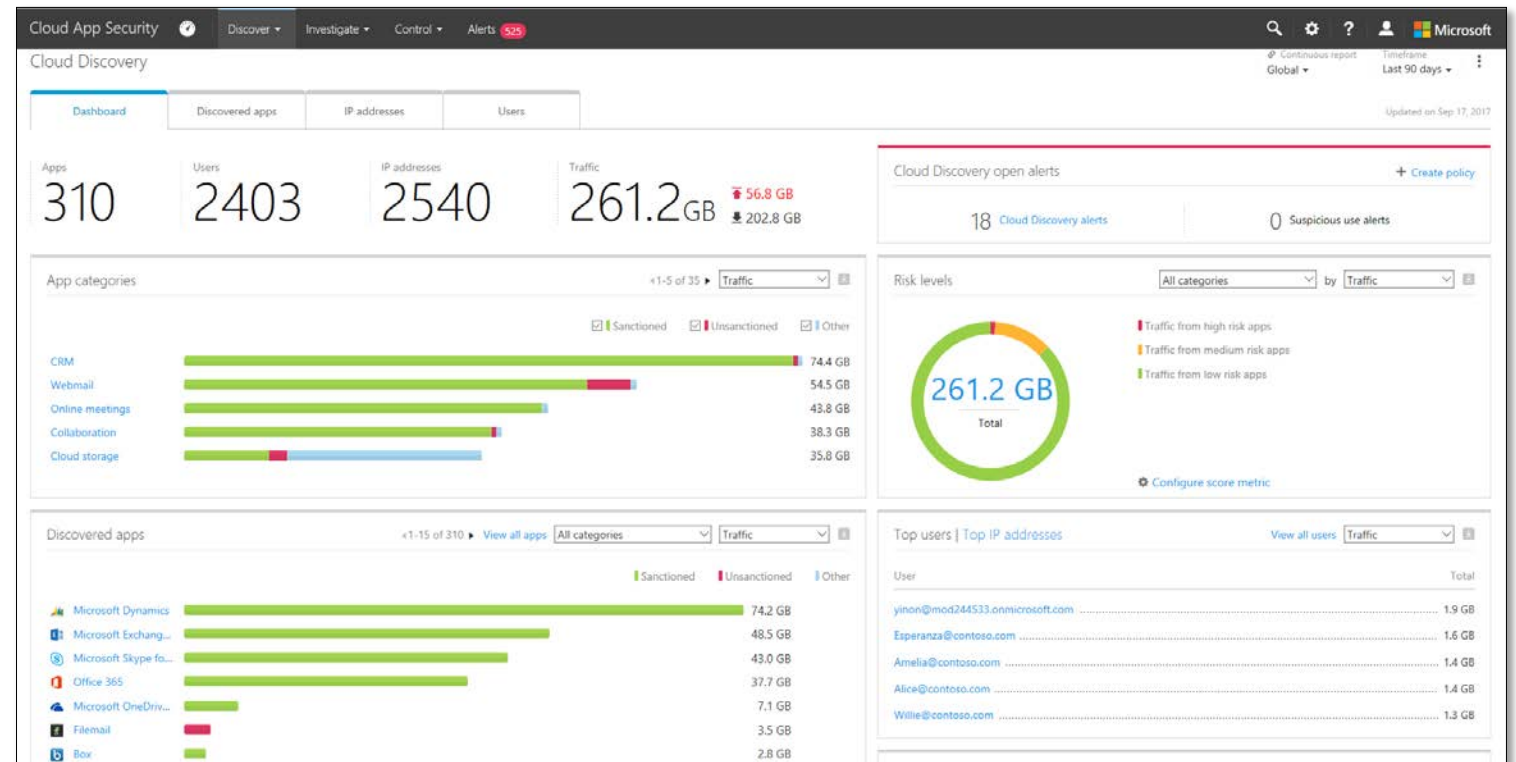
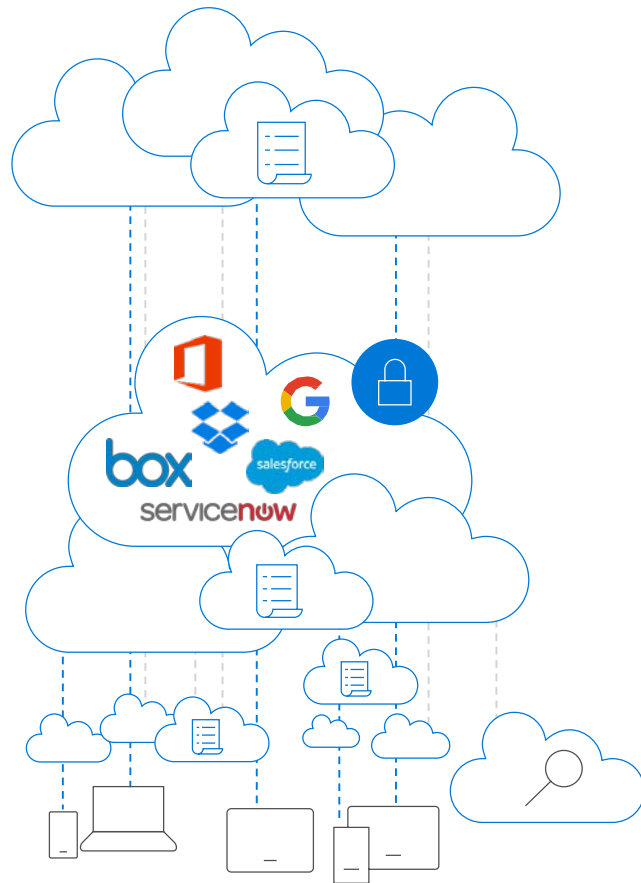
- Name: Communication to a malicious network destination
- ID: 17386
- Status: Fully remediated
- Alert severity: High Exploit
- Category: Privilege Escalation
- Detection source: Windows Defender ATP
- Data source: WDATP Graph-API
- Remediation tools: Windows Firewall, Windows Defender Antivirus

The "Investigation time" section shows a circular progress indicator for the investigation, which is completed. The investigation started on 9/15/2017 at 12:46 PM and ended at the same time. The total time taken was 00:01:23. A pending time of 35 minutes is also indicated.

The "Investigation graph" section on the right shows a network diagram of the investigation. The central node is a laptop representing the machine, which is marked as "Fully Remediated". It is connected to a user node labeled "Jonathan Wolcot Dev 2" and "Jacob Gall Dev 2". The machine node is also connected to several other nodes: "Windows Defender ATP Exploit", "cont-jonathanw Important Machine", "cont-jecobgall", "2257 Files 2 Remediated", "84 Processes 2 Remediated", and "10 IP addresses 1 Remediated".

Microsoft Cloud App Security

A comprehensive, intelligent security solution that brings the visibility, real-time control, and security you have in your on-premises network to your cloud applications.



Discover

Control

Protect

Integrates with your SIEM, Identity and Access Management, DLP and Information Protection solutions

How Microsoft CAS works

Discovery

Use traffic logs to discover and analyze which cloud apps are in use. Manually or automatically upload your firewall and proxy log files for analysis.

Sanctioning and un-sanctioning

Sanction or block apps in your organization using the cloud app catalog.

App connectors

Leverage APIs provided by various cloud app providers to extend protection to Cloud App Security.

Proxy apps

Azure AD redirects risky sessions to the reverse proxy to apply app restrictions

