

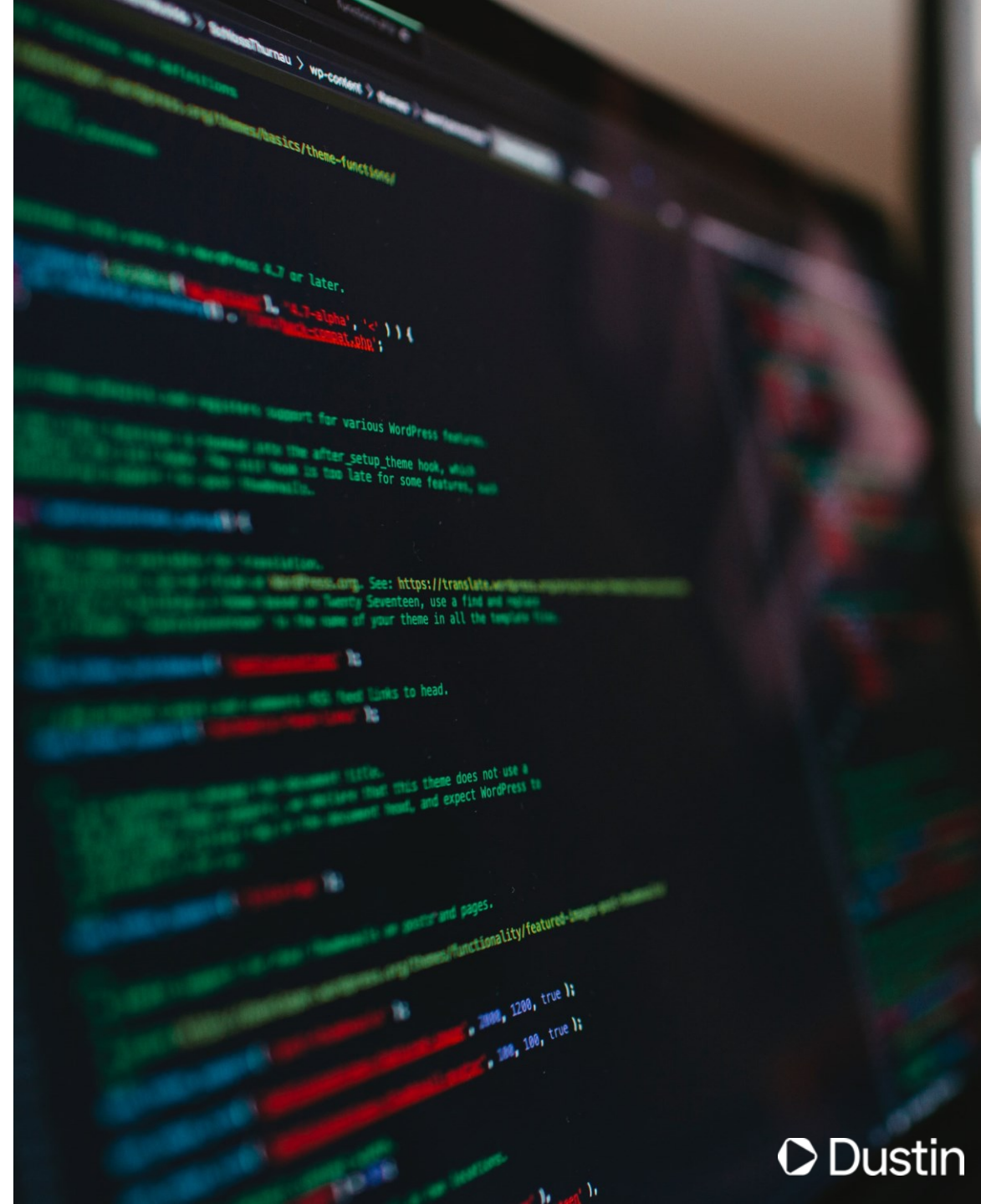
Managed Detection & Response

► Dustin

Threat Landscape

1. Threat Actors Are Faster
2. It's Too Easy to Get Full Control of a Network
3. Increased Use of Vulnerability Exploits
4. Passwords Are Not Enough
5. Dependencies Can Be Exploited
6. Denial of Service Attacks Are Increasing
7. Large Flat Networks Are Easy to Exploit

Source: Truesec 2022 Threat Intelligence Report



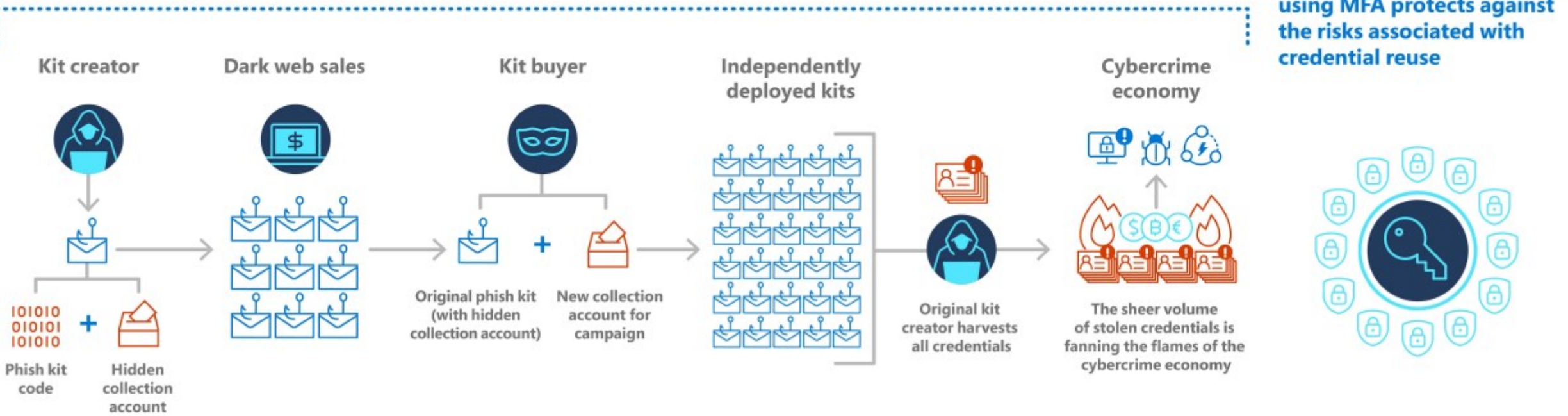
Threat Landscape - Phishing

66\$



250\$

Phish kits: enabling credential harvesting at scale



Phish kit creator writes code that allows phish kit to be configured by kit buyer to indicate collection account where phished credentials are sent. Also included in code is a hidden collection account that will also receive phished credentials.

Phish kits are sold on the dark web. Each kit buyer configures the kit to meet their phishing campaign needs, including their own collection account to receive phished credentials.



Who's phishing whom?
Kit creators have expertise and resources to carry out more sophisticated and targeted attacks at scale.

Each kit buyer deploys their own campaign. Phished credentials are delivered to both the kit buyer and the kit creator.

Lists of newly harvested credentials feed more targeted attacks at scale.

Even well-protected organizations can become victims of more costly attacks exploiting credential reuse if not using MFA.

30,720

Potential new domains generated by DGAs in just 3-4 days

Threat Landscape

How quickly do you discover a hacked server and what do you do!

Detection & Response

Proactive protection against cyber attacks,
around the clock



Powered by Truesec

Comprehensive protection

50% of small and medium-sized enterprises have experienced a cyber attack in recent years. As the methods become increasingly advanced, and we work from different locations, it is absolutely crucial to have a security solution that protects you from the human factor. At the same time, it can be expensive and difficult to find the right skills in IT security.

To solve this, we have created a security service that allows even **small and medium-sized companies** to receive professional protection against data breaches. Together with the **Truesec**, we can offer market-leading expertise that was previously only available to larger companies with their own IT department. You get comprehensive protection against, for example, phishing, ransomware and other types of intrusion.



This is part of the service:

- ✓ 24/7 incident handling
- ✓ Investigation of incident
- ✓ Security automations
- ✓ **Safety recommendations**
- ✓ Fixed price per employee per month

What does the service mean?

When we detect an abnormal behavior or attack, we stop it right away. We will then send you an incident report and carry out an investigation of what has happened. Your business can continue as usual because we monitor proactively.

What are the benefits of Detection & Response?

Detect & Response is a managed service, which means that we monitor your system 24/7. Whether you are exposed once or a thousand times, we stop a data breach before a disaster is a fact. There are no limits to how much data we can monitor or how many incidents we handle. Rather, the more data we have access to, the better the security.

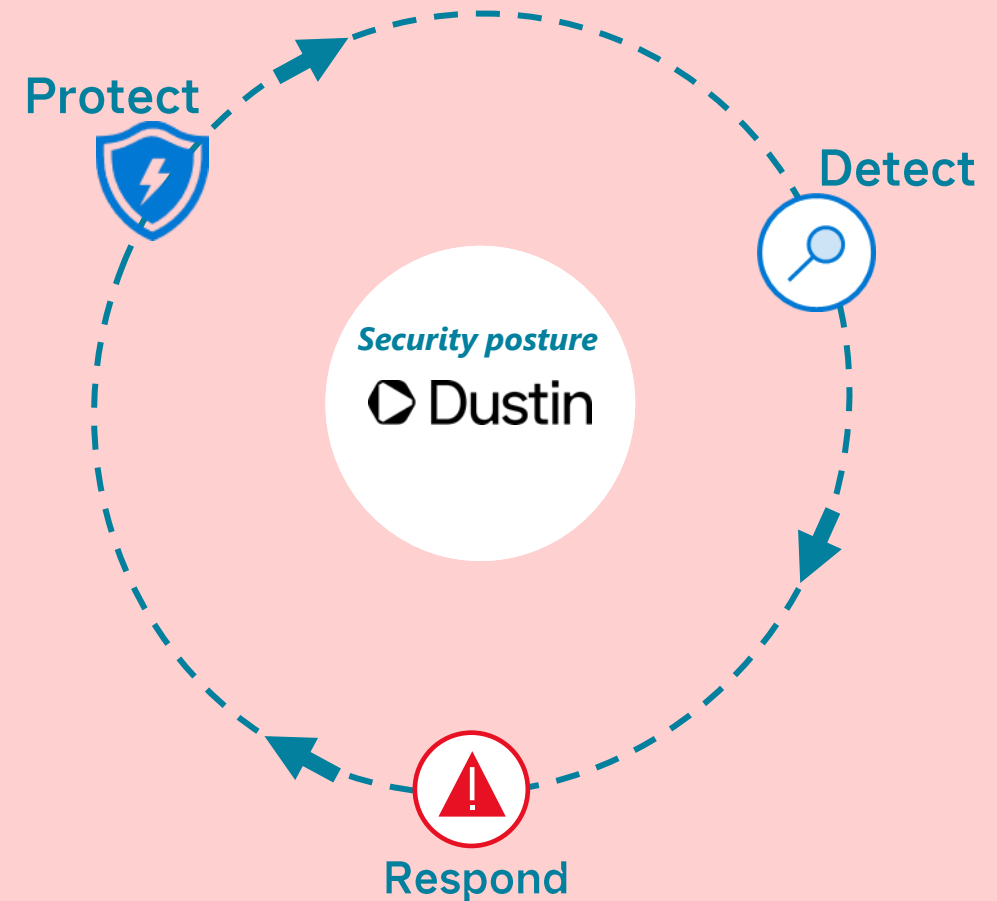
You get predictable and scalable costs with a fixed price per user per month. A legitimate investment considering how much a single breach can cost in time, money and loss of personal data.

Detection and Response

Managed Detection and Response security solution is built on top of the **Microsoft Security stack** and uses standard components. The standard features used in the offering are Microsoft Defender and Microsoft Sentinel.

- Protect - Enhanced Endpoint Protection
- Detect - Detection and Response
- Response – 24/7 Incident Response

Powered by **TRUESEC**



Detection and Response

Information is the key to a good cybersecurity defense, and to give the best protection for the customer, Microsoft Defender and **Microsoft Sentinel** work great together.

The more Security data send to Microsoft Sentinel, the better protection we can give the customer. Our recommendation is to have the whole Microsoft 365 Defender suite set up to provide 360-degree protection within the customer's cloud infrastructure.

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender Cloud App
- Microsoft Defender for Cloud



Why Microsoft

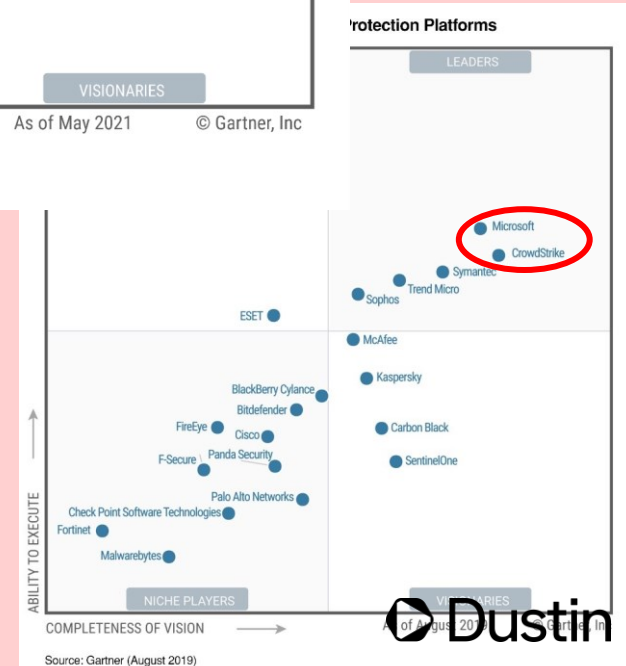
All of these innovations are seamlessly built into Microsoft 365 Defender, our solution offering XDR capabilities for identities, endpoints, cloud apps, email, and documents. Microsoft 365 Defender delivers intelligent, automated, and integrated security in a unified SecOps experience, with detailed threat analytics and insights, unified threat hunting, and rapid detection and automation across domains—detecting and stopping attacks anywhere in the kill chain and eliminating persistent threats.

- Delivering the best of breed in endpoint security
- Offering security for all devices and platforms
- Enabling org. to rapidly improve their security
- Extending endpoint security capabilities

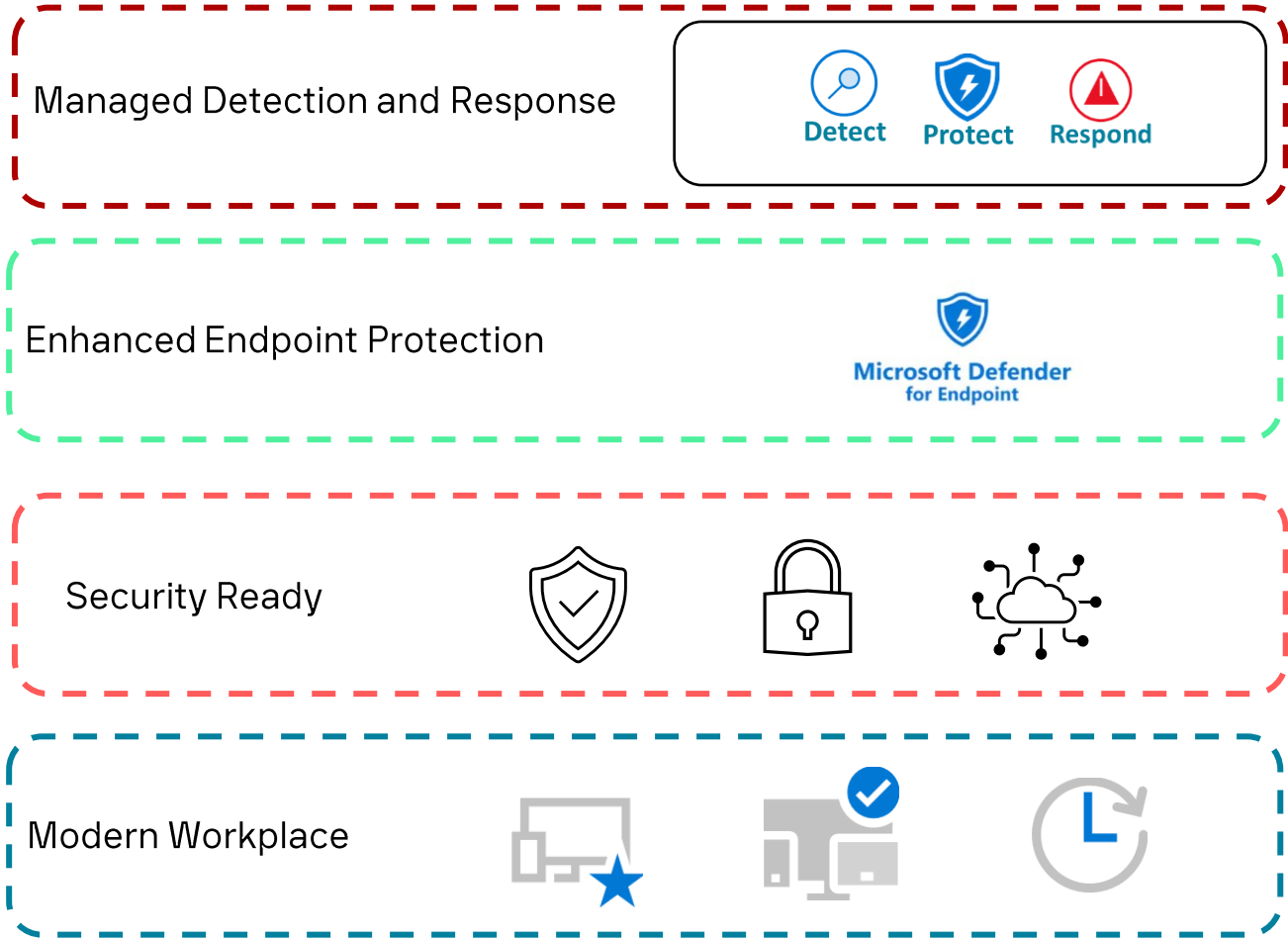
Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (May 2021)



Modern Workplace customer



- **24/7 Incident Response**
 - Incident Investigation
 - Security automations
 - Incident reporting
 - Security recommendations
 - Fixed fee per user per month
- **Based on Defender for Endpoint**
 - Support and management
 - Automated response
 - Security optimized configuration
 - Advance security policy
 - Fixed fee per user per month
- Endpoint management
 - Security Defaults
 - Build on Zero Trust
 - Based on Microsoft 365
 - Enhanced Security
 - **Continuous security enhancement**
- Based on Microsoft 365
 - Support and management
 - Zero Touch Deployments
 - Device management
 - Basic Security

Assessments – The first touch



Modern Workplace Ready Assessment

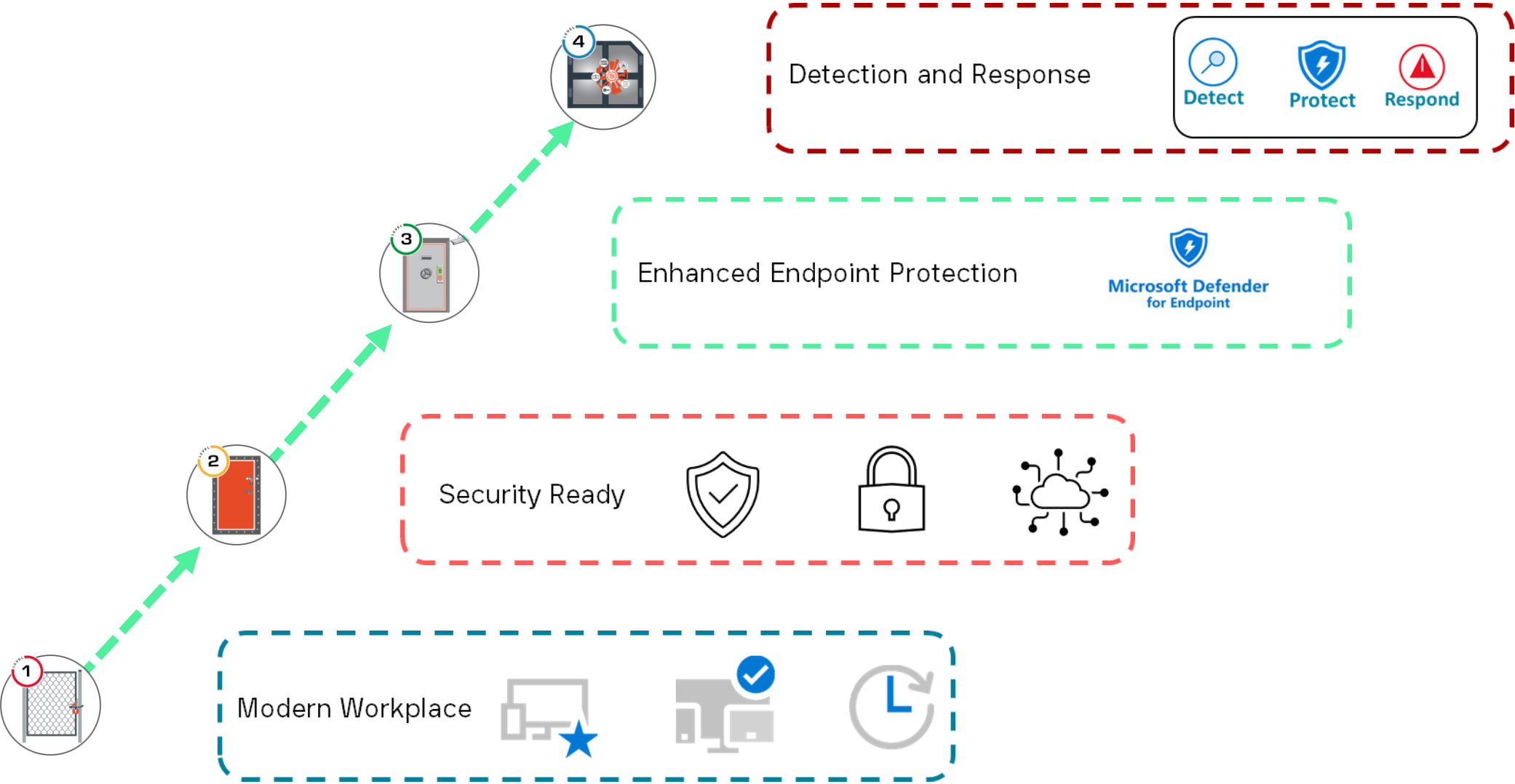


Microsoft 365 Security Essentials












Microsoft 365 Security Advanced

Security offering and implementation





Security options

	Modern Workplace	Modern Workplace + Enhanced Security	Modern Workplace + Enhanced Security + Detection & Response
 Productivity tools			
 Collaboration			
 Basic security			
 Security ready			
 Enhanced Endpoint Protection			
 Managed Detection and Response			
 Device management			
 Device of your choice*			
 Support and management			
 Fixed fee user/month			

*Not included in monthly fee

Why Dustin and Truesec

TRUESEC

- Custom and optimized IOC (Indicator of compromise)
- Threat intelligence based on large data insight
- EU based company
- Dustin and Truesec Build together
- There are no limits to how much data we can monitor or how many incidents we handle
- Unique' way of approaching Cybersecurity
- Threat Hunting on all Customer



Cybersecurity. That's what we do!

Security Recommendations 2022*

1. Protect all Workloads
2. Stop Modern Attacks
3. Adopt Zero Trust
4. Eliminate Misconfigurations
5. Invest in Elite Threat Hunting
6. Be Ready and know who to call

Modern Workplace

Security Ready

Enhanced Endpoint Protection

Manage Detection and Response

* Gartner Identifies Top Security and Risk Management Trends for 2022

Why Managed Security

Proactive cyber security services around the clock

Summary

- Build on Microsoft Security stack
- 24/7 Incident Response
- Based on Defender for Endpoint
- Continuous security enhancement
- Global cybersecurity Partner
- Safety recommendations

