cprime

Case Study

Helge Heupel GmbH Doubles Cybersecurity Readiness With Cprime

HH HELGE HEUPEL

cprime.com | 877.800.5221 (US) | +44 (0) 203 811 0424 (UK)

Company Details

Industry: Automotive Software Supplier

Location: Germany

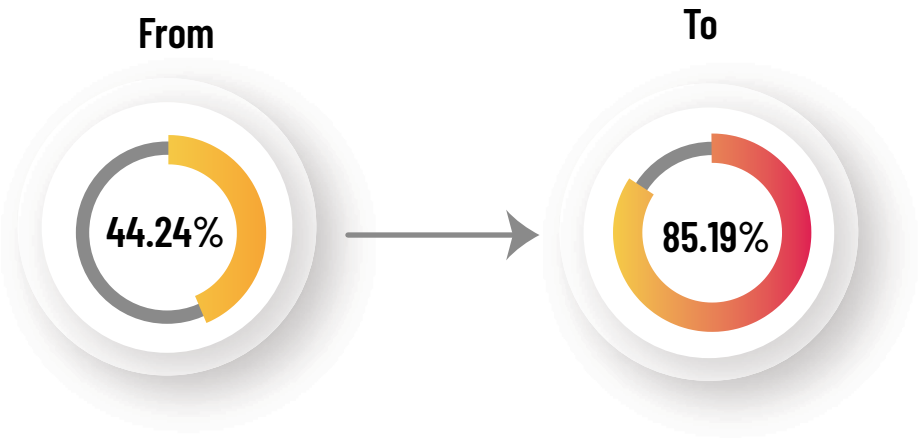
Cprime Services: Security as a Service

Executive Summary:

Cprime consultants helped Helge Heupel increase their Microsoft Defender Secure Score from 44.24% to 85.19%, ensuring compliance with regulations like GDPR and ISO standards. This improvement also enhanced cybersecurity, protecting the company from costly cyber attacks.

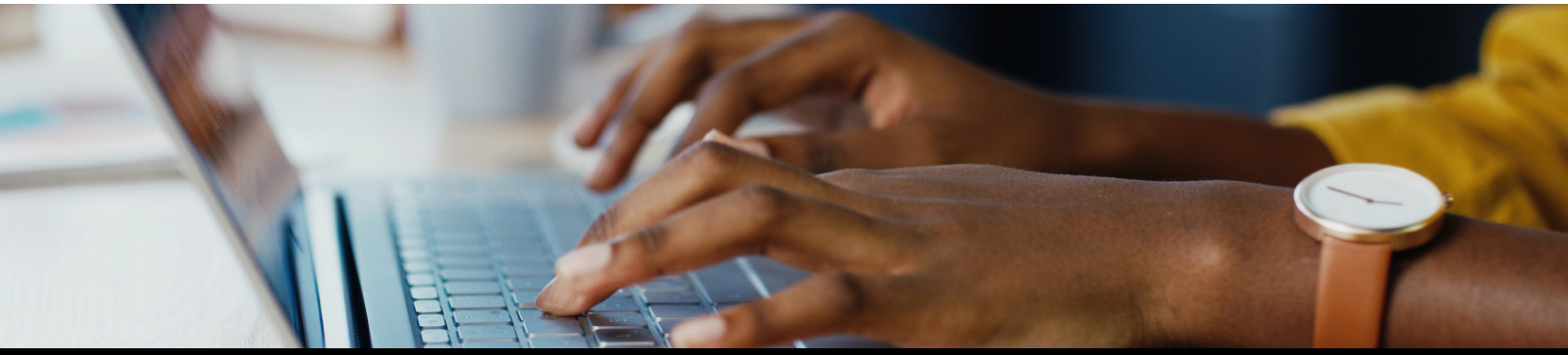
The automotive industry is subject to various regulatory frameworks, such as GDPR, HIPAA, and ISO standards. Increasing Secure Score—a widely-recognized cybersecurity metric found within the popular Microsoft Defender 365 solution—ensures compliance with these regulations by implementing recommended security controls and best practices. Beyond legal compliance, a high Secure Score means the company is protecting itself from potentially harmful and expensive cyber attacks, saving valuable time, money, and brand reputation.

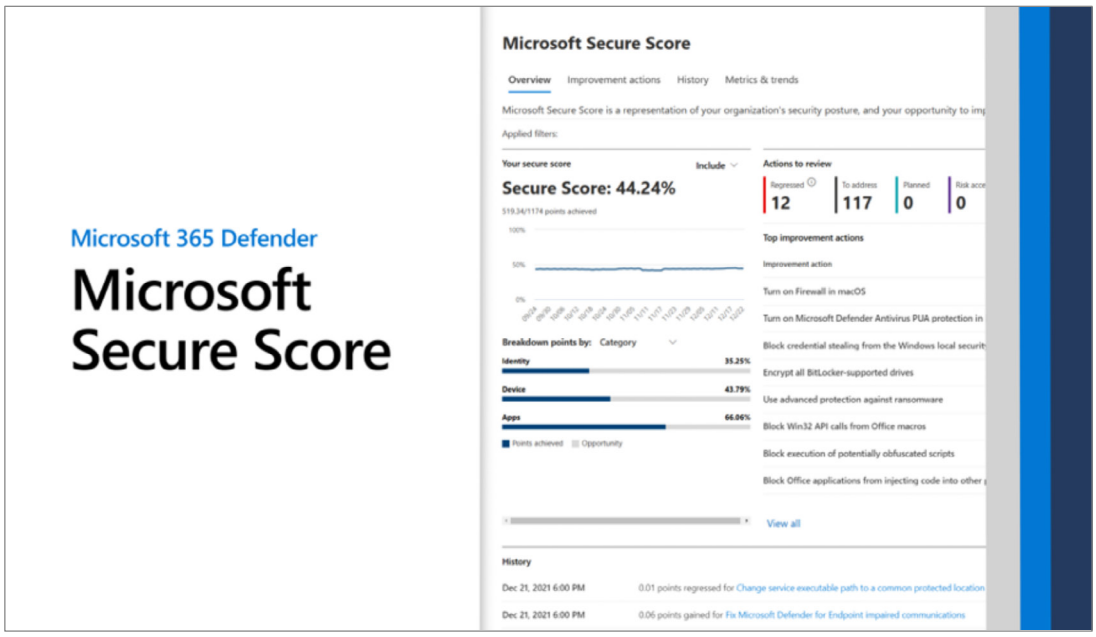
The case study documents the dramatic increase one automobile software solution company realized in its Secure Score with the help of Cprime consultants:



Driving Toward More Secure Automotive Software

Helge Heupel GmbH, a leading automobile software solution company wanted to boost customer confidence, and protect data and system security by enhancing its Secure Score within Microsoft Defender 365. Secure Score is a pivotal metric reflecting an organization's security posture, measured through the implementation of recommended security actions.





Why would a company want to increase its Secure Score?

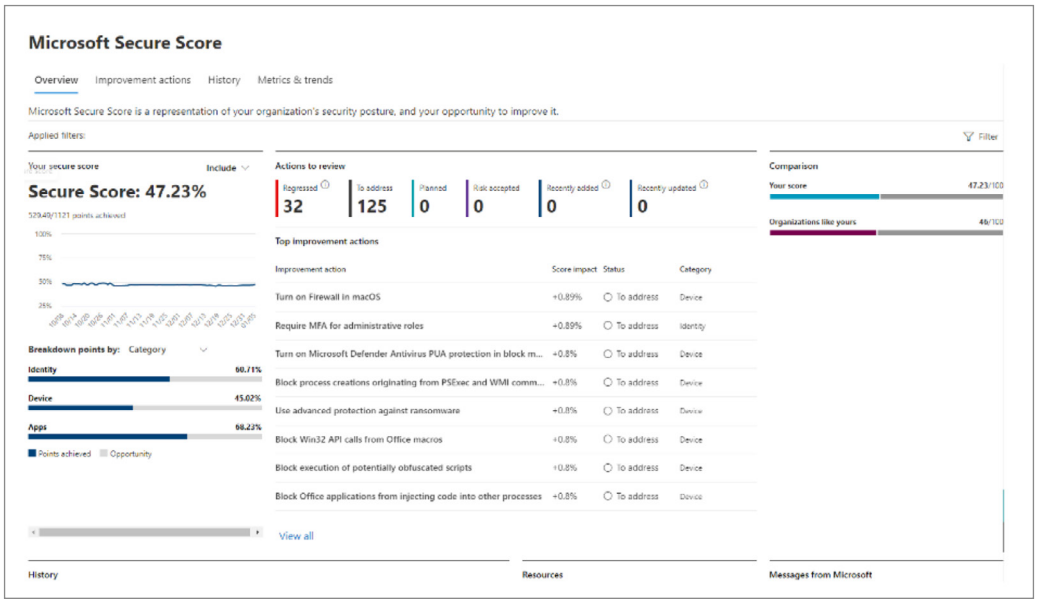
An automotive software company, like any other organization, would have several compelling reasons to increase its Secure Score in Microsoft 365. Here are some key motivations: Protection of Sensitive Data: Automobile companies deal with a vast amount of sensitive data, including proprietary designs, customer information, and manufacturing processes. Enhancing Secure Score helps in safeguarding this data against unauthorized access, data breaches, and cyber threats.

- **Regulatory Compliance**: The automotive industry is subject to various regulatory frameworks, such as GDPR, HIPAA, and ISO standards. Increasing Secure Score ensures compliance with these regulations by implementing recommended security controls and best practices.
- **Prevention of Intellectual Property Theft**: Automobile companies invest heavily in research and development to innovate new technologies and designs. A higher Secure Score mitigates the risk of intellectual property theft by strengthening data protection measures and access controls.
- **Protection of Customer Trust**: Automobile companies rely on customer trust and loyalty to maintain their market position. By increasing Secure Score, companies demonstrate their commitment to safeguarding customer data and protecting their privacy, thereby enhancing brand reputation and trust.

- **Mitigation of Operational Risks**: Cyberattacks and data breaches can disrupt manufacturing processes, supply chains, and customer services, leading to significant operational and financial losses. Improving Secure Score helps in mitigating these risks by fortifying security defenses and incident response capabilities.
- **Partnership and Supplier Requirements**: Automobile companies often collaborate with various partners, suppliers, and vendors across the supply chain. Increasing Secure Score may be necessary to meet contractual obligations, security requirements, and third-party audits imposed by partners and suppliers.
- **Competitive Advantage**: In today's digital landscape, cybersecurity is increasingly becoming a differentiator for businesses. Automobile companies with a high Secure Score can leverage this as a competitive advantage to win contracts, partnerships, and customers who prioritize security in their procurement decisions.

The Story

When Helge Heupel called Cprime in to assist, they were at a baseline Secure Score of 44.24 percent—a number right in line with most software organizations in the automotive and similar industries. It indicated they had taken many of the usual steps to make their systems secure, but that there was plenty of room for improvement; there was still a significant gap in the overall security posture.



(Snapshot taken after some improvements had been made. Original baseline was 44.24%.)

The Goal: Raise the Secure Score to 75% or Better

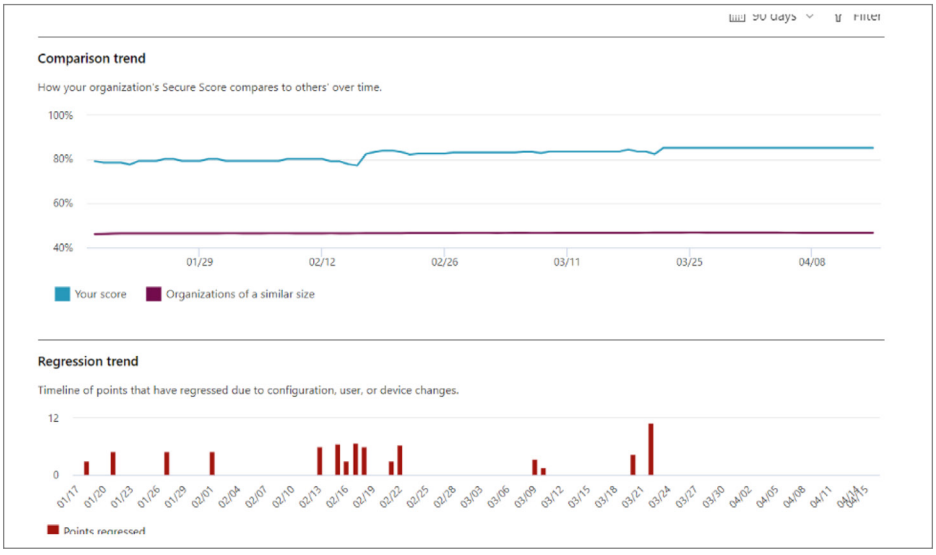
The primary objective was to elevate the Secure Score to the maximum achievable number, signifying robust implementation of security controls and adherence to industry best practices. An initial goal was 75%, which would have put this automotive supplier ahead of most organizations in their industry. We also established a stretch goal of 85%, seeking out as many value-add improvements as we could reasonably make.

Methodology and Action

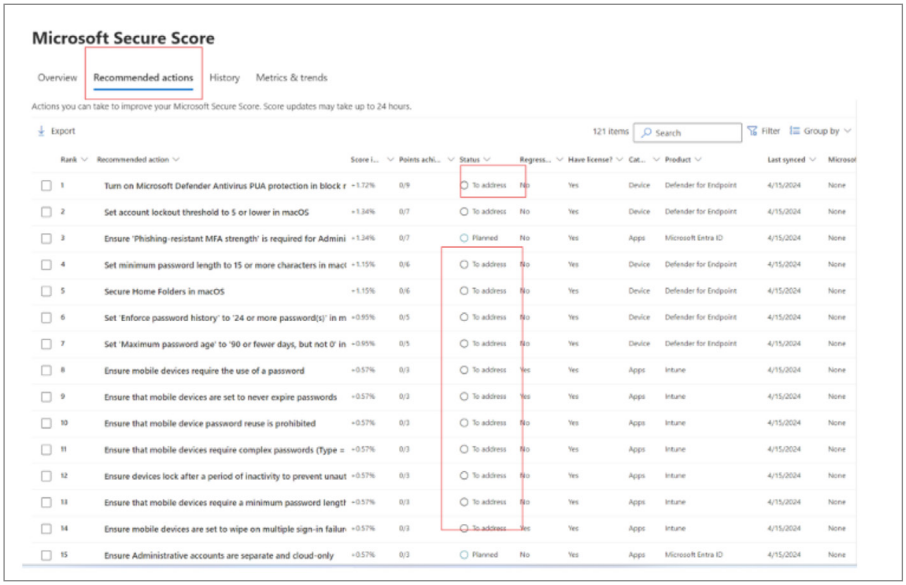
Collaborating with the company, Cprime consultants followed a structured approach to enhance their Secure Score:

1. **Assessment and Analysis**: Comprehensive evaluation of existing security configurations to identify vulnerabilities and gaps.

2. **Secure Score Benchmarking**: Comparison of Secure Score against industry standards and Microsoft recommendations to determine necessary improvements.



3. **Prioritization**: Determining which improvements were both immediately doable and would have the greatest impact on improving the Secure Score, allowing us to affect the greatest improvement as quickly as possible.
4. **Recommendation Implementation**: Diligent execution of recommended security enhancements across various domains including Identity, Data, Devices, Infrastructure, and Apps.

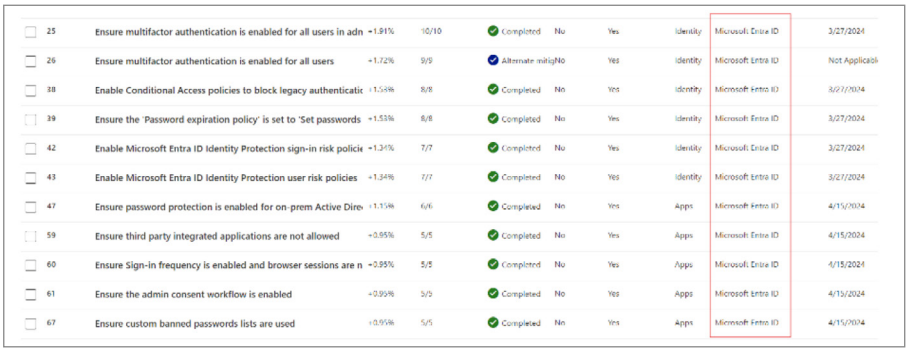


5. **Policy Enforcement**: Implementation of stringent security policies governing access control, data handling, and incident response.

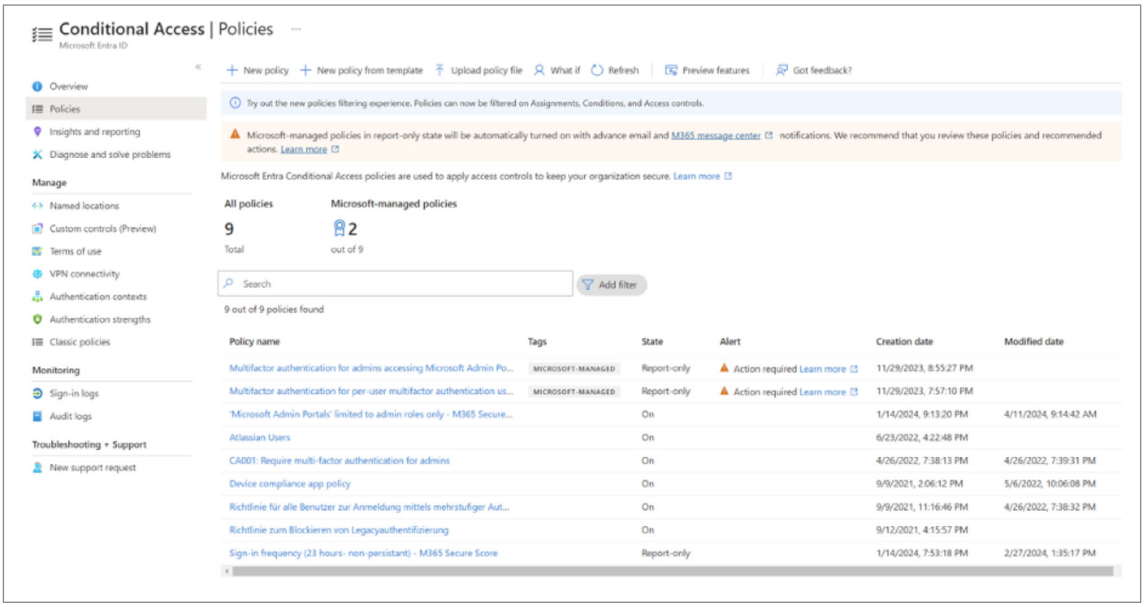
What follows are examples of areas we addressed to achieve the 85% Secure Score..

Security Improvement in Action

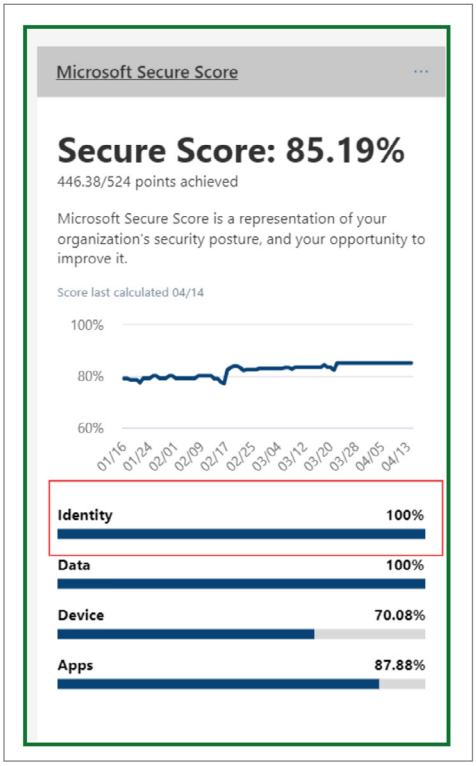
The following recommendations were targeting 'Microsoft Entra ID' the Identity and Access avenue of an organization.



In order to achieve robust security in this area, we followed the recommendations and implemented nine policies governing things like multifactor identification, personal device usage, and strictly limiting admin access.

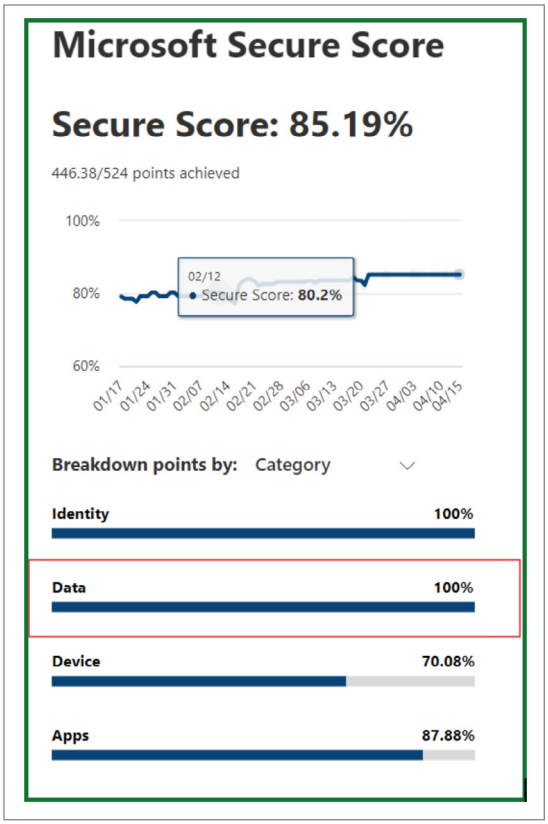


As a result, we achieved a 100% Score on the Identity.



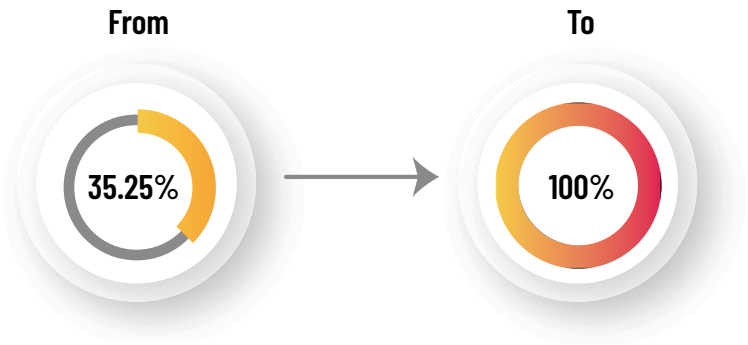
We enforced the following Data Protection Policies to achieve a 100% Score on Data as well:

- **Data Encryption**: All sensitive data, both in transit and at rest, is encrypted using industry-standard encryption algorithms. This includes data stored in databases, files shared internally or externally, and data transmitted over networks.
- **Data Classification**: A data classification policy is implemented to categorize data based on its sensitivity level (e.g., public, internal, confidential, or restricted). This helps in applying appropriate security controls and access restrictions based on the sensitivity of the data.
- **Data Retention and Disposal**: A data retention policy defines how long different types of data should be retained based on regulatory requirements, business needs, and legal obligations. Data that is no longer required is securely disposed of using methods such as shredding or secure deletion.
- **Data Loss Prevention (DLP)**: DLP policies are implemented to prevent the unauthorized sharing or leakage of sensitive data. This includes monitoring outbound communications, detecting sensitive data patterns, and blocking or alerting on unauthorized data transfers.

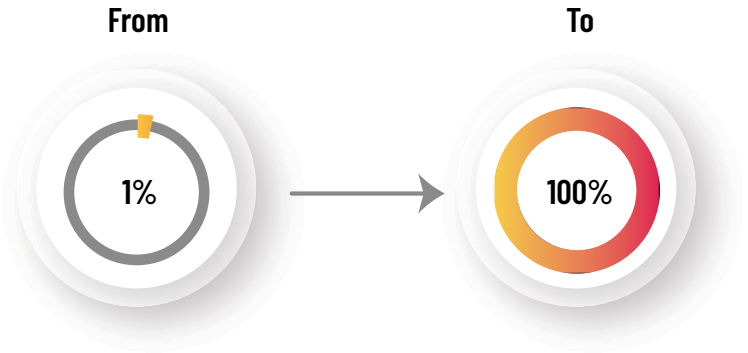


In all, we made improvements across all the Secure Score components:

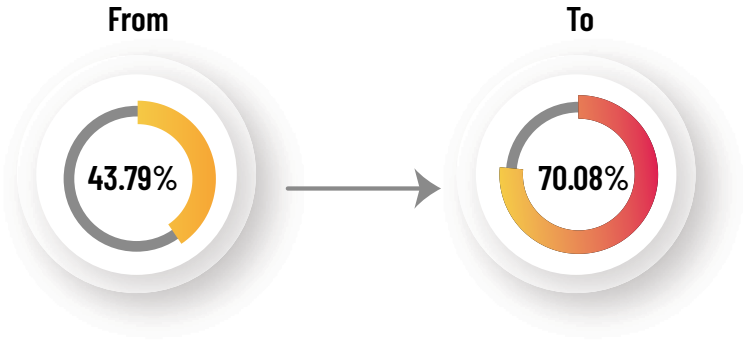
- **Identity**: Strengthened authentication mechanisms, enforced multi-factor authentication, and minimized privileges.



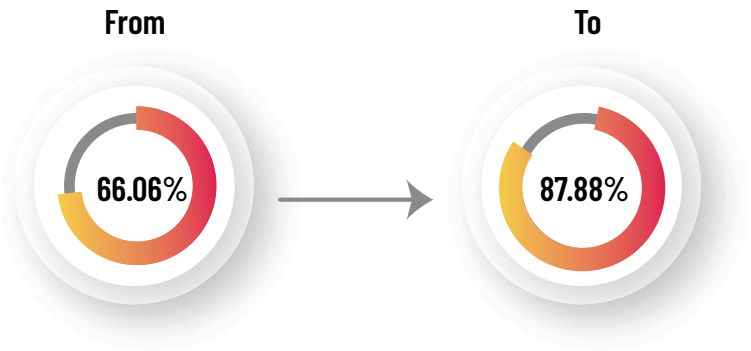
- **Data**: Enhanced data encryption, implemented data loss prevention policies, and restricted unauthorized access.



- **Devices**: Enforced device encryption, deployed endpoint detection and response solutions, and ensured compliance with security baselines.

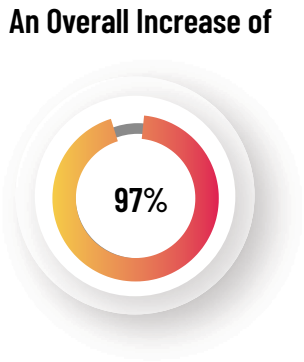


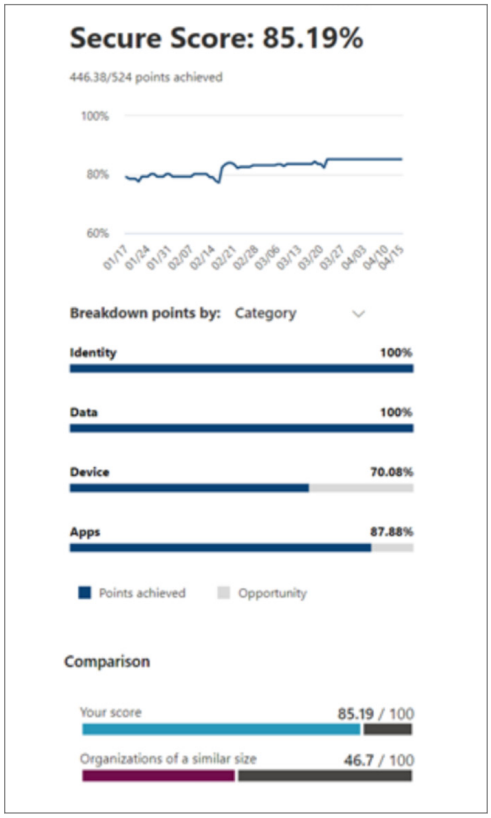
- **Apps / Infrastructure**: Strengthened application security, enforced secure coding practices, and conducted regular vulnerability assessments. Improved network security, implemented robust firewall configurations, and enhanced server hardening measures.



Outcome

Through dedicated efforts and strategic implementation of security measures, Helge Heupel GmbH and Cprime successfully elevated the Secure Score to 85.19% (an overall increase of 97% from baseline), signifying a strengthened security posture and reduced susceptibility to cyber threats.





Maintaining Vigilance

Improving Secure Score is undoubtedly a significant step towards enhancing an organization's security posture. However, it's essential to recognize that achieving a high Secure Score is not the final solution to security but rather the beginning of an ongoing process. Security is a dynamic and ever-evolving field, and the landscape of threats and vulnerabilities continually changes.

Therefore, even after achieving a desirable Secure Score, this automotive supplier will remain vigilant and proactive in monitoring their systems, networks, and applications for potential vulnerabilities and threats. This involves:

- **Regular Security Assessments**: Conducting periodic security assessments and audits to identify any new vulnerabilities or weaknesses in the organization's infrastructure, systems, and applications. These assessments may include penetration testing, vulnerability scanning, and security risk assessments.
- **Threat Intelligence**: Staying informed about the latest cybersecurity threats, trends, and attack techniques through threat intelligence sources, security advisories, and information sharing forums. This enables organizations to proactively anticipate and mitigate emerging threats.
- **Patch Management**: Implementing a robust patch management process to promptly apply security patches and updates to software, firmware, and operating systems. Patching known vulnerabilities helps prevent threat actors from exploiting security weaknesses.
- **Security Awareness Training**: Providing regular security awareness training to employees to educate them about common security threats, phishing scams, social engineering tactics, and best practices for safeguarding sensitive information. Employees are often the first line of defense against cyber threats and must be equipped with the knowledge and skills to recognize and respond to security incidents.

- **Incident Response Planning**: Developing and regularly testing incident response plans to ensure a timely and effective response to security incidents or data breaches. This includes defining roles and responsibilities, establishing communication channels, and outlining steps for containment, eradication, and recovery.
- **Continuous Monitoring and Optimization**: Proactive monitoring and optimization of security measures to adapt to emerging threats and evolving security requirements.
- **Continuous Improvement**: Continuously evaluating and refining security controls, policies, and procedures based on lessons learned from security incidents, industry best practices, and changes in the threat landscape. Security is a journey, and organizations must strive for continuous improvement to stay ahead of evolving threats.

What's Your Secure Score?

The journey of enhancing Secure Score underscores Helge Heupe's commitment to prioritizing cybersecurity and safeguarding its digital assets. By diligently implementing recommended security improvements and adopting a proactive approach towards security, the company has fortified its defenses, ensuring resilience against potential cyber threats.

What about your organization? Whether you use Microsoft Secure Score or not, all the same principles and best practices apply. If you've only done the minimum to get by—like most of your competitors—then you're probably hovering around the 45% mark like this automotive supplier was.

Partner with Cprime to assess your current security situation and double your cybersecurity protection starting right now.

Start Now!

Contributors

Jason Francis
Managing Consultant

Akansha Kochar
Microsoft Azure Consultant

Hannah Bowen
Delivery Consultant

About Cprime

As full-service consultants leading at the dynamic intersection of product and platform innovation, Cprime empowers organizations not only to accelerate change but to embrace it as a catalyst for strategic growth. With a proven track record as a trusted global consulting partner backed by Goldman Sachs and Everstone Capital, we go beyond traditional consulting and guidance to help clients anticipate market shifts, seize opportunities, and proactively shape their industries. Together, we drive innovation, foster flexibility and adaptability, and ensure sustainable growth amid continuous change to exceed customer and market expectations.

Visit us at cprime.com or call 877.800.5221 (US)
+44 (0) 203 811 0424 (UK)