TAKE CONTROL

Navigate & Address CIS Controls

In an era of swiftly advancing cybersecurity challenges, using a cybersecurity framework can help shape a path to navigate the chaos. One such framework from **The Center for Internet Security (CIS)** provides 18 cybersecurity controls that organizations can use to safeguard their systems and data. For MSPs, these controls can help pinpoint vulnerabilities in clients infrastructure - and serve as a guide for selling security solutions.

What are *CIS Controls?*

CIS Controls are vendor agnostic best practices and guidelines for organizations to strengthen their cybersecurity posture and protect against common cyber threats. These 18 controls (v8) are designed to be practical and actionable, providing organizations with a prioritized framework to implement cybersecurity measures effectively. Within each control are a number of safeguards representing an emerging minimum standard, with each safeguard requiring you to do one thing to improve your cyber hygiene.

Trend Score 78

Trend's Worry-Free™ Platform helps you address 78 Safeguards

What are *Implementation Groups?*

CIS Controls map to three implementation groups, based on resources and maturity, to enhance organizations' security posture. These implementation groups help organizations prioritize their efforts and focus on the controls that are most relevant to their current state.

Essential Cyber Hygiene (IG1)	Foundational Cyber Hygiene (IG2)	Advanced Cyber Hygiene (IG3)
74 Safeguards Trend's Worry-Free™ Platform Addresses 16	56 Safeguards Trend's Worry-Free™ Platform Addresses 30	153 Safeguards Trend's Worry-Free™ Platform Addresses 32
Minimum standard of cyber hygiene for small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel.	Builds upon the controls in IG1 and includes additional measures to enhance security, with dedicated individuals to manage & protect IT infrastructure.	Represents the highest level of cybersecurity maturity and includes controls that go beyond foundational practices. Must be able to abate sophisticated attacks, as well as reduce the impact of zero-day attacks.

Unlocking CIS
WITH TREND MICRO

With the assistance of Trend's Worry-Free™ Platform you can address four key controls: Malware Defenses, Email & Web Browser Protections, Incident Response and Security Awareness & Skills Training.
As a global leader in cyber security, if there are other controls you need support with, please contact us at Trend Micro and we can recommend additional products to suit your specific needs.

1	Inventory and Control of Enterprise Assets	2	Inventory and Control of Software Assets
3	Data Protection	4	Secure Configuration of Enterprise Assets & Software
5	Account Management	6	Access Control Management
7	Continuous Vulnerability	8	Audit Log Management
9	**Email and Web Browser Protections**	**10**	**Malware Defenses**
11	Data Recovery	12	Network Infrastructure
13	Network Monitoring and Defense	**14**	**Security Awareness & Skills Training**
15	Service Provider Management	16	Application Software Security
17	**Incident Response**	18	Penetration Testing

CIS CONTROLS

Strengthen Your
Business Safeguards Today

Trend Micro is ready to assist you in implementing these CIS controls, collaborating to fortify businesses and reduce the risk of your customers becoming a victim of future cybersecurity threats.

Contact one of our experienced cybersecurity Account Managers today and take control!

BOOK A
1 TO 1 MEETING

TAKE CONTROL

Email and Web Browser Protections

Malware Defenses
COMING SOON

Security Awareness & Skills Training
COMING SOON

Incident Response
COMING SOON

TREND MICRO

CIS CONTROL 9 Email & Web Browser Protections

7 SAFEGUARDS | IG1 2/7 | IG2 6/7 | IG3 7/7 | 7/7

Control 9 of the CIS Controls is **Email & Web Browser Protections**, which asks organizations to improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement. There are seven safeguards in this control, all of which are addressed by Trend's Worry-Free™ Platform.

CIS Safeguard	Title	Description	IG1	IG2	IG3	Trend's Worry-Free™ Platform		
						EDR	XDR	Managed XDR
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●	●	●	●
9.2	Use DNS Filtering Services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.	●	●	●	●	●	●
9.3	Maintain and Enforce Network-Based URL Filters	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or using block lists. Enforce filters for all enterprise assets.		●	●	●	●	●
9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●	●	●	●
9.5	Implement DMARC	To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.		●	●		●	●
9.6	Block Unnecessary File Types	Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●		●	●
9.7	Deploy and Maintain Email Server Anti-Malware Protections	Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.			●		●	●

How to secure, protect & TAKE CONTROL of your Cyber Security

WITH TREND MICRO

CIS CONTROL 9 **Email & Web Browser Protections**

7 SAFEGUARDS | IG1 2/7 | IG2 6/7 | IG3 7/7 | 7/7

Utilizing Trend's Worry-Free™ Platform, you can address each of the seven safeguards required in Control 9, but how? Here, we have taken a snapshot of just some of the advanced security functionality of this platform, which enables you to satisfy Control 9 and advance your client's security posture.

APPLICATION CONTROL

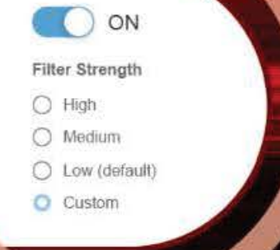
To address safeguard 9.1 - Ensure use of only fully supported browsers and Email clients, we use Application Control.

Organizations can choose between two modes of application control; **Block** Specific Applications or **Lockdown** mode - where only authorized applications are allowed to run.

URL FILTERING

Using URL Filtering safeguard 9.3 Maintain and Enforce Network-Based URL Filters, is taken care of.

Our URL filtering and web reputation services enforces web browsing policies across hybrid workforces, with custom set-up options available to suit your business requirements.



High	Blocks known or potential security threats, inappropriate or possibly offensive content, content that can affect productivity or bandwidth, and unrated pages
Medium	Blocks known security threats and inappropriate content
Low (default)	Blocks known security threats
Custom	Specify URL categories to block (Adult/Business/Communications and Search/General) - *Further options available*

WRITING Style DNA

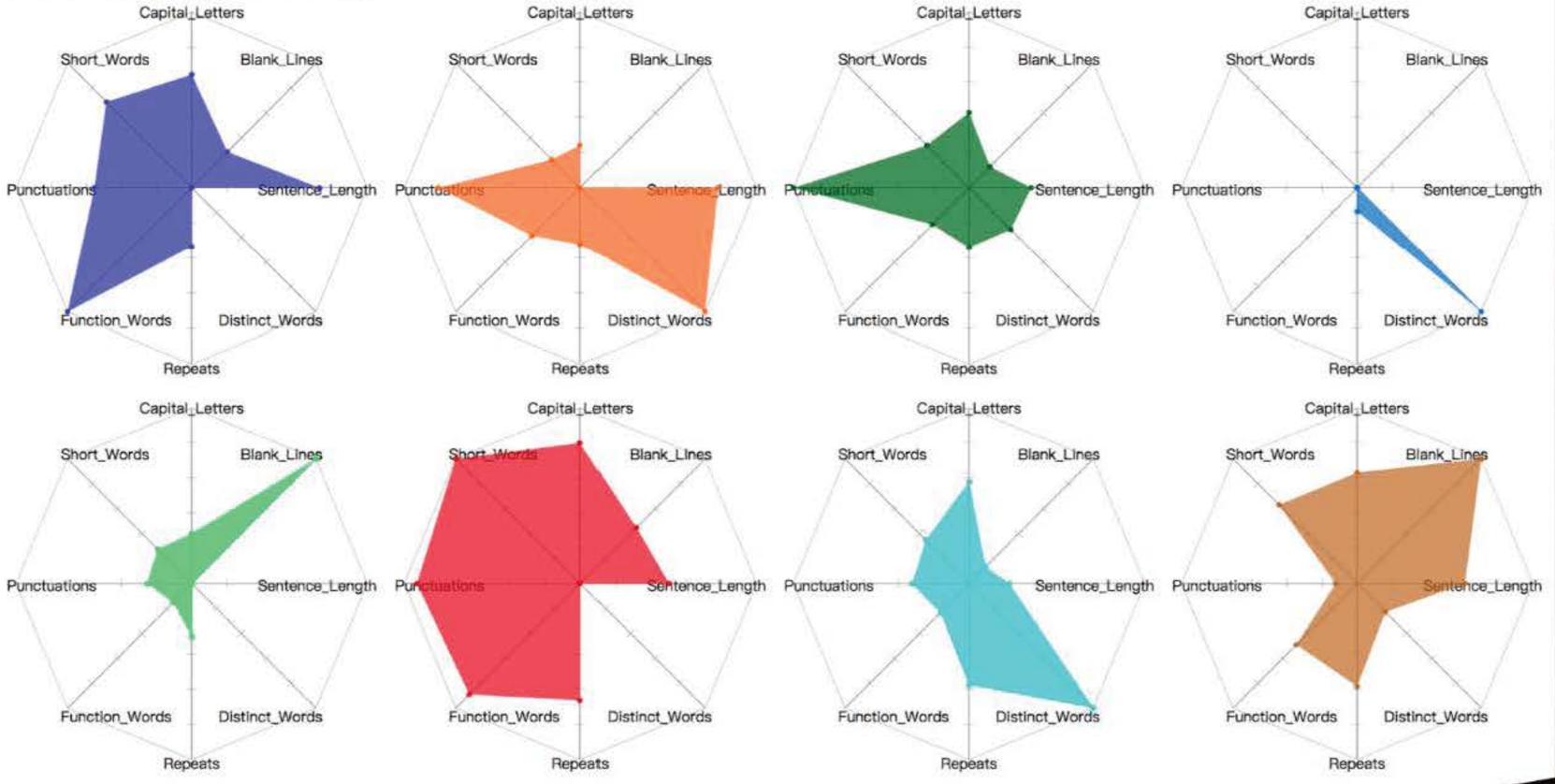
Writing Style DNA is the answer for safeguard 9.7 and advanced phishing attacks.

A writing style AI-model gets built for each high-profile user, and when an email comes in saying it's from that user, the AI model will be able to decipher if it is.

Start training | Stop training | Reset

Mail number : 494

Performance Variance : 0.17662187

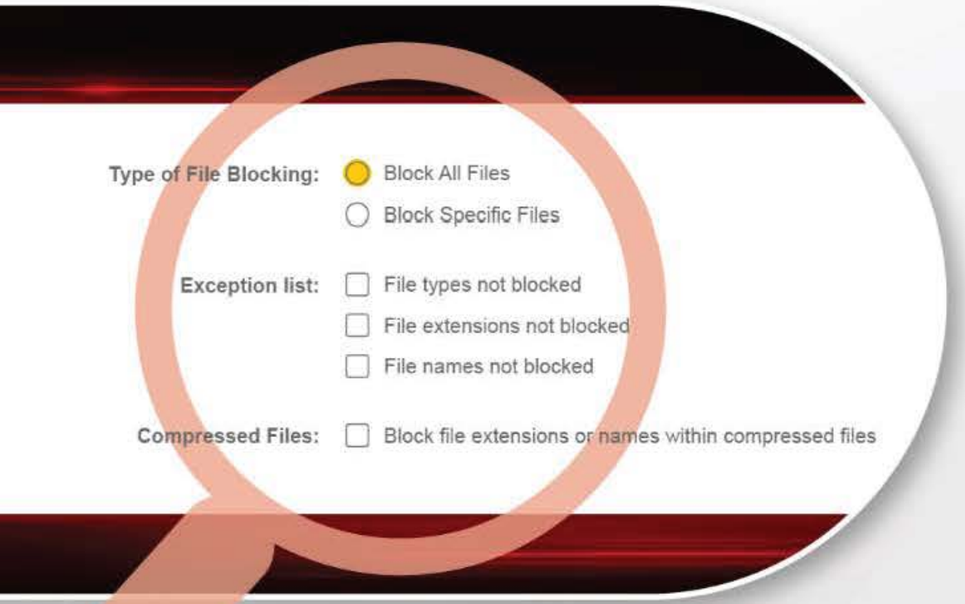


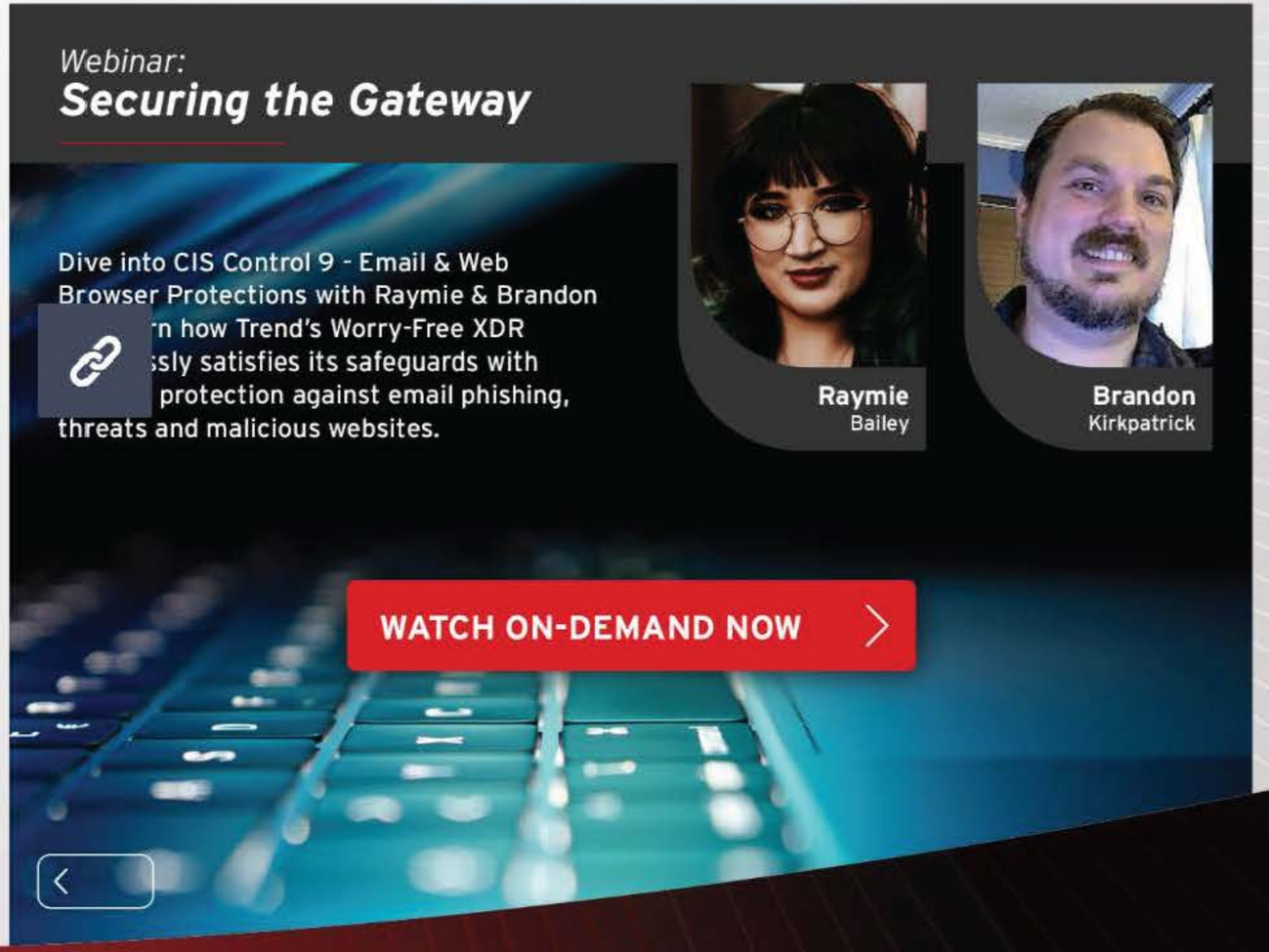
FILE Blocking

CIS CONTROL 9 **Email & Web Browser Protections**

7 SAFEGUARDS | IG1 2/7 | IG2 6/7 | IG3 7/7 | 7/7

Trend Micro can help you address ransomware arriving from compromised attachments, but also enhance compliance by preventing the sharing of sensitive data with flexible email File Blocking.





TAKE CONTROL

Email and Web Browser Protections | Malware Defenses | Security Awareness & Skills Training | Incident Response

TREND MICRO