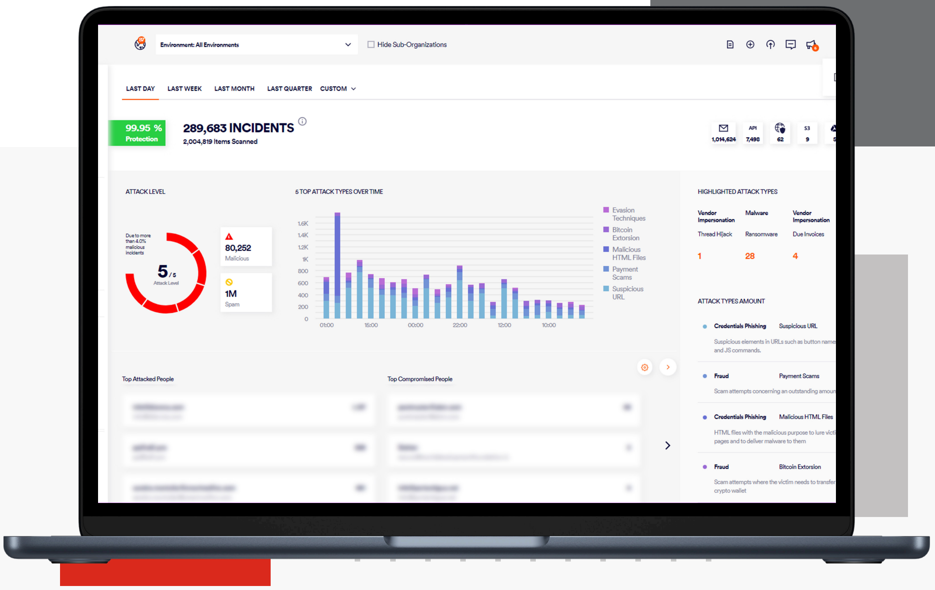
Fortinet Perception Point

Comprehensive cyber security platform



Environment: All Environments ☐ Hide Sub-Organizations

LAST DAY LAST WEEK LAST MONTH LAST QUARTER CUSTOM

99.95 % Protection

289,683 INCIDENTS
2,004,819 Items Scanned

1,014,624 | API 7,498 | 62 | S3 9

ATTACK LEVEL

Due to more than 4.0% malicious incidents

5 / 5 Attack Level

80,252 Malicious

1M Spam

HIGHLIGHTED ATTACK TYPES

Vendor Impersonation	Malware	Vendor Impersonation
Thread Hijack	Ransomware	Due Invoices
1	28	4

ATTACK TYPES AMOUNT

- Credentials Phishing Suspicious URL
  Suspicious elements in URLs such as button name and JS commands.
- Fraud Payment Scams
  Scam attempts concerning an outstanding amoun
- Credentials Phishing Malicious HTML Files
  HTML files with the malicious purpose to lure victi pages and to deliver malware to them
- Fraud Bitcoin Extorsion
  Scam attempts where the victim needs to transfer crypto wallet

Top Attacked People

Top Compromised People

Key Features

100% Dynamic Scanning. Dynamically scan 100% of email traffic including embedded files and URLs regardless of volume

Detection Rate 99.95%. Catch any threat type including evasive malware, social engineering attacks, and ATO takeover attempts with unprecedented accuracy

15 Seconds on Average. Intercept threats at the speed of your business for unhindered productivity and near-zero delay

75% SOC Time-Saving. Save up to 75% of SOC time with a natively integrated, managed Incident Respnse service managing incidents and remediating threats.

Security for the modern workforce

Modern enterprises operate in an increasingly hostile digital landscape where cyber threats are more sophisticated, evasive, and persistent than ever before. With over 90% of cyberattacks originating from email, traditional security solutions struggle to detect and mitigate advanced threats such as phishing, business email compromise (BEC), ransomware, and account takeovers. Additionally, cloud-based collaboration tools, browsers, and storage platforms introduce new attack vectors that traditional security architectures fail to address.

The Fortinet Perception Point platform is engineered to close these security gaps, providing an integrated, multi-layered cybersecurity solution that offers advanced threat protection across email, browsers, collaboration applications, and cloud storage. Unlike conventional security solutions that rely on static detection methods, Perception Point employs AI-powered real-time scanning, patented anti-evasion technology, and CPU-level exploit detection to prevent threats before they reach end-users.

Critical challenges

1. Advanced Threat Evasion – Many email and web threats leverage sophisticated evasion techniques, such as URL cloaking, file obfuscation, and sandbox-aware malware, to bypass conventional security layers.
2. Slow Incident Response – Security teams often face overwhelming volumes of incidents, leading to delays in detection and response.
3. Security Blind Spots – Traditional email security solutions fail to protect against threats originating from cloud-based applications, file-sharing platforms, and web browsers.
4. Account Takeover and Payload-less Attacks – Social engineering-based attacks that lack traditional malware payloads are difficult to detect using signature-based security methods.
5. High Operational Overhead – Managing multiple security solutions across different vectors increases complexity and reduces operational efficiency.

Key benefits

Comprehensive Multi-Channel Security

Fortinet Perception Point provides 360-degree protection across email, browsers, cloud collaboration tools, and storage applications, ensuring organizations are safeguarded across all communication and file-sharing channels.

High-Accuracy AI-Powered Detection

The platform utilizes AI, ML-based anomaly detection, and dynamic content analysis to identify and neutralize threats before they reach users. Its proprietary recursive unpacking engine ensures that 100% of files and URLs are scanned in real time, preventing even the most evasive threats.

Real-Time Threat Interception

Unlike legacy security solutions that rely on retrospective analysis, Perception Point prevents threats at the exploit phase—before malware is even executed—using patented CPU-level detection technology.

Automated Incident Response

The platform provides a fully managed 24/7 incident response service, drastically reducing the workload of security teams by handling threat remediation, forensic analysis, and policy optimizations.

Seamless Integration and Centralized Management

Designed for modern IT environments, the platform offers native API integrations with Microsoft 365, Google Workspace, Slack, Salesforce, Dropbox, and other cloud-based apps, consolidating threat intelligence and response under a unified security dashboard.

By leveraging Fortinet Perception Point, organizations can eliminate security blind spots, accelerate response times, and enhance operational efficiency while ensuring robust protection against emerging cyber threats.

Feature highlights

One Platform

Seven Layers of Security. Detect and prevent all major cyber threats across all channels in under 30 seconds from one, central platform.

Spam Filter

Anti-Spam (Email Only). Reputation and anti-spam filters quickly flag an email as spam.

Threat Intelligence

Known Attacks. Multiple threat intelligence sources and in-house engines scan URLs and files to warn about potential or current attacks.

Static Signatures

File Analysis. Leading signature-based anti-virus engines identify malicious attacks. Novel algorithms act to identify highly complicated signatures.

Hardware-Assisted Platform (HAP™)

Dynamic analysis Zero-days and unknown attacks. Unique CPU-level technology acts early in the kill chain to block attacks at the exploit phase—pre-malware release—for true APT prevention.

Recursive Unpacker

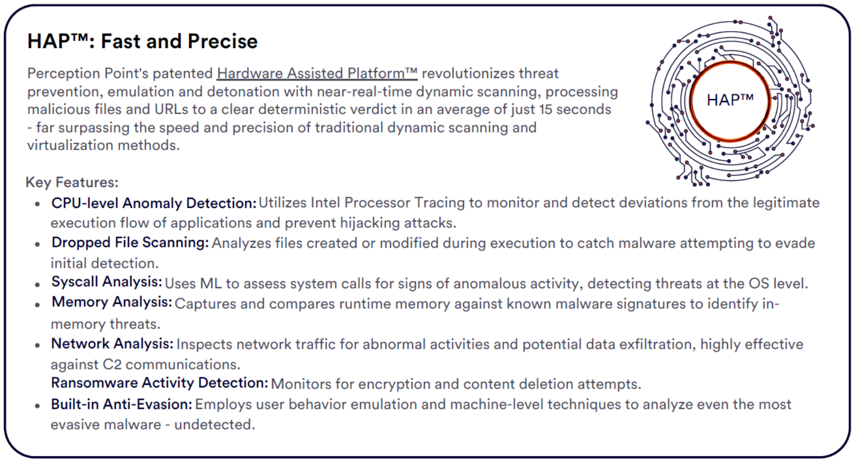
Anti-Evasion. Unpacks content into smaller units (files and URLs) to undo evasion techniques and identify hidden malicious attacks. Extracted components go separately through next security layers.

Anti-Phishing

URL analysis, AI and Image Recognition. URL reputation engines coupled with in-house image recognition analysis engine identify impersonation techniques and phishing attacks.

Anti-BEC and ATO

Payload-less Threats and Account Takeover. Prevents attacks that don’t necessarily include malicious files/URLs and intercepts account takeover.



HAP™: Fast and Precise

Perception Point's patented Hardware Assisted Platform™ revolutionizes threat prevention, emulation and detonation with near-real-time dynamic scanning, processing malicious files and URLs to a clear deterministic verdict in an average of just 15 seconds - far surpassing the speed and precision of traditional dynamic scanning and virtualization methods.

Key Features:

- **CPU-level Anomaly Detection:** Utilizes Intel Processor Tracing to monitor and detect deviations from the legitimate execution flow of applications and prevent hijacking attacks.
- **Dropped File Scanning:** Analyzes files created or modified during execution to catch malware attempting to evade initial detection.
- **Syscall Analysis:** Uses ML to assess system calls for signs of anomalous activity, detecting threats at the OS level.
- **Memory Analysis:** Captures and compares runtime memory against known malware signatures to identify in-memory threats.
- **Network Analysis:** Inspects network traffic for abnormal activities and potential data exfiltration, highly effective against C2 communications.
  Ransomware Activity Detection: Monitors for encryption and content deletion attempts.
- **Built-in Anti-Evasion:** Employs user behavior emulation and machine-level techniques to analyze even the most evasive malware - undetected.

Advanced Cloud Email Security

With advanced cloud email security, you can prevent email threats before they reach user inboxes. Phishing, BEC, ransomware, credential theft, and spam are just some of today's email-borne threats organizations need to protect against. While more than 90% of cyberattacks begin with an email, many of them easily evade Cloud email architectures. Moreover, new supplementary point solutions leave organizations vulnerable to the wide variety of attacks that they were not designed to prevent.

Advanced Cloud Email Security is a leading Integrated Cloud Email Security (ICES) solution recognized by Gartner. Combining high detection accuracy enriched by patented anti-evasion technology and AI with a managed Incident Response service, the solution delivers security for the modern workforce.

Advanced Email Security prevents phishing, BEC, malware, account takeover, and Zero-day exploits before they reach organizations using Microsoft 365, Google Workspace, or any cloud email service.

The platform is recognized by many major regulatory agencies, including GDPR, HIPAA, Gartner, AICPA SOC 2, a AAA rating at SE Labs, and is ISO-27001 certified.

Benefits

Service: fully managed, all-included incident response service

Advanced Cloud Email Security provides Prevention-as-a-Service. You receive a set of value-added tools that are an integral part of the product to help you better intercept, investigate, and remediate any malicious event.

The integrated team of cybersecurity experts act as 24/7 extension of the organization's SOC/ security provider. The team will handle all your activities concerning email security; managing incidents, maintaining and optimizing policies, on-demand investigations, reporting, FP+FN hunting, SOC team updating, and much much more.

Platform: eliminate security blind spots with 360° channel coverage

Fortinet delivers its security solution via a centralized, modular platform allowing organizations to protect their most targeted channels all in one place.

Beyond Advanced Cloud Email Security, Fortinet provides advanced threat protection to your standard web browsers, cloud collaboration and messaging apps, storage platforms, CRMs, proprietary apps, and unsourced file streams and uploads.

All modules can work separately or together to provide maximal protection via a unified management dashboard, displaying threats and live incident insights all in one place.

Advanced Email and Advanced Browser Security

Secure your data and endpoints with a browser-centric solution offering unprecedented web and email protection synergy. Combining Fortinet's Advanced Email Security and browser extension elevates threat prevention to new heights by:

- Correlating cross-channel evidence to prevent the most evasive threats
- Tracing attacks back to their source and identifying impacted end users
- Remediating web and email incidents rapidly from a centralized view

Gartner Peer Insights™
4.8 ★★★★★

State Of The Art Technology

We did a very detailed evaluation about 15+ email security solutions than can be plugged in onto Office 365 Mailing and EOP. The vendor was new to us but we compared capabilities in a very fact based approach. The solution showed both in prevention capabilities and in Incident Response support capabilities the best results on the market.

Matthias Leckel,
Global Infrastructure Security Architect at Red Bull

Advanced Collaboration Security

With the shift to remote and hybrid working, communication is moving beyond just email to include collaboration tools such as LinkedIn, Teams and Slack with users outside the organization. Attackers can potentially use these for phishing and malware distribution.

2023 Gartner® Market Guide for Email Security

Threat detection and response across the modern workspace.

Collaboration apps come with security risks. In today's digital workspace, collaboration, messaging, and storage SaaS application have long become integral to daily operations. The increasing adoption of tools such as Slack, Microsoft 365 cloud apps, Salesforce, and others has transformed these cloud platforms into hotbeds and vectors for advanced cyber attacks. Phishing links, sophisticated malware, and zero-day exploits, are increasingly being delivered through third party apps, posing a significant risk to end-users and the enterprise security posture.

Significant Blind Spots

- **Lack of Native Defense:** contrary to popular belief, many SaaS apps like Salesforce and Slack, do not offer built-in content scanning, allowing even for known threats to be seamlessly uploaded or delivered
- **Advanced Threat Landscape:** most detection tools and CASB solutions are not equipped to combat the ever evolving adversaries and fail to stop innovative attack techniques and evasive threats
- **Volume of Traffic:** the high volumes of data and files being shared and stored on these apps makes it difficult to properly scan all incoming traffic in a timely manner
- **Multi-Vector Attacks:** most organizations use multiple third party apps from various vendors and product suites, making it difficult to effectively manage security across all channels
- **Third Party Access:** external collaborators with access to the enterprise workspaces and messaging apps pose a serious threat in cases of potential partner and vendor compromise or account takeover

Osterman Research

Many newly adopted cloud collaboration apps and services have only been around for a few years. Worryingly, the rate of malicious incidents against these new apps and services is already 60% of what organizations experience against their email services. Threat actors have responded quickly to the emergence of new channels for employee productivity and collaboration.

Osterman Research's Report on Emerging Cyber Threats

Advanced Collaboration Security

A unique, next-gen platform that delivers unparalleled threat protection across all enterprise communication and storage platforms while maintaining an optimal user experience. The cloud-based solution is easily deployed via API integration to ensure no malicious URL or file is affecting the end-users.

Powered by a multi-layered detection and a natively integrated Incident Response service, Fortinet prevents content-based attacks across popular communication apps, effectively scanning 100% of the data in seconds, and allowing employees to collaborate freely and safely.

This solution offers holistic threat prevention with static and dynamic-detection layers working together with proprietary anti-evasion engine. With light-speed results, it scans content without causing any delays to ongoing operations. It enables security policy extension from the email domain to other communication channels, significantly enhancing the line of defense against sophisticated attackers, securing your enterprise collaboration workspace.

Advanced Collaboration Security

Preventing content-based threats in an instant.

Inspect 100% of the content dynamically to detect malicious uploaded files and messages in seconds. Preventing phishing campaigns, complex and everyday malware, zero-days, APTs, or any harmful document and URL across messaging channels, file sharing platforms, cloud hosting services, CRMs, and more.

Supercharge incident investigation and advanced threat analysis with cross-channel data and actionable insights. Proving prevention-as-a-service, the manage Incident Response team assists security and IT teams to take action and remediate any threat on the protected channels.

Leverage a simple Plug & Play deployment via API and agile performance with zero-impact on business flows and frictionless end-user experience.

Fully managed, all-included incident response service.

Fortinet provides Prevention-as-a-Service. You receive a free of charge set of value-added tools that are an integral part of the product to help you better intercept, investigate, and remediate any malicious event.

Our integrated team of cybersecurity experts act as 24/7 extension of the organization's SOC/ security provider. The team will handle all your activities concerning Advanced Collaboration Security; managing incidents, maintaining and optimizing policies, on-demand investigations, reporting, FP+FN hunting, SOC team updating, and much much more.

Platform advantage: eliminate security blind spots with 360° channel coverage.

Fortinet delivers its security solution via a centralized, modular platform allowing organizations to protect their most targeted channels all in one place.

Beyond Advanced Collaboration Security, Fortinet can provide threat protection to email, standard web browsers, proprietary apps, and unsourced file streams and uploads.

All modules can work separately or together to provide maximal protection via a unified management dashboard, displaying threats and live incident insights all in one place.

The ultimate combo: advanced email and advanced browser security.

Secure your data and endpoints with a browser-centric solution offering unprecedented web and email protection synergy. Combining Fortinet's Advanced Email Security and browser extension elevates threat prevention to new heights by:

- Correlating cross-channel evidence to prevent the most evasive threats
- Tracing attacks back to their source and identifying impacted end users
- Remediating web and email incidents rapidly from a centralized view

Refreshing Advanced Browser Security and Control

The Advanced Browser Security extension integrates with any browser to protect your employees and SaaS apps against web-borne attacks and data-loss, and allows you to regain control over your users' last ungoverned app.

Why Enterprise Advanced Browser Security?

The browser has become the de-facto workspace of the modern organization. It is the most used application with users spending the bulk of their working hours switching between one tab to another to communicate, collaborate, and complete tasks. As the "windows to the web", browsers present fundamental security and IT challenges such as the following.

Highly Targeted Attack Surface

Browsers are prime targets for cyber attacks that easily bypass traditional security measures like firewalls and Secure Browser Gateways (SWG) and only detonate in the target browser. From evasive zero hour phishing attacks to malware and zero-day exploits, threat actors leverage the native accessibility of browsers to circumvent detection and launch attacks on users and endpoints.

A Source for Data Loss

Designed inherently for information access and sharing, browsers are also a critical vector for data exfiltration. Whether through inadvertent actions by employees (e.g. GenAI usage) or deliberate maneuvers by malicious insiders and third parties, browsers are often the means for the unauthorized transfer of sensitive data outside the organization.

A Governance Blindspot

The interactions between your users and their browsers represent a significant blindspot for endpoint and network security solutions. This lack of visibility leaves IT teams unable to enforce security policies or detect anomalous user activities within the browser application.

Internal Threats

- Data Exfiltration
- Malicious Insiders
- Unsafe GenAI Usage
- Shadow IT
- Compliance Violations

External Threats

- Phishing
- Malicious Browser Extensions
- Malware Downloads
- XSS
- HTML Smuggling

Introducing Advanced Browser Security

The Advanced Browser Security solution integrates with any browser via a lightweight extension to ensure dynamic protection and governance with zero impact on user experience or browsing quality, empowering employees to work and maintain productivity while staying secure.

Stop attacks at the point-of-click

Leveraging textual and image recognition AI models, proprietary anti-evasion, and a patented sandbox, to instantly identify and prevent web-borne threats. From evasive zero-hour phishing sites to malicious file downloads and cross-site scripting (XSS) exploits, Fortinet neutralizes them at the point-of-click.

Enforce safe access and prevent data loss

Equipping security and IT professionals with a comprehensive suite of tools and granular web policies to enable and enforce safe access to enterprise web apps and SaaS platforms while preventing sensitive data loss and risky behaviors across both managed and unmanaged devices.

Get visibility and control over the browser

Unlocking browser-level control and effective monitoring capabilities across all of the organization's browsers from one intuitive cloud console. Allowing for web-content filtering, remediation of risky browsing events, clear visibility to unsanctioned apps and browser extensions in use, and more.

CRITICAL USE CASE	FEATURES
SAFE BROWSING	
Prevent phishing, evasive malware, zero-days, and harmful browser extensions from compromising your users and data in real time.	Anti-phishing via image recognition models (detecting logo impersonation, login forms, and brand favicons) Full dynamic scanning of all file downloads, recognized by SE Labs as best-in-class file detection CPU-level sandbox - HAP™* (ransomware and zero-day exploits) Recursive file unpacking (anti-evasion) ML models to detect and prevent malicious HTML snippets Malicious URL detection HTML smuggling prevention Detect XSS attempts Block uncategorized websites and risky website categories
SAFE ACCESS AND DLP	
Enforce safe access to your SaaS and web apps, stop deliberate and accidental data leaks, malicious insiders and third party threats.	Require the extension as a condition to accessing enterprise web apps via conditional access** Granular clipboard controls to limit risky behaviors across sensitive sites and apps Granular download/upload controls Safe GenAI/ChatGPT enablement (sensitive content detection and user warning) Watermarking - deterring users from capturing on-screen sensitive data Real-time PII detection in user data submission (conditional warn/restrict, regex-based) PII detection in downloaded files (NER/LLM-based) Anomalous mass data exfiltration detection Shoulder surfing protection - blur sensitive websites while not in use Optionally audit all file uploads Anti-tampering - restrict developer tools use
BROWSER GOVERNANCE	
Transform any browser into a secured workspace with granular browser-level controls and 360° visibility.	Installed browser extensions discovery, governance and risk analysis, leveraging both reputation data, static analysis and dynamic sandbox-based analysis of extensions Risky extensions detection and automatic disablement Browser login events monitoring Browser inventory and version information Password-reuse monitoring and alerts Browsersite categories, content and URL filtering and restriction Restrict downloads (per file type or website category for example) Seamless deployment and offboarding for contractors and third party users IdP SSO integration Customizable end-user notifications and warnings

How Does It Work?

Extension

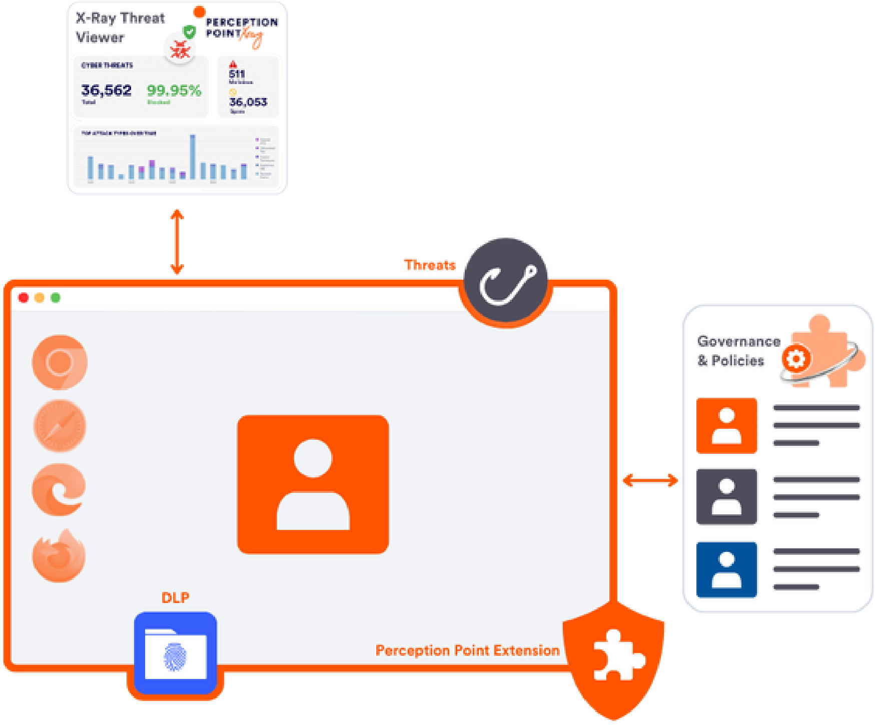
Deployed across any browser on both managed and unmanaged devices, with multiple deployment options to comply with different IT requirements (unattended and silent deployment via UEM, IdP integration, script-based, manual/automated email-invites).

Admin Console

The Advanced Browser Security admin console provides full threat analysis and remediation capabilities, empowering security teams with detailed insights of malicious or risky behaviors, comprehensive forensic information of prevented attacks, and unique cross-channel cases and context.

Governance and Policies

Configure and manage how the Fortinet extensions operate in your enterprise. The console allows admins to govern end-users and devices, develop and maintain web policies and DLP rules, and more.



Combining Email and Advanced Browser Security

Secure your users and data with unparalleled web and email protection synergy. Combine Fortinet's market leading Advanced Cloud Email Security with the Advanced Browser Security extension to elevate threat prevention to new heights.

Correlating Cross-Channel Evidence to Stop the Most Evasive Threats

Scanning threats from the user's point of view renders the most advanced evasion techniques ineffective. Geofencing, CAPTCHAs, password-protection, or time-based tactics designed to evade detection are prevented in real-time once the user encounters the malicious website/payload on the browser. Contextual evidence gathered from email (e.g. sender, domain) is leveraged to enhance detection and users' awareness of web-borne attacks—and vice versa.

Tracing Attacks Back to Their Source and Identifying Impacted Users

Combining live browsing data with email events allows security professionals to easily and visually connect the dots and investigate the impact of an attack or an ongoing incident: Which users inserted their credentials? Who clicked/downloaded the malicious content? What unsanctioned apps do my employees use?

Rapid Remediation of Browser and Email Incidents + Enhanced Email DLP

Faster, more efficient remediation of phished users and Account Takeover incidents with login events monitoring and visibility. Weaponized files or URLs scanned by the extension in the wild get automatically remediated from all inboxes. Warn or prevent end users from email-related data exfiltration, audit sensitive email attachments (e.g. employee offboarding) and receive email DLP alerts.

Uncompromising Workspace Security and Productivity

Superior Detection

AI-powered threat detection with proven accuracy of 99.95%. 100% of file downloads are scanned dynamically using a multi-layered architecture.

Rapid Agentless Deployment

Onboard employees and contractors easily via a lightweight browser extension compatible with any standard browser.

Workspace Security-Ready

Leverage with Advanced Email Security and cloud app protection, to holistically protect your user-centric attack vectors against advanced threats.

Centralized Control

Configure and enforce all website rules and policies from Fortinet's intuitive cloud management console.

Unhindered User Experience

Allow your users to continue working with their existing browsers. Unless a web-borne threat is detected, they won't feel the extension is there.

Managed Advanced Browser Security

An all-included incident response and support service alleviates the overhead and fully supports your SOC/IT teams or MSP staff 24/7, to provide enterprise-grade Advanced Browser Security and save up to 75% in operational resources.

Technical Specifications

Feature and Description
Manageability
Cloud-based management console and user inventory
Dashboards and reporting
Configure threat protection mode (silent/warn/block)
Customizable UX for end-users (warnings, toast messages, block pages)
Identity provider integration (via SAML)
Automatic policy assignment based on user properties (e.g. SAML attributes)
Role-based access control (RBAC)
User and admin auditing
Forensics and Incident Response
An all-included 24×7 incident response service powered by cybersecurity and web security experts
In-depth forensics view of all security incidents and cases
Correlation of browser and email events (Advanced Email Security)
Cross-channel correlation and remediation of security incidents (e.g. remediation across all protected cloud channels)
Compliance
SOC2
GDPR
ISO 27001
HIPAA
Supported Browsers
Google Chrome
Microsoft Edge
Firefox
Safari
Any other Chromium-based browser such as Opera, Brave, or Arc
Supported OS
Windows
MacOS
ChromeOS
LinuxiOS (preview)
Deployment and Updates
UEM solutions (Microsoft Intune, JumpCloud, Jamf Pro, and Google Workspace)
Self-service install by users via email invite
Operating in the background in silent/transparent mode (configurable)
Automatic updates (configurable)
No tunneling/remote browsing/proxying web traffic
Compatible with any existing VPN/proxy/network infrastructure

Order Information

Advanced Cloud Email Security (SaaS)

Please note that billing is based on customer declaration (the number of active mailboxes a customer declares to Fortinet). Fortinet uses internal methods to validate the customers declared number users.

Product	Advanced Cloud Email Security	Advanced Internal Cloud Email Security	Full Email Security Bundle
Security Services			
Inbound Email Security	✓		✓
Internal Email Security		✓	✓
Threat Intelligence	✓	✓	✓
Static File Analysis	✓	✓	✓
Anti-Phishing	✓	✓	✓
Anti-BEC	✓	✓	✓
Account Takeover Protection - M365	✓	✓	✓
Dynamic File Analysis (HAP Sandbox	✓	✓	✓
Threat Intelligence	✓	✓	✓
Additional Services			
24×7 Support	✓	✓	✓
24×7 Incident Response Service		✓	✓
Advanced Collaboration Security		Add-on per collaboration application	Add-on per collaboration application
Advanced Browser Security for Governance and DLP		Add-on	Add-on
99.99% Service Level Target	✓	✓	✓
Reporting	✓	✓	✓
Internal Email Scanning	Add-on	✓	✓
URL Dynamic Analysis	✓	✓	✓
Number of Domains Protected	Unlimited	Unlimited	Unlimited
VIP Protection	✓	✓	✓
Email Disclaimers	✓		✓

Order Information

Advanced Cloud Email Security (SaaS)

Product	SKU	Tier	Description
Advanced Cloud Email Security	FPP-ADES1-ST-AE01	0-999 users	Fast interception of any advanced attack across the organization's email, preventing phishing, spear-phishing, whaWling, malware, ransomware, BEC, ATO, spam, N-days, and Zero-days well before they reach the enterprise's end-users. Includes a fully managed Incident Response service.
	FPP-ADES1-ST-AE02	1000-2499 users	
	FPP-ADES1-ST-AE03	2500-4999 users	
	FPP-ADES1-ST-AE04	5000-9999 users	
	FPP-ADES1-ST-AE05	10 000-14 999 users	
	FPP-ADES1-ST-AE06	15 000-24 999 users	
	FPP-ADES1-ST-AE07	25 000+ users	
Advanced Internal Cloud Email Security	FPP-AIES1-ST-AE01	0-999	Protection against any type of intradomain threats - files, URLs, and text-based attacks within the organization, guarding users from internal breaches and impersonation tactics. Includes a fully managed Incident Response service.
	FPP-AIES1-ST-AE02	1000-2499	
	FPP-AIES1-ST-AE03	2500-4999	
	FPP-AIES1-ST-AE04	5000-9999	
	FPP-AIES1-ST-AE05	10 000-14 999	
	FPP-AIES1-ST-AE06	15 000-24 999	
	FPP-AIES1-ST-AE07	25 000+	
Advanced Cloud Email Security Bundles	FPP-FESB1-BD-AE01	0-999	Security for Advanced Email + Internal Email.
	FPP-FESB1-BD-AE02	1000-2499	
	FPP-FESB1-BD-AE03	2500-4999	
	FPP-FESB1-BD-AE04	5000-9999	
	FPP-FESB1-BD-AE05	10 000-14 999	
	FPP-FESB1-BD-AE06	15 000-24 999	
	FPP-FESB1-BD-AE07	25 000+	

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Order Information

Advanced Collaboration Security

Advanced Collaboration Security is provided on a per user basis per collaboration application. Security for Microsoft products covers Sharepoint, OneDrive, and Teams under the same subscription SKU.

Product	SKU	Tier	Description
Microsoft: Sharepoint, OneDrive, and Teams	FPP-ACSM1-ST-AC01	0-999 users	Protect the organization's Microsoft Collaboration apps from malicious files, URLs, and novel threats, backed by a fully managed Incident Response service.
	FPP-ACSM1-ST-AC01	1000-2499 users	
	FPP-ACSM1-ST-AC01	2500-4999 users	
	FPP-ACSM1-ST-AC01	5000-9999 users	
	FPP-ACSM1-ST-AC01	10 000-14 999 users	
	FPP-ACSM1-ST-AC01	15 000-24 999 users	
	FPP-ACSM1-ST-AC01	25 000+ users	
Advanced Collaboration Security for Google Drive	FPP-ACSG1-ST-AC01	0-999	Protecting the organization's Google Drive storage from malicious files, URLs, and novel threats, backed by a fully managed Incident Response service.
	FPP-ACSG1-ST-AC01	1000-2499	
	FPP-ACSG1-ST-AC01	2500-4999	
	FPP-ACSG1-ST-AC01	5000-9999	
	FPP-ACSG1-ST-AC01	10 000-14 999	
	FPP-ACSG1-ST-AC01	15 000-24 999	
	FPP-ACSG1-ST-AC01	25 000+	
Advanced Collaboration Security for Box	FPP-ACSB1-ST-AC01	0-999	Protect the organization's Box cloud storage from malicious files, URLs, and novel threats, backed by a fully managed Incident Response service.
	FPP-ACSB1-ST-AC01	1000-2499	
	FPP-ACSB1-ST-AC01	2500-4999	
	FPP-ACSB1-ST-AC01	5000-9999	
	FPP-ACSB1-ST-AC01	10 000-14 999	
	FPP-ACSB1-ST-AC01	15 000-24 999	
	FPP-ACSB1-ST-AC01	25 000+	
Advanced Collaboration Security for DropBox	FPP-ACSD1-ST-AC01	0-999	Protect the organization's Dropbox storage from malicious files, URLs, and novel threats, backed by a fully managed Incident Response service.
	FPP-ACSD1-ST-AC01	1000-2499	
	FPP-ACSD1-ST-AC01	2500-4999	
	FPP-ACSD1-ST-AC01	5000-9999	
	FPP-ACSD1-ST-AC01	10 000-14 999	
	FPP-ACSD1-ST-AC01	15 000-24 999	
	FPP-ACSD1-ST-AC01	25 000+	
Advanced Collaboration Security for Slack	FPP-ACSK1-ST-AC01	0-999	Protecting the organization's Slack collaboration tool from malicious files, URLs, and novel threats, backed by a fully managed Incident Response service.
	FPP-ACSK1-ST-AC01	1000-2499	
	FPP-ACSK1-ST-AC01	2500-4999	
	FPP-ACSK1-ST-AC01	5000-9999	
	FPP-ACSK1-ST-AC01	10 000-14 999	
	FPP-ACSK1-ST-AC01	15 000-24 999	
	FPP-ACSK1-ST-AC01	25 000+	
Advanced Collaboration Security for Zendesk Advanced Collaboration Security: Salesforce and API based. Advanced Cloud Storage Security for Salesforce is charged on a per user (no tier) basis. API based Advanced Collaboration Security scanning is charged per scan	FPP-ACSZ1-ST-AC01	0-999	Protecting the organization's Slack collaboration tool from malicious files, URLs, and novel threats, backed by a fully managed Incident Response service.
	FPP-ACSZ1-ST-AC01	1000-2499	
	FPP-ACSZ1-ST-AC01	2500-4999	
	FPP-ACSZ1-ST-AC01	5000-9999	
	FPP-ACSZ1-ST-AC01	10 000-14 999	
	FPP-ACSZ1-ST-AC01	15 000-24 999	
	FPP-ACSZ1-ST-AC01	25 000+	
Advanced Cloud Storage Security for Salesforce	FPP-ACSS1-ST-AC00		One Month Protecting the organization's Salesforce channels from malicious files, URLs, and novel threats, backed by a fully managed Incident Response service.
API	FPP-AWBS1-ST-CS00		Next-gen API security, preventing the transmission of malicious files, URLs and social-engineering attacks through the organizations API channels, backed by a fully managed Incident Response service.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Order Information

Advanced Browser Security

Prevent phishing, evasive malware, zero-days, and harmful browser extensions from compromising users and data. Enforce safe access to SaaS and web apps, stop data leaks, malicious insiders and third party threats. Provide granular browser-level controls and 360° visibility.

PRODUCT	SKU	TIER	DESCRIPTION
Advanced Browser Security			
Advanced Browser Security	FPP-AWBS1-ST-AB01	0-999 users	One Month Securing the organization's web browsing with user controls and multi-layer detection engines that prevent all web-based threats including phishing, ransomware, malware, APTs, zero-day vulnerabilities and more, backed by a fully managed Incident Response service.
	FPP-AWBS1-ST-AB02	1000-2499 users	
	FPP-AWBS1-ST-AB03	2500-4999 users	
	FPP-AWBS1-ST-AB04	5000-9999 users	
	FPP-AWBS1-ST-AB05	10 000-14 999 users	
	FPP-AWBS1-ST-AB06	15 000-24 999 users	
	FPP-AWBS1-ST-AB07	25 000+ users	
Security Bundles			
Email and Advanced Browser Security Bundle	FPP-EWSB1-BD-BD01	0-999	One Month Security for Advanced Email + Browser Extension.
	FPP-EWSB1-BD-BD02	1000-2499	
	FPP-EWSB1-BD-BD03	2500-4999	
	FPP-EWSB1-BD-BD04	5000-9999	
	FPP-EWSB1-BD-BD05	10 000-14 999	
	FPP-EWSB1-BD-BD06	15 000-24 999	
	FPP-EWSB1-BD-BD07	25 000+	
Ultimate Email, Google Workspace and Advanced Browser Security Bundle	FPP-UGWB1-BD-BD01	0-999	One Month Security for Advanced Email + Internal Email + Google Drive Storage + Browser Extension.
	FPP-UGWB1-BD-BD02	1000-2499	
	FPP-UGWB1-BD-BD03	2500-4999	
	FPP-UGWB1-BD-BD04	5000-9999	
	FPP-UGWB1-BD-BD05	10 000-14 999	
	FPP-UGWB1-BD-BD06	15 000-24 999	
	FPP-UGWB1-BD-BD07	25 000+	
Ultimate Email, MS Package and Advanced Browser Security Bundle	FPP-UMWB1-BD-BD01	0-999	One Month Security for Advanced Email + Internal Email + MS Package + Browser Extension.
	FPP-UMWB1-BD-BD02	1000-2499	
	FPP-UMWB1-BD-BD03	2500-4999	
	FPP-UMWB1-BD-BD04	5000-9999	
	FPP-UMWB1-BD-BD05	10 000-14 999	
	FPP-UMWB1-BD-BD06	15 000-24 999	
	FPP-UMWB1-BD-BD07	25 000+	

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

FORTINET

www.fortinet.com

February 18, 2025

FPP-DAT-R01-20250217