Distributed DNS Defense (ITP)

Co-Managed Internet Threat Protection

Remote work increases the odds that employees will use unsecured networks. As a first line of defense, employees need a secure onramp to the internet.

Today, "the office" can be anywhere, and traditional security just can't keep up. Distributed DNS Defense (ITP) acts as your first line of defense against threats. ITP secures internet access and controls cloud app usage from your network, branch offices, and roaming users.

We bring together best in class security operations and best in breed threat intelligence to stop threats before they reach your network or endpoints and protect your users against today's sophisticated threats. Our unified toolset provides secure web gateway, cloud-delivered firewall, DNS-layer security, and cloud access security broker (CASB) functionality in a single easy to consume platform.

ITP provides the second layer of defense in our eXtended Detection & Response (XDR) managed security offering, and serves as a critical component of our Secure Service Edge (SSE) offerings. ITP secures access to the internet, with deep inspection and control, to support compliance and provide effective threat protection.

ITP Editions

Starter

SMALL COMPANIES

Good for small companies or as a first line of defense for any size company

Essentials

MID-SIZED ENTERPRISE

Good for mid-sized companies; interactive threat intelligence and on-demand API to enrich other tools and systems

Premium

LARGE ENTERPRISE

Ideal for large companies with advanced security and web policy needs; cloud delivered firewall and ability to create policies with granular controls

KEY BENEFITS

- Protect users anywhere with DNS-layer security
- 24 x 7 x 365 eyes on glass: fully staffed security operations team, geo-redundant SOC
- Block domains associated with phishing, malware, botnets, newly, etc.
- Prevent malware or phishing attempts from malicious websites
- Prevent web and non-web callbacks from compromised systems
- Proxy and decrypt risky domains for deeper inspection of URLs and files
- Enable web filtering using 85+ domain content categories
- Pinpoint compromised systems using real-time security activity reports
- Discover and block shadow IT (based on domains) with the App Discovery report
- Investigate with interactive threat intel
- Protect off-network mobile and roaming users

CONTACT US

By enforcing security at the DNS and IP layers, ITP blocks requests to malware, ransomware, phishing, and botnets before a connection is even established—stopping threats over any port or protocol before they reach your network or endpoints.

Every edition of ITP is monitored and managed by our 24 x 7 x 365 security operations center, providing you eyes on glass around the clock. DataEndure adds value by ensuring that every threat is reviewed, acted upon, documented, and escalated as needed. In most cases we interpret and resolve threats in about 20 minutes and only contact you for urgent matters.

The platform also supports APIs for network devices, management, and reporting. Starting with the Essentials edition, you also have access to enforcement APIs which enables third-party security services integration for extended enforcement everywhere.

- **On-network:** Any network device (e.g. router, DHCP server) can be used to connect to ITP. Simply redirect your DNS to the platform's IP address. That's it. You can also leverage your existing Cisco footprint — Cisco AnyConnect, Cisco routers (ISR 1K and 4K series), Cisco Wireless LAN Controllers, and Meraki MR/MX — to provision thousands of network devices and laptops in minutes.
- **Off-network laptops and mobile devices:** Available for laptops that use Windows, macOS, Chrome OS, and supervised Apple devices that run iOS 11.3 or higher. The ITP roaming client allows you to provide the same level of controls and security no matter where the endpoint connects from.

Starter

Starter is the foundational DNS Security offering, which is best suited for small companies or as our second line of defense for any size company. Essentials features include:

- 24 x 7 x 365 Security Operations Center
- Protect users on the corporate network via integration with the networking devices
- Protect off-network users via the Roaming client
- Block domains associated with malware, phishing, botnets, and other threats
- Perform web filtering by domain and domain category
- Discover and block shadow IT based on domains
- Create policies and view reports by user with Active Directory integration
- Integrate with existing tools and workflows with APIs for enforcement, reporting, management, and deployment
- Integrate with threat response to aggregate activity across offerings

Unmatched threat intelligence to stop attacks earlier.

KEY FEATURES

- 24 x 7 x 365 Security Operations Center (SOC)
- Global SaaS implementation. Highly available. Choice of locality (US, EU, APAC)
- Block malware without the latency of appliance-based centralized solutions
- Improve visibility and network protection by monitoring DNS request and IP connections
- Manage and control cloud apps and detect shadow IT
- Unmatched threat intelligence
- Data-driven Dashboard Security Analytics
- Improve performance with geo-cached DNS across 30+ data centers
- API-driven DNS integrations (SIEM, sandbox, Slack, 3rd party threat intelligence, etc)
- Single API for extended enforcement
- Agents and policies are managed via our globally available multi-tenant SaaS platform

Ask about our complimentary **Security Health Check** to identify gaps.

Essentials

Essentials is well-suited for mid-sized enterprises that need modern distributed endpoint protection and control plus advanced threat hunting and investigation features.

Essentials adds threat hunting with forensics that automatically contextualizes all DNS activity for your future investigations. This saves analysts from tedious event correlation tasks and allows you to get to the root cause fast. Essentials is designed to lighten the load on security administrators, SOC analysts, threat hunters, and incident responders by automatically correlating DNS request telemetry and mapping it to subsequent IP connections.

Essentials features include:

- All Starter features
- Proxy risky domains for URL and file inspection and selective proxying
- Decrypt and inspect SSL (HTTPS) traffic associated with risky domains using selective proxying
- Access to investigate, perform threat hunting and forensic investigation via the web console for deeper context during an investigation

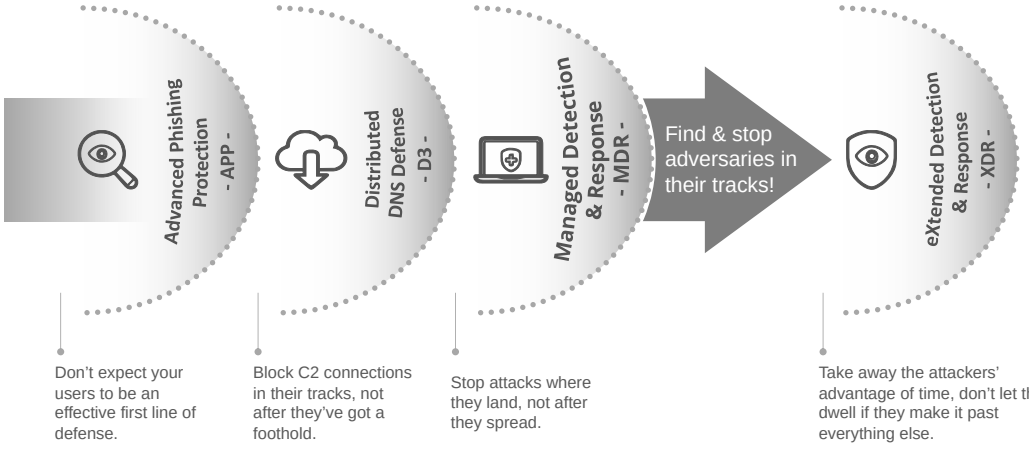
Premium

Premium is made for large enterprises with advanced security and web policy needs. Premium empowers customers to focus only on the incidents that matter, making it the perfect endpoint add-on solution for overstretched IT/SOC Teams. Premium is a fully managed platform including agent updates, incident response and remediation services.

Premium features include:

- All Essentials features
- Proxy all web traffic for URL and file inspection
- Decrypt and inspect all (HTTPS) traffic
- Provide web filtering by domain, URL and category
- See retrospective events for files that were previously considered benign, but were found to be malicious
- Cloud Access Security Broker (CASB)
- Discover and block shadow IT based on URLs
- Create policies with granular control (block uploads, attachments, and posts) for select apps

Accelerate your security maturity. Leverage our layered defense to achieve #cyberresilience in a highly distributed world.



Distributed DNS Defense (ITP)	Starter	Essentials	Premium	Complete
Co-Managed Global SaaS Platform				
Secure Access, High Availability, EPP Policy Administration	✓	✓	✓	
EDR Incident Response & Threat Hunting	✓	✓	✓	
24 x 7 x 365 Security Operations Center and Subscription as a Service	✓	✓	✓	
Real time identification and response to threats by SOC	✓	✓	✓	
Post Action Reports	✓	✓	✓	
DNS-layer security				
Block domains associated with phishing, malware, botnets, etc.	✓	✓	✓	
Block domains based on partner integrations via enforcement APO	✓	✓	✓	
Traffic forwarding				
On and Off-network User Protection	✓	✓	✓	
Always on VPN	✓	✓	✓	
Secure web gateway				
Proxy web traffic for inspection		✓	✓	
Decrypt and inspect SSL (HTTPS) traffic		✓	✓	
Create custom block/allow lists		✓	✓	
Block URLs based on threat feeds, and block files based on AV		✓	✓	
Investigate				
Console for interactive threat intelligence		✓	✓	
Aggregate threat activity across offerings		✓	✓	
Cloud Access Security Broker (CASB)				
Discover and block shadow IT, with App Discovery report			✓	
Create granular controls (block uploads, attachments, and posts) for apps			✓	

Windows agents
All Windows workstation starting with 7 SP1 through Windows 11

All Windows Server starting with 2008 R2 SP1 through Server 2022

Mac agents
Big Sur, Monterey, Ventura, Sonoma

Windows Legacy agents
XP, Server 2003 & 2008, POS2009

Linux agents
Ubuntu, Redhat (RHEL), CentOS, Oracle, Amazon AMI, SUSE Linux Enterprise Server, Fedora, Debian, Virtuozzo, Scientific Linux

Container Support
N/A

Virtualization & VDI
Citrix XenApp, Citrix XenDesktop, Oracle VirtualBox, VMware vSphere, VMware Workstation, VMware Fusion, VMware Horizon, Microsoft Hyper-V