Forcepoint™ was created to empower organizations to drive their mission forward by safely embracing transformative technologies – cloud, mobility, Internet of Things (IoT), and others – through a unified, cloud-centric platform that safeguards users, networks and data, while eliminating the inefficiencies involved in managing a collection of point security products.

Our platform protects against threats from insider threats (accidental and malicious) as well as outside attackers, rapidly detects breaches, minimizes “dwell time” – the period between compromise and remediation – and stops theft. We safeguard users, networks and data in the cloud, in the field and in the office throughout the entire threat lifecycle.

Our approach is to provide a unified cloud-centric platform to defend against attacks, detect suspicious activity sooner, and give the context needed to decide what actions to take to defeat the attack and stop data theft. We protect the data that guides and guards the mission. Defend, Detect, Decide, and Defeat – this is our vision for Forcepoint 4D Security.
Cross Domain Solutions for Secure Data Access and Transfer

**Trusted Thin Client** - Gives users secure, simultaneous access to information on any number of networks from a single endpoint. Designed for enterprise deployments, Trusted Thin Client provides administrators with centralized management and monitoring, scalability to easily add networks and clients and the flexibility to enable users in offices, in-theater and in the field.

**High Speed Guard** - Permits highly complex, bi-directional, automated data transfers between multiple domains, specializing in real-time streaming video. High Speed Guard has demonstrated the fastest bi-directional transfer rates of more than nine gigabits per second (Gb/s) on dual processor commodity servers.

**Small Format Guard** - A small, lightweight, and low-power guard that delivers high throughput and low latency. Ideal for operations outside of traditional data centers, Small Format Guard supports robust security protocols and is adaptable to specific mission needs where strict size, weight, power, and cooling (SWaP-C) specifications are required.

**Trusted Gateway System** - Delivers exceptional built-in manual review and automatic validations, such as virus scanning, file type verification, dirty word search and deep content inspection, enabling safe and simultaneous data movement between networks at different sensitivity levels.

**Trusted Print Delivery** - Allows users to print from existing applications at different security or sensitivity levels to a single printer located on the high-side network. Because it enables reduced printer hardware at individual security levels, it reduces capital investment, printer inventory, hardware maintenance/supplies and administration.

**Trusted Mail System** - Enables the policy-enforced exchange of emails and attachments between users on different networks eliminating the need to switch between email systems at multiple levels. Trusted Mail System provides a ‘single inbox’ that consolidates email and calendar entries residing on multiple networks, at the highest level, making it less likely that important and mission-sensitive email communications are overlooked.

**SimShield** - A fixed-format data guard with the capability to label, segregate, protect, and exchange data between systems executing at different sensitivity or classification levels. SimShield meets the data format, near real-time performance, and low latency requirements for distributed simulation operations, live training exercises, and test events.

**WebShield** - Delivers secure web search and browse-down capabilities from high side networks to lower level networks. Users surfing lower level networks can be restricted to specific server and file types as defined by security policies. All requests, responses and transfers go through security controls, such as, dirty word search, virus scan and malicious content checks.
Insider Threat Data Protection

**SureView® Insider Threat** - Enables safe and effective use of mission-critical technologies by capturing technically observable human behaviors that include policy violations, compliance incidents, or malicious acts that may be warning signs of an impending breach. SureView Insider Threat provides all the details, insight, and complete context using video replay to immediately assess the severity of the threat, remediate the problem, and build the policies to prevent it from happening in the future.

**TRITON® AP-DATA** – Provides you with the defenses you need to protect your sensitive data wherever it resides — on endpoints, in the cloud, or on-premise. Its powerful Data Loss Prevention (DLP) functionality and other features help you secure financial records, intellectual property, personally identifying information (PII), and other sensitive data, while a user-friendly wizard makes it easy to deploy. For even greater protection against malicious or careless insiders, combine AP-DATA with SureView Insider Threat.

**TRITON AP-ENDPOINT** - Protects your users against data theft, whether they are on or off the organization’s network. Its powerful DLP capabilities enable you to secure personal data, intellectual property, and other sensitive information on MacOS, Linux®, or Windows® endpoints. Additionally, its preconfigured policies allow you to quickly and easily meet compliance requirements.

www.forcepoint.com
Network Security

Stonesoft® Next Generation Firewall - Integrates application control, sophisticated evasion prevention and an intrusion prevention system (IPS) into a single solution that is cost-effective and easy to deploy. It has a proven capability to identify advanced evasion techniques (AETs) that evade other devices, and delivers exfiltration protection using both application and endpoint intelligence.

Content Security

TRITON APX Suite - TRITON APX solutions share a common architecture based on the TRITON ACE and ThreatSeeker® Intelligence Cloud, which work together in real time to accurately identify and classify network traffic, apply policies and detect threats.

TRITON APX's unified management and reporting functions streamline work for your security team, giving them the context and insights they need to make more informed decisions, minimize the dwell time of attacks and prevent the exfiltration of your sensitive data.

The common architecture makes it simple to deploy any combination of TRITON AP-WEB, TRITON AP-EMAIL, TRITON AP-DATA, and TRITON AP-ENDPOINT, and we have made it easy to purchase with our TRITON APX Enterprise bundle. TRITON APX solutions easily integrate with Threat Protection Cloud and SureView Insider Threat.

TRITON AP-EMAIL - Protects against multi-stage advanced threats that often exploit email to penetrate your IT environment. Identifies targeted attacks, high-risk users, and Insider Threats while empowering mobile workers and safe adoption of new technologies like Microsoft® Office 365™.

TRITON AP-WEB - Provides comprehensive real-time, inline protection against advanced threats that use sophisticated techniques to evade detection while they're stealing your sensitive data, as well as insider threats, such as employee theft and malware, that slips into your network. Offers deployment options for both on-premise and remote users.

Websense® Web Filter and Security - Blocks Web threats to reduce malware infections, decrease help-desk incidents and free up valuable IT resources. With more than 120 security and filtering categories, hundreds of Web application and protocol controls, and 60-plus reports with customization and role-based access, Web Filter & Security is an easy-to-deploy, transparent filter and security solution that avoids the complexity of a proxy gateway.
Security for Cloud

TRITON AP-EMAIL Cloud - Gives you the security you need by protecting you against multi-stage advanced threats that often exploit email to penetrate your IT defenses and is available in the cloud. It applies thousands of real time threat analytics, behavioral sandboxing and other advanced defense technologies to identify targeted attacks.

TRITON AP-WEB Cloud – Makes available via the cloud comprehensive real-time protection against advanced threats that use sophisticated techniques to evade detection while they are stealing your sensitive data, as well as insider threats, such as employee theft and malware that slips into your network.

TRITON RiskVision - Uses industry-leading threat analytics, security intelligence, and behavioral sandboxing to deliver visibility into advanced threats, along with an extensible platform for additional threat detection. It gives you the information you need to detect attacker movement and get back to normal quickly after an attack occurs.

Threat Protection for Linux - Makes use of memory forensics to acquire and analyze volatile memory from Linux® systems providing malware detection using an integrity verification approach to validate that all software running is known and unaltered. When responding to a confirmed or potential computer security incident on a Linux system, Threat Protection for Linux quickly highlights stealth malware, unknown, or unauthorized programs and other potential indicators of compromise and vulnerability.

Our unified, cloud-centric security platform and robust multilevel security solutions safeguard users, data and networks.