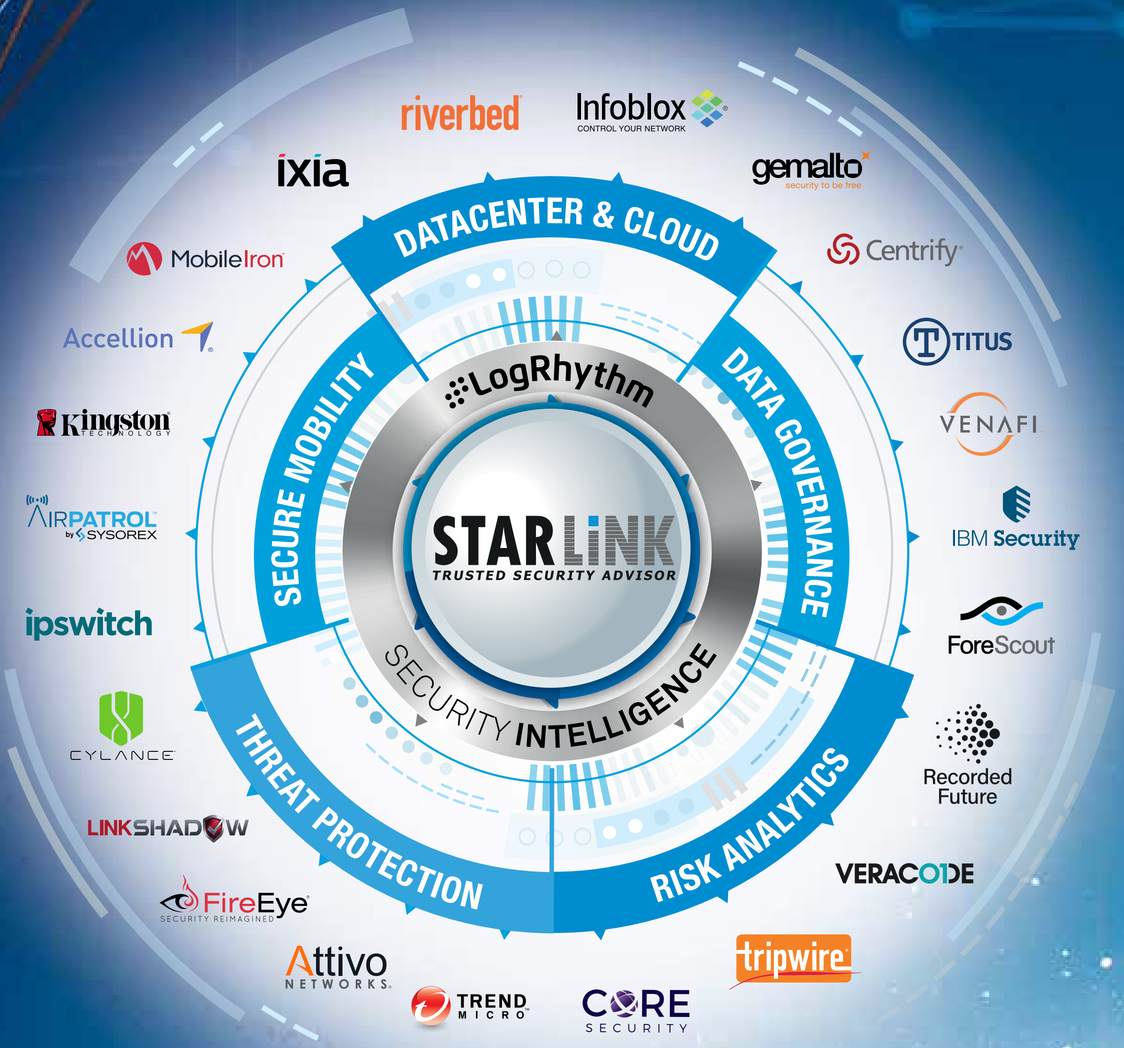
STARLINK

TRUSTED SECURITY ADVISOR

TRUE VALUE-ADDED IT SECURITY DISTRIBUTOR



MOMENTUM

THE POWER BEHIND STARLINK

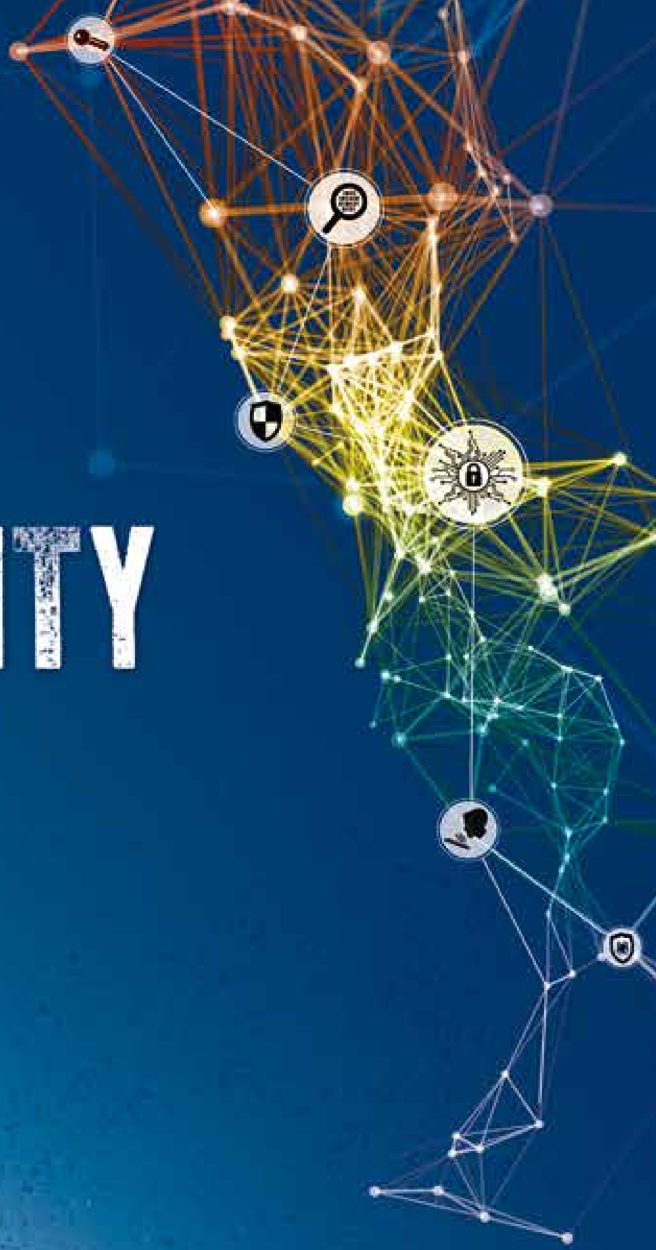
STARLINK
TRUSTED SECURITY ADVISOR

MOMENTUM

THE POWER BEHIND STARLINK

CELEBRATING ELEVEN YEARS OF TRUST

LARGEST AND FASTEST GROWING TRUE IT SECURITY VAD FOR 11 YEARS, AND SUSTAINING...



MOMENTUM

THE POWER BEHIND STARLINK

Who We Are

StarLink is acclaimed as the largest and fastest growing "True" Value-Added IT Security Distributor across the Middle East, Turkey and Africa regions with on-the-ground presence in 11 countries.

With its innovative Security Framework and Vertical Security Trend Matrix StarLink is also recognized as a "Trusted Security Advisor" to over 1000 enterprise and government customers that use one or more of StarLink's best-of-breed and market-leading technologies, sold through our Channel network of over 250 Partners.

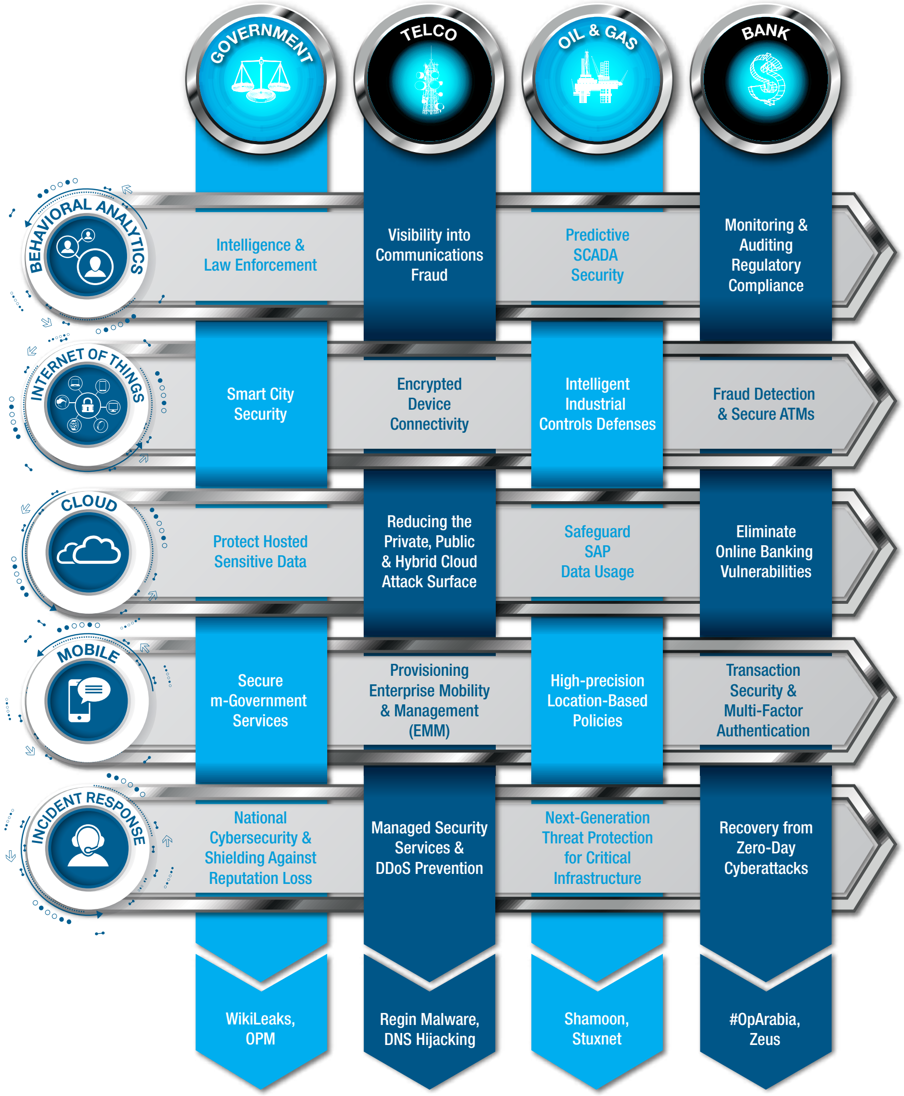
The StarLink Solutions Lifecycle helps Channel Partners differentiate offerings, and assists customers to identify key risks and define priorities for addressing IT Security gaps relating to compliance and next-generation threat protection.

GLOBAL PRESENCE IN 11 COUNTRIES, AND EXPANDING . . .

MOMENTUM

THE POWER BEHIND STARLINK

Overview



	GOVERNMENT	TELCO	OIL & GAS	BANK
BEHAVIORAL ANALYTICS	Intelligence & Law Enforcement	Visibility into Communications Fraud	Predictive SCADA Security	Monitoring & Auditing Regulatory Compliance
INTERNET OF THINGS	Smart City Security	Encrypted Device Connectivity	Intelligent Industrial Controls Defenses	Fraud Detection & Secure ATMs
CLOUD	Protect Hosted Sensitive Data	Reducing the Private, Public & Hybrid Cloud Attack Surface	Safeguard SAP Data Usage	Eliminate Online Banking Vulnerabilities
MOBILE	Secure m-Government Services	Provisioning Enterprise Mobility & Management (EMM)	High-precision Location-Based Policies	Transaction Security & Multi-Factor Authentication
INCIDENT RESPONSE	National Cybersecurity & Shielding Against Reputation Loss	Managed Security Services & DDoS Prevention	Next-Generation Threat Protection for Critical Infrastructure	Recovery from Zero-Day Cyberattacks
	WikiLeaks, OPM	Regin Malware, DNS Hijacking	Shamoon, Stuxnet	#OpArabia, Zeus

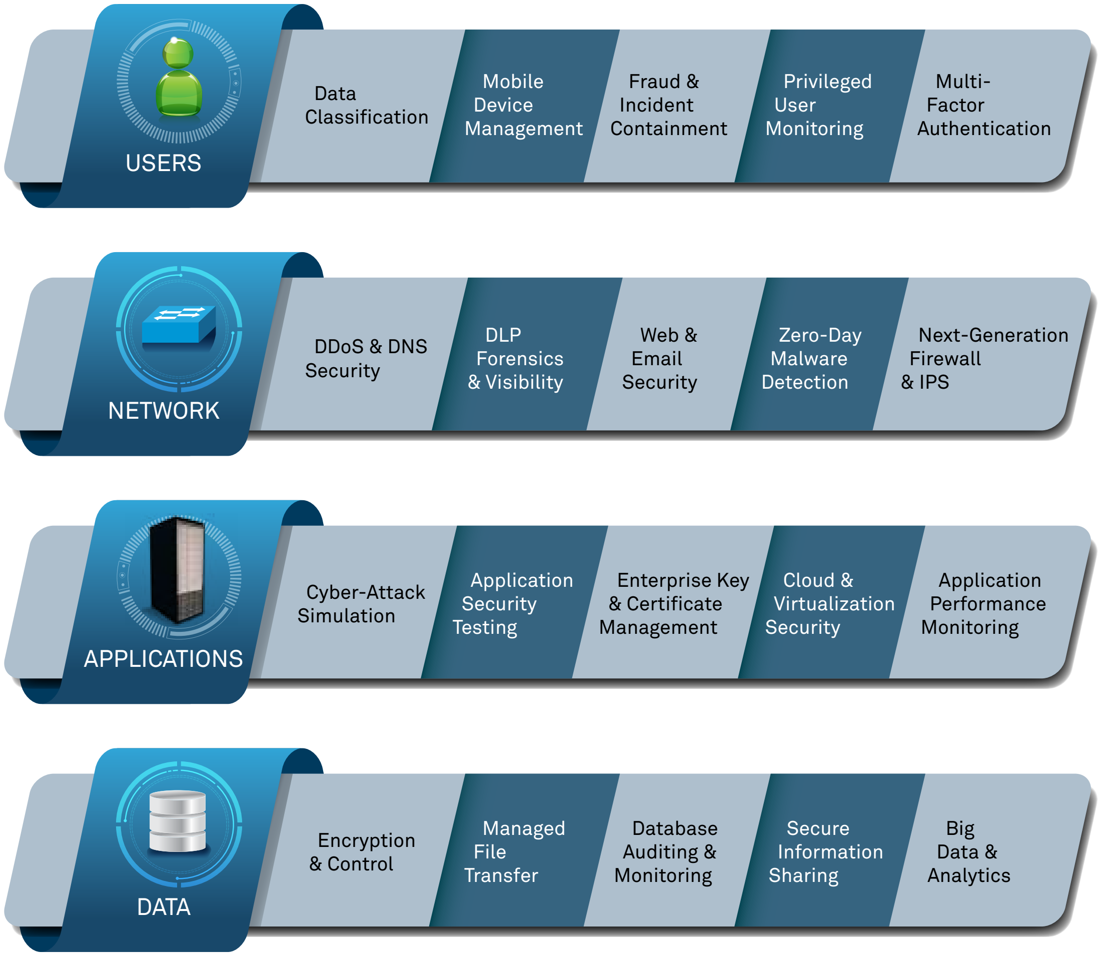
StarLink Vertical Security Trend Matrix

In recent years we have seen many changes in IT security. In an attempt to keep up with new and increasing threats to enterprise and government entities, traditional approaches to IT Security have limited impact. Organizations are dedicating more resources to IT Security and risk but attacks and vulnerabilities are increasing in frequency and sophistication.

The StarLink Vertical Security Trend Matrix provides Security leaders in the key verticals of Government, Telco, Oil & Gas and Banking, insight into how the latest IT Security trends cater to their respective industries, in order to address today's compliance and next-generation threat protection requirements.

The top 5 IT Security trends are namely, Behavioral Analytics, Internet of Things, Cloud, Mobile and Incident Response.

Overview



USERS	Data Classification	Mobile Device Management	Fraud & Incident Containment	Privileged User Monitoring	Multi-Factor Authentication
NETWORK	DDoS & DNS Security	DLP Forensics & Visibility	Web & Email Security	Zero-Day Malware Detection	Next-Generation Firewall & IPS
APPLICATIONS	Cyber-Attack Simulation	Application Security Testing	Enterprise Key & Certificate Management	Cloud & Virtualization Security	Application Performance Monitoring
DATA	Encryption & Control	Managed File Transfer	Database Auditing & Monitoring	Secure Information Sharing	Big Data & Analytics

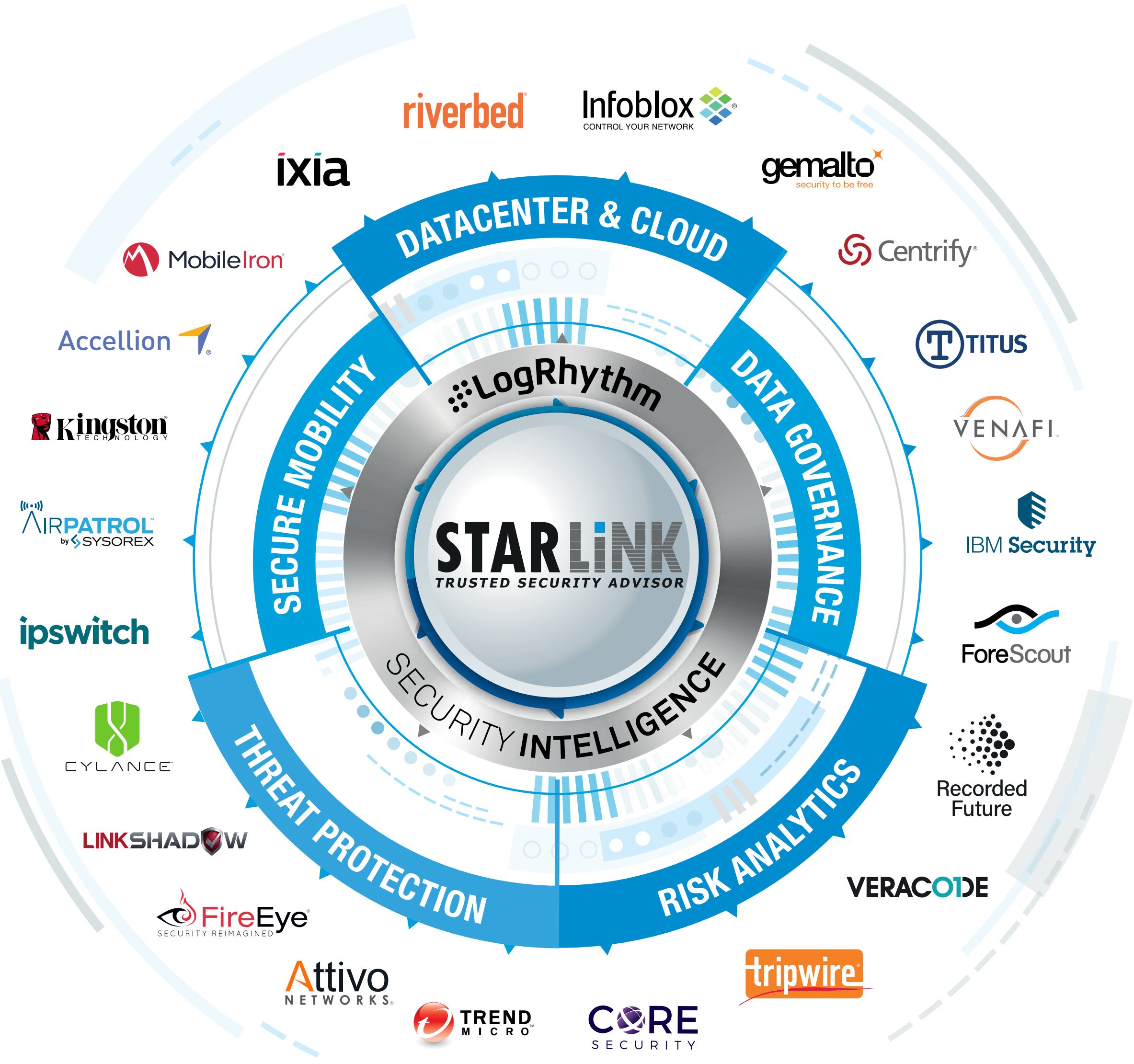
StarLink Security Framework

IT Security is a fragmented market, proliferated with many point products that are designed to address specific risks, and which may meet targeted compliance goals, but these solutions typically fail to provide a comprehensive, integrated picture of the threat landscape.

Instead of organizations becoming more relevant and agile in their response to security challenges, increased complexity is created that can overwhelm IT Security teams. The challenge is compounded by patient attackers, sophisticated advanced threats, and the increasing use of cloud and mobile technologies, which expand the potential attack surface.

To successfully deliver security capable of addressing today's risks, organizations need to take a holistic approach to IT Security. The StarLink Security Framework provides a strategic approach that cuts through the clutter and is designed to simplify risk management and ensure that all critical controls for effective enterprise IT Security are in place.

StarLink delivers real value to customers and partners with its vendor-agnostic and technology-centric Security Framework. Decision-makers can quickly and easily visualize multiple security domains to help understand, prioritize and mitigate risk. The innovative defense-in-depth Security Framework helps customers define their strategic objectives, top-down. Customers are able to comprehensively achieve their IT security vision, from the User to the Network to the Application and finally to the Data.



StarLink Solutions Lifecycle

IT security challenges can no longer be addressed by point products. Such products typically fail to provide a comprehensive, integrated picture of the threat landscape, each returning its own results but missing the opportunity to put results into context, falling short of enterprise-wide insights, and increasing the complexity of managing the IT security platform. At the root of the problem is the fact that most point solutions operate in silos; they typically do not integrate with other products in the security infrastructure. It becomes difficult for the security team to see through the noise and understand where real threats and real vulnerabilities are hidden.

An integrated approach requires capabilities to achieve compliance, as well as, to monitor for and prevent attacks on the network, on the endpoint and across other IT assets. Detected security concerns must be investigated quickly with tools that can integrate context from across the environment with the passing of security information, alerts and policies between security domains. Once this analysis is complete, security gaps can be bridged, and ongoing protection can be implemented. This methodology allows for faster, more effective identification and mitigation of potential security threats, as well as, helps in identification of behavior anomalies, risk prioritization, and increased visibility and control.

StarLink's portfolio has evolved into a uniquely integrated Solutions Lifecycle consisting of Datacenter & Cloud, Data Governance, Risk Analytics, Threat Protection, Secure Mobility, Incident Response, and Operational Intelligence. Each of these solutions comprise of vendors' core competencies, and feed into each other giving customers the ability to quickly understand their IT Security gaps, and set priorities accordingly, starting from achieving effective application performance and traffic visibility, to implementing critical controls, to verification of those controls, to zero-day malware protection, to sensitive data consumption, to remediation of next-generation threats, and then back around again, while centrally consolidating visibility of all machine data to generate valuable insights.

EXPONENTIAL REVENUE AMBITION AT $145 MILLION, AND HIGHER . . .

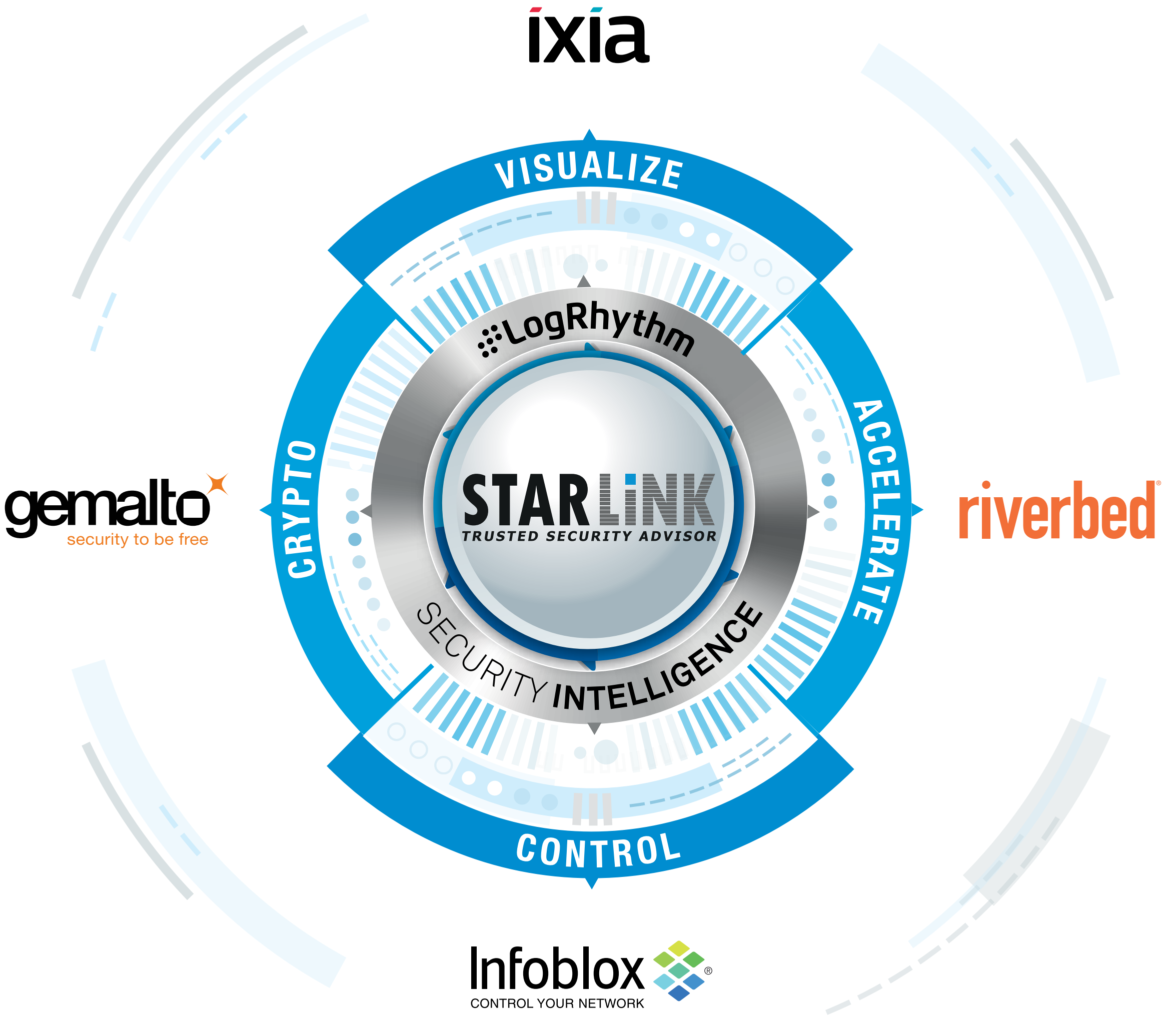
MOMENTUM

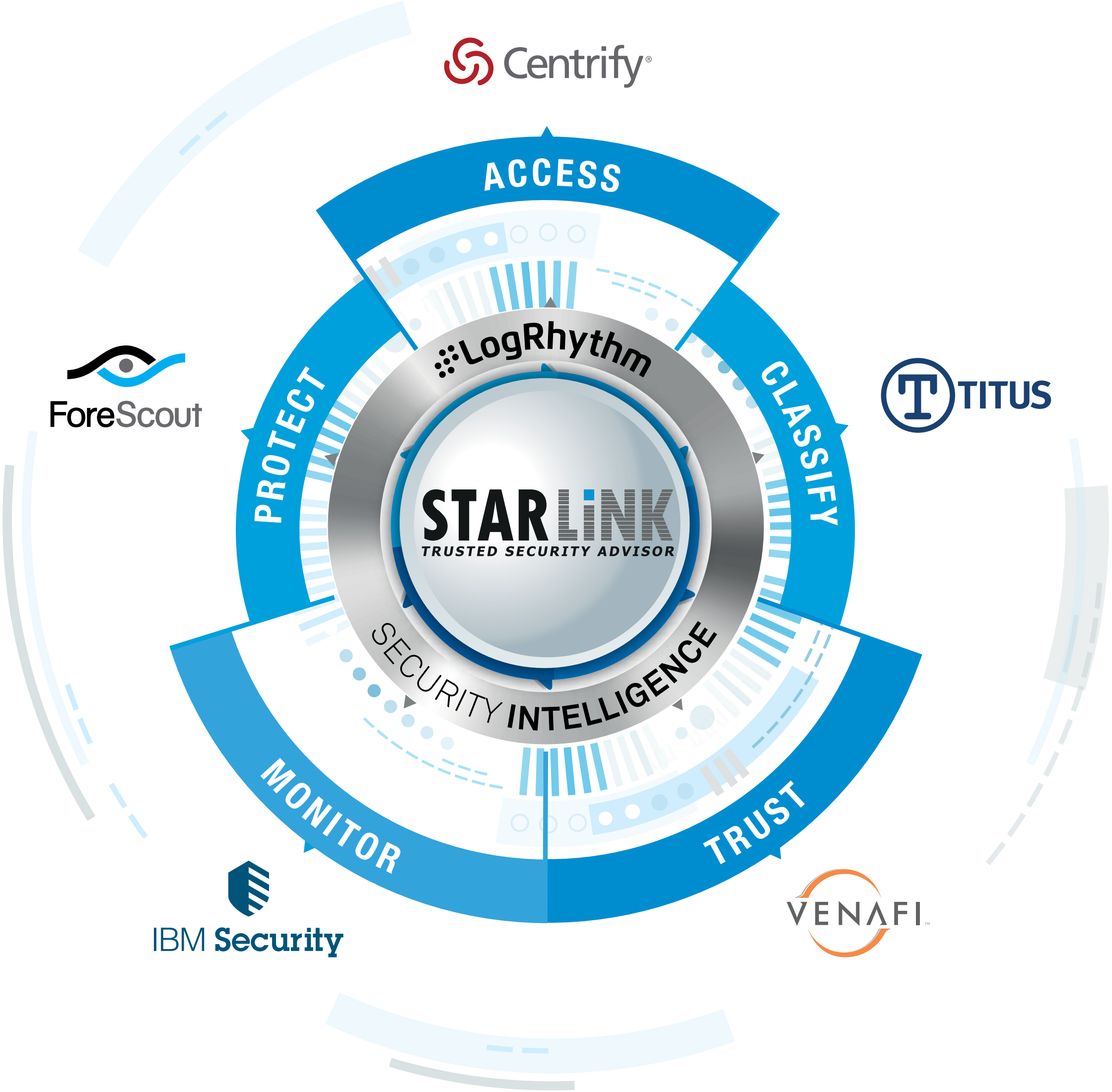
THE POWER BEHIND STARLINK

Datacenter & Cloud

Is my Sensitive Data optimized?

Increasing Datacenter & Cloud performance and accelerating delivery, positively impacts storage, network and application environments, enabling the rapid detection of issues while securing sensitive data to minimize risk and ensure business continuity. Furthermore automation of network services for cloud and virtualization allows for enforcement of security policies, as well as, configuration and change management. Finally, more devices are now connecting to more data from more sources, which creates network blind spots and have become a costly and risk-filled challenge. It is therefore critical to deploy a highly scalable visibility and secure DNS architecture that enables the elimination of current blind spots, while providing resilience and control to sensitive data without added complexity.





Data Governance

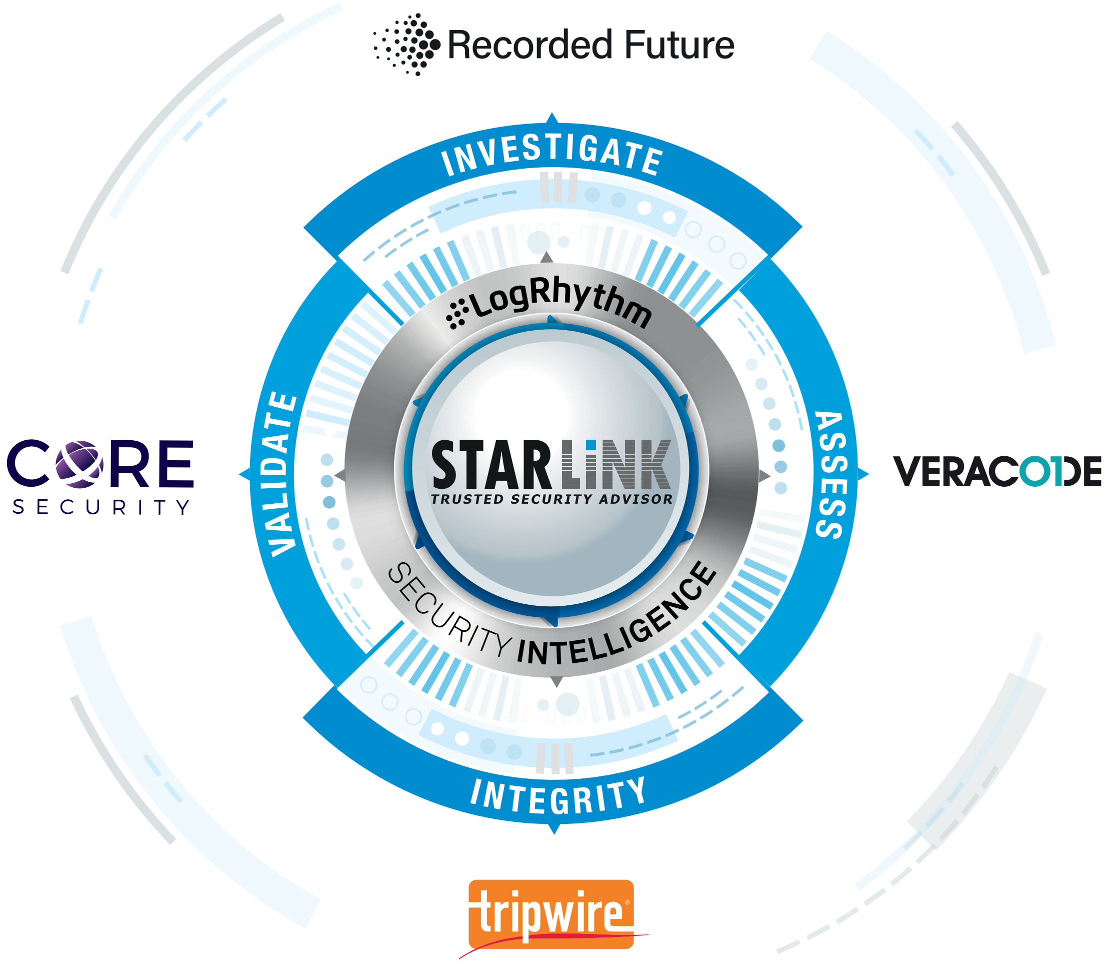
Where is my Sensitive Data?

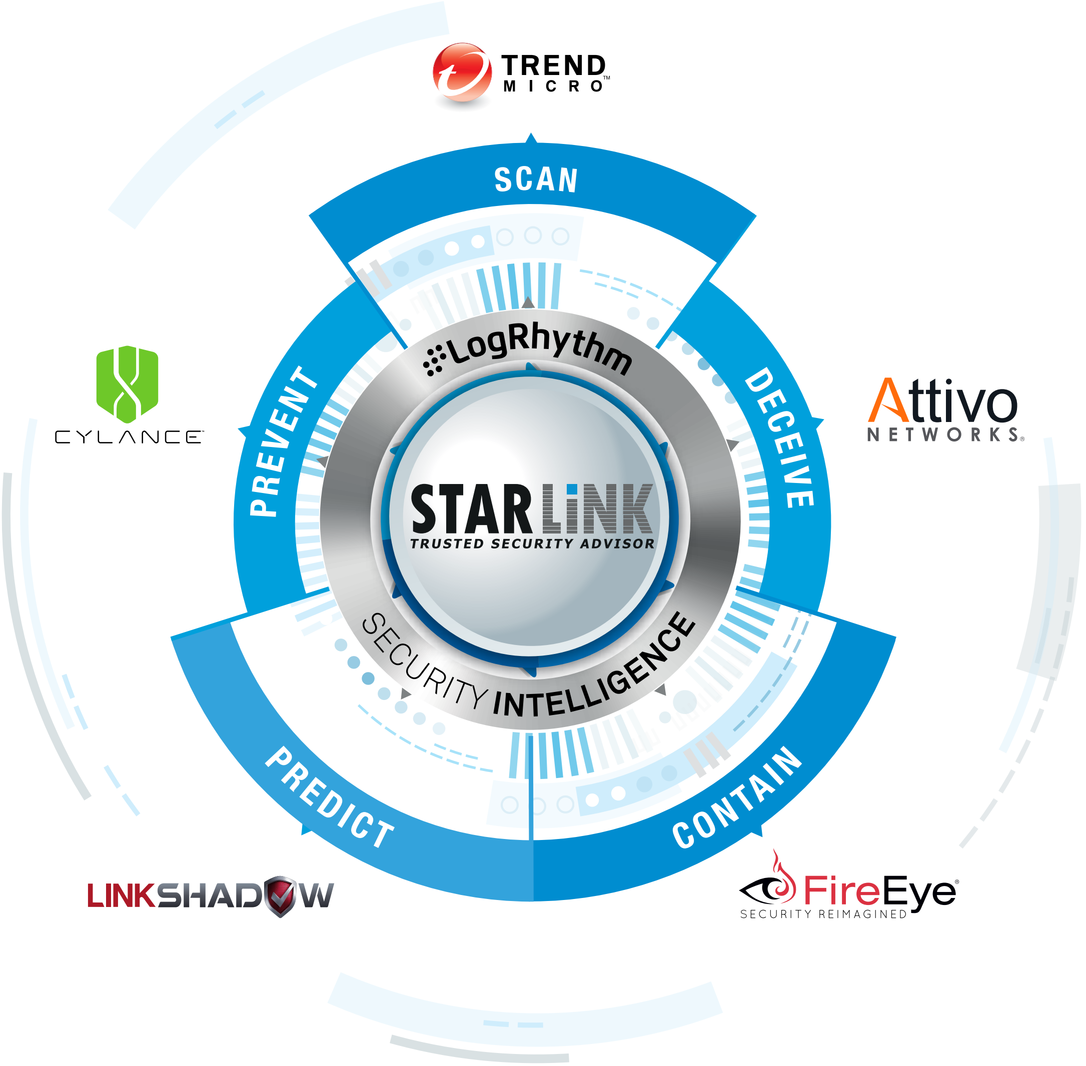
Data Governance enables the organization to control access to sensitive data by understanding user privileges, securing privileged access and monitoring changes to directories, files, data repositories and databases, as well as, user activity. This in turn leads to alerts ensuring that sensitive data is only accessed by authorized users by providing comprehensive real-time visibility into all activities. Furthermore, classification mechanisms are put in place to guarantee that sensitive data cannot be leaked to unauthorized users. Finally the required processes and procedures to achieve continuous compliance are automated so that human error or risk of insider threats are minimized.

Risk Analytics

Is my sensitive data at risk?

Risk Analytics ensures continuous monitoring of the entire corporate network and generates lists of vulnerabilities and deep risk metrics prioritized by importance for the IT Security decision maker. To ensure that the vulnerabilities are in fact relevant and do exist in context for the organization, it is then critical to automate the penetration testing of each of the vulnerabilities so that the list can be narrowed down to what is truly important to look at right away. It is also crucial to automatically produce a visual network topology map in order to understand how vulnerabilities at the network level, due to security configuration not being compliant in some areas of the network, can affect other areas of the network. This enables organizations to create threat models to proactively understand where threats can come from. Finally, many modern threats today, whether they be internal or external, can impact the entire network stack, and require effective traffic visibility and network forensics capabilities.





Threat Protection

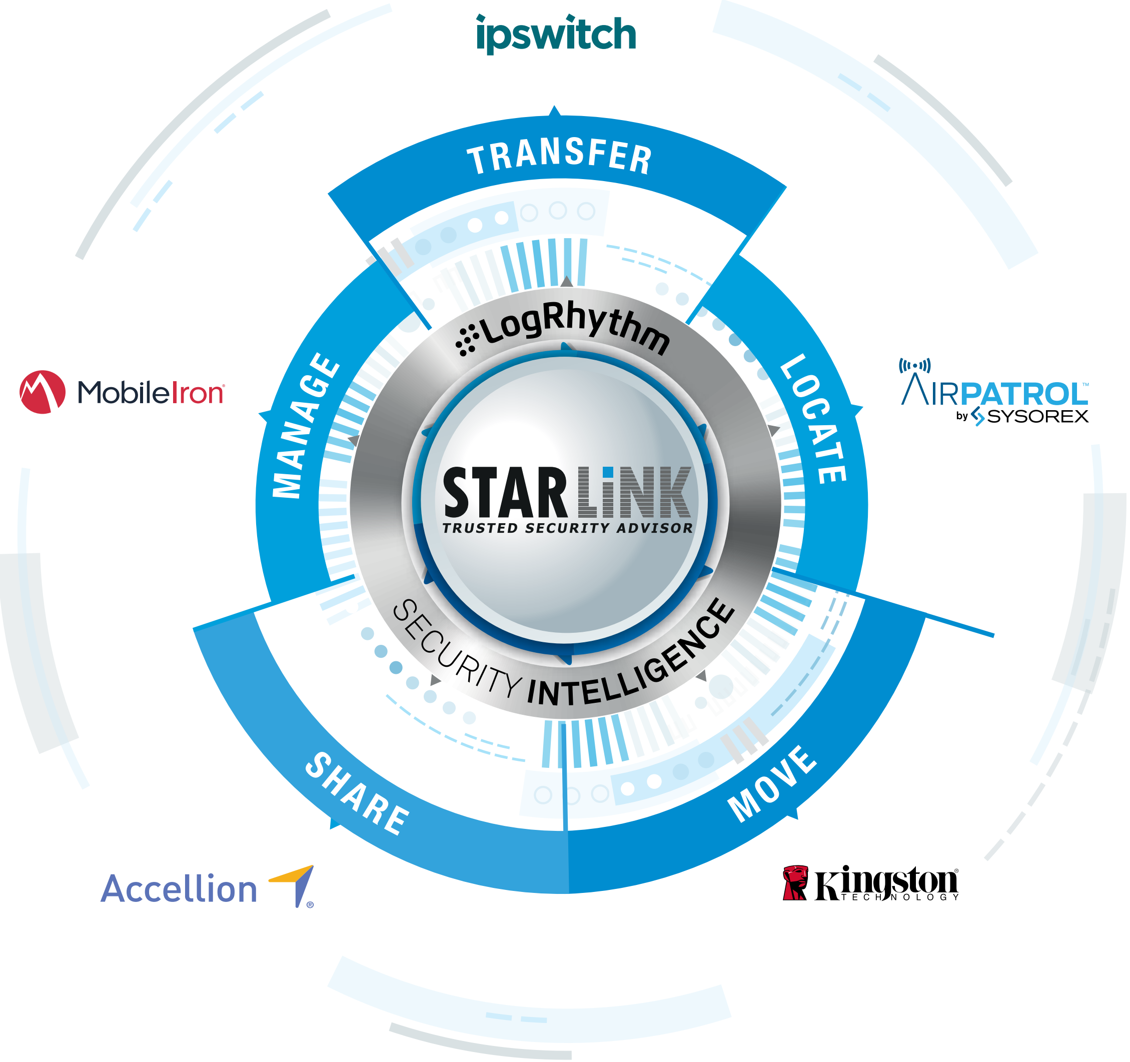
How can I protect my sensitive data?

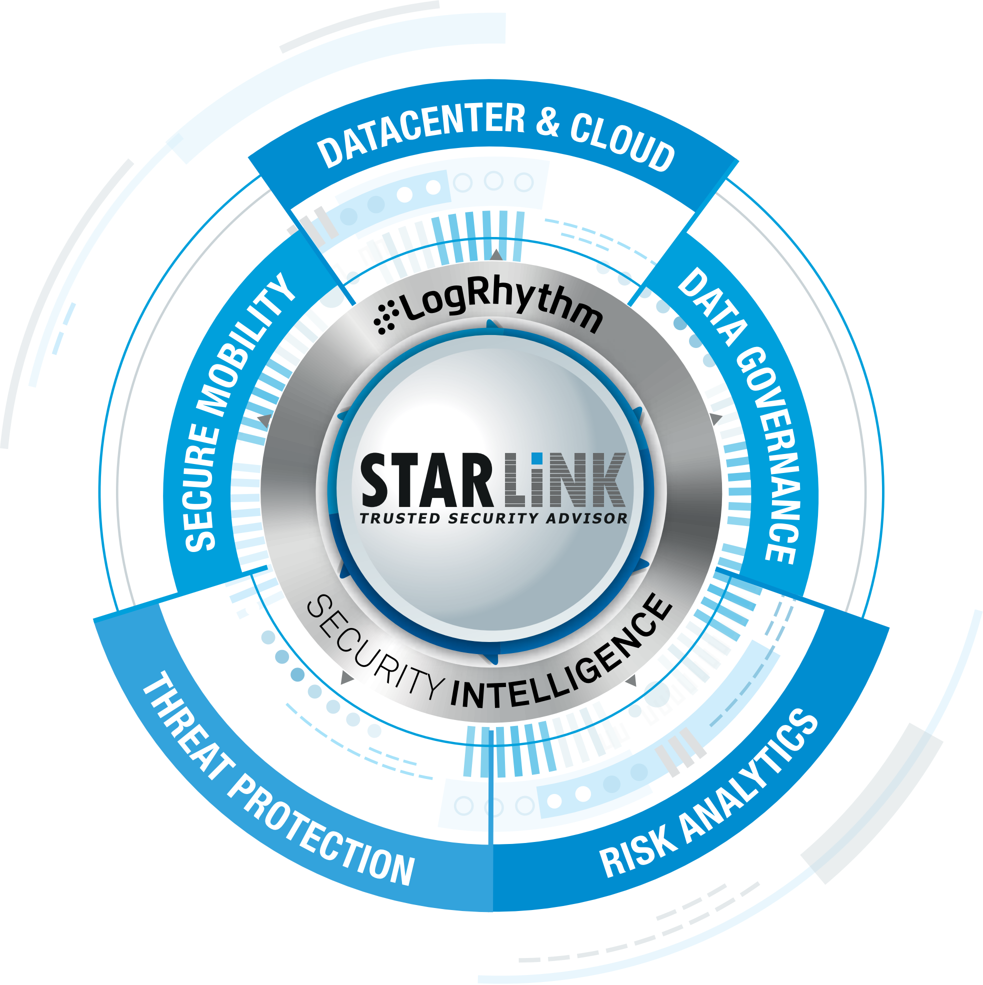
Threat Protection provides visibility into all relevant network traffic coming in and going out of the organization. This ensures that protection mechanisms are applied only where attacks can happen by analyzing the required traffic, web, email, file etc., to determine whether the traffic contains signature-based or signature-less threats that attempt to do damage or communicate back to a command and control centers (CnCs) for data exfiltration, and to stop any such communication. Once malware does enter a corporate environment, it is crucial to gain security intelligence into where it attempts to travel within the corporate network and protect endpoints and the datacenter. Simultaneously, a platform needs to be in place to ensure that any unknown malware cannot execute on any IT-managed resource so as to avoid any adverse direct effects to the computing environment. Finally with effective and powerful authentication, encryption and key management, data is always safe even if it falls into the wrong hands.

Secure Mobility

How do I share my sensitive data?

Secure Mobility enables collaboration of sensitive data by putting platforms into place to ensure that managing mobile devices, sharing of files and distributing content is done securely, both internal, as well as, external to an organization, so that data cannot be maliciously or mistakenly leaked. It is even possible to control from which location inside an organization that a user can access sensitive data. Secure file sharing can seamlessly automate secure site-to-site and user-to-site transfers, as well as, use email to securely send and receive large attachments without restrictions. Finally sensitive data needs to be available today to the mission-critical workforce, 24x7 online, as well as offline. So portability being critical, trusted users can securely transport data, and even their entire workspace environment, on hardware-encrypted portable storage, with comprehensive management of this media.





Operational Intelligence

How do I visualize my Sensitive Data?

Operational Intelligence provides real-time understanding of machine data across IT systems and technology infrastructure so that informed decisions can be made. All websites, communications, networking and complex IT infrastructures generate massive streams of machine data constantly. This machine-generated data holds critical information on user behavior, security risks, capacity consumption, service levels, fraudulent activity, customer experience and much more. By implementing effective centralized dashboards, business activities can be monitored across multiple tools facilitating the identification and detection of situations relating to inefficiencies, opportunities, and threats and provide operational solutions.

EXPERT WORKFORCE OF 220 EMPLOYEES, AND INCREASING...

MOMENTUM
THE POWER BEHIND STARLINK

Network Visibility, Tap & Packet Broker

ixia

ixiacom.com

Ixia is a leading provider of network performance solutions that enable organizations to achieve optimized application and service delivery. Ixia's network lifecycle solutions enable customers to assess and validate the scale, performance, and security of network infrastructure, devices and services, including resiliency testing and validation with real-world application traffic and attack simulation, and deliver end-to-end visibility across physical and virtual networks by providing access to data from any point in the network.

Infoblox is the leader in Automated Network Control. Unlike traditional networks which are manual, fragile and vulnerable–Infoblox technologies make essential services of the modern network (such as DNS, DHCP and IP Address Management), automated, resilient and performing at their highest levels. Infoblox revolutionized network services in 1999 when we delivered the first hardened DNS appliance, bringing a level of security and reliability network managers could not achieve previously. Infoblox has led the market ever since, and have the largest installed base of DNS, DHCP and IP address management (DDI) appliances.

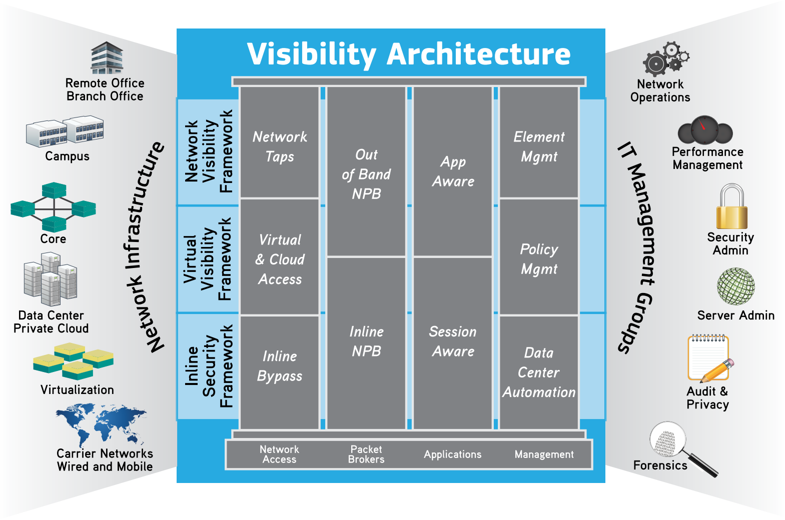
The Ixia Visibility Architecture

More mobile devices are now connecting to more data from more sources. IT challenges are complicated by increasingly high customer expectations for always-on access and immediate application response. This complexity creates network "blind spots" where latent errors germinate and pre-attack activity lurks. Stressed-out monitoring systems make it hard, if not impossible, to keep up with traffic and filter data "noise" at a rate that they were not designed to handle. Network blind spots have become a costly and risk-filled challenge for network operators.

PROTECTION AGAINST WIDEST RANGE OF DNS ATTACKS

The answer to these challenges is a highly scalable visibility architecture that enables the elimination of network "blind spots", while providing resilience and control without added complexity.

The Ixia Visibility Architecture is built on the industry's most comprehensive network visibility product portfolio and includes network access solutions, network packet brokers, application and session visibility solutions, and an integrated management platform.



WAN Optimization & Application Performance Platform

riverbed

riverbed.com

The Riverbed Application Performance Platform [illegible] complete platform for location-independent computing. [illegible] to power their business applications [illegible] Riverbed technology [illegible] namely through SteelHead, SteelCentral and SteelFusion [illegible] WAN optimization, APM/NPM and [illegible] IT to drive better business outcomes.

The Nutanix Xtreme Computing Platform is a 100% software-driven infrastructure solution that natively converges storage, compute and virtualization into a turnkey appliance that can be deployed in minutes to run any application out of the box. Datacenter capacity can be easily expanded one node at a time, with no disruption, delivering linear and predictable scalability with pay-as-you-grow flexibility. Nutanix eliminates complexity and allows [illegible]

SteelHead is the industry's #1 optimization technology for accelerated delivery of all applications across the hybrid enterprise [illegible] applications.

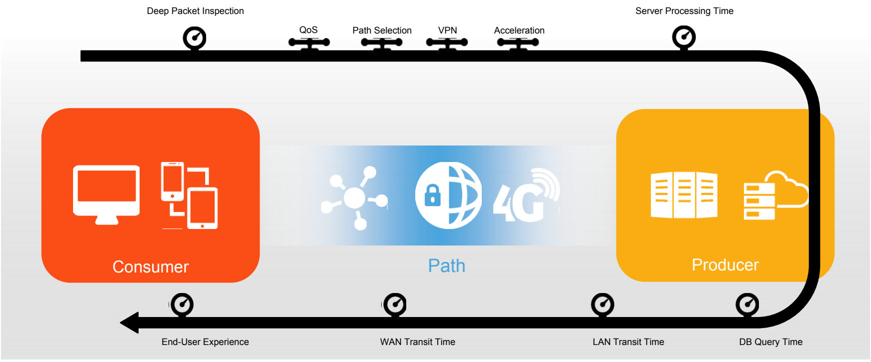
Nutanix is built with the same web-scale technologies and architecture that power leading internet companies such as Google, Facebook, and Amazon – and now any enterprise. The Xtreme Computing Platform brings together web-scale engineering with consumer-grade management to make infrastructure invisible and elevate IT teams so they can focus on what matters most – applications.

SteelCentral drastically reduces [illegible] Riverbed performance management [illegible] end-to-end visibility to detect and resolve issues before end users notice.

At the heart of the Xtreme Computing Platform are two products, Nutanix Acropolis and Nutanix Prism. Acropolis provides a distributed storage fabric [illegible] application mobility fabric that enables workloads to move freely between virtualization environments without penalty. Nutanix Prism, a comprehensive management solution for Acropolis, delivering unprecedented one-click simplicity to the IT infrastructure lifecycle.

SteelFusion is the first and only hyper-converged infrastructure for branch IT, enables 100% consolidation of branch data and servers from remote sites into data centers, delivering complete data security and centralized data protection, without compromising on any of the benefits of running branch services locally for your users. SteelFusion eliminates the need for physical servers, storage and backup infrastructure at branch locations, creates the ability to instantly provision and recover branch services, and provides full visibility and superior performance of on-premises and cloud-based applications, leading to dramatic increases in data security, business continuity, agility and operational efficiency.

End-to-End Visibility, Optimization, and Control



DNS, DHCP & IP Address Management

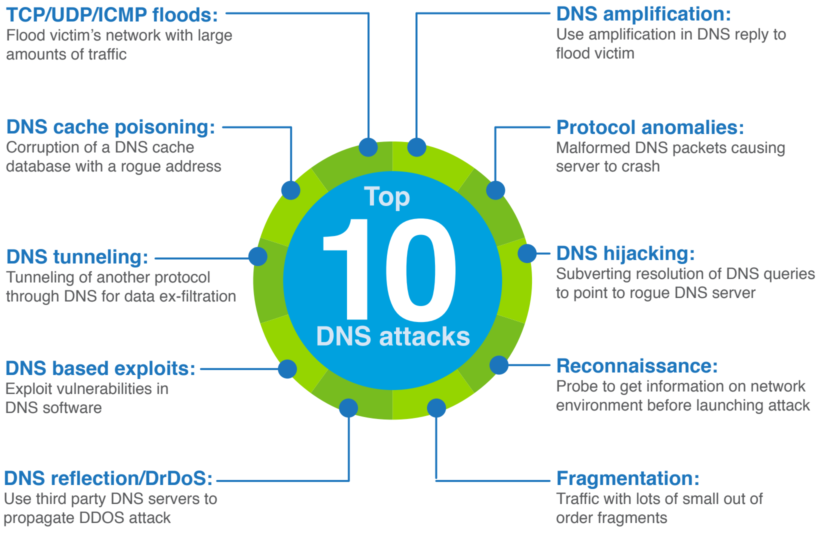
Infoblox
CONTROL YOUR NETWORK

infoblox.com

Infoblox is the leader in Automated Network Control. Unlike traditional networks which are manual, fragile and vulnerable–Infoblox technologies make essential services of the modern network (such as DNS, DHCP and IP Address Management), automated, resilient and performing at their highest levels.

Infoblox revolutionized network services in 1999 when we delivered the first hardened DNS appliance, bringing a level of security and reliability network managers could not achieve previously. Infoblox has led the market ever since, and have the largest installed base of DNS, DHCP and IP address management (DDI) appliances.

PROTECTION AGAINST WIDEST RANGE OF DNS ATTACKS



TCP/UDP/ICMP floods: Flood victim's network with large amounts of traffic

DNS amplification: Use amplification in DNS reply to flood victim

DNS cache poisoning: Corruption of a DNS cache database with a rogue address

Protocol anomalies: Malformed DNS packets causing server to crash

DNS tunneling: Tunneling of another protocol through DNS for data ex-filtration

DNS hijacking: Subverting resolution of DNS queries to point to rogue DNS server

DNS based exploits: Exploit vulnerabilities in DNS software

Reconnaissance: Probe to get information on network environment before launching attack

DNS reflection/DrDoS: Use third party DNS servers to propagate DDOS attack

Fragmentation: Traffic with lots of small out of order fragments

Multi-Factor Authentication, HSM's & Data Encryption

gemalto
security to be free

gemalto.com

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments and data – from the edge to the core.

SafeNet delivers the breadth of solutions that enable security teams to centrally employ defense-in-depth strategies—and ultimately make sure encryption yields true security. If access controls are lacking, the efficacy of encryption can be compromised. If cryptographic keys are vulnerable, so is encrypted data.

To truly protect sensitive data, organizations must follow encryption best practices as well as establish a strong Crypto Foundation — an approach that incorporates crypto processing and acceleration, key storage, key management, and crypto resource management.

Along with a comprehensive set of encryption platforms, SafeNet delivers the robust access controls and key management capabilities that enable organizations to practically, cost effectively, and comprehensively leverage encryption to address their security objectives.

Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

BUILDING ON STRATEGIC RELATIONSHIPS WITH 250 PARTNERS, AND MORE...

MOMENTUM

THE POWER BEHIND STARLINK

Identity and Acccess Management

Centrify®

centrify.com

Centrify is the leader in securing enterprise identities against cyberthreats that target today's hybrid IT environment of cloud, mobile and on-premises. The Centrify Identity Platform protects against the leading point of attack used in data breaches — compromised credentials — by securing an enterprise's internal and external users as well as its privileged accounts. Centrify delivers stronger security, continuous compliance and enhanced user productivity through single sign-on, multi-factor authentication, mobile and Mac management, privileged access security and session monitoring. Centrify is trusted by over 5000 customers, including more than half of the Fortune 50.

WHAT WE DELIVER

Stronger Security + Continuous Compliance + Enhanced User Productivity

Single sign-on	Active directory bridging	Privileged access security
Multi-factor authentication	Mac management	Session monitoring
Provisioning	Enterprise mobility management	Shared password management

User-Centric Data Classification

TITUS

titus.com

TITUS is one of the world's most recognized data security and governance solution providers. Our products assist more than 2 million users in over 100 countries around the world to protect their sensitive information.

Our Difference: Involving the User in Data Security and Governance

A successful data security and governance strategy starts with ensuring that important data assets are formally managed and secured throughout the enterprise. Data security and governance becomes most effective when all employees are involved.

Our Innovation: Ensure the Right Users Have Access to the Right Data

TITUS solutions ensure that information is governed properly by clearly identifying the sensitivity of every piece of information. Once information is identified, organizations can control governance policy to automate data security and information management.

With TITUS, information is clearly identified and easily protected, compliance mandates are being met and inadvertent data loss is radically reduced.

TITUS solutions focus on:

Data Classification – TITUS provides user-friendly solutions to classify information in order to prevent data loss, raise security awareness, and comply with regulations.

Data Loss Prevention – TITUS makes users the first line of defense against data loss and leverages metadata to enhance existing security technologies.

SharePoint Security – TITUS helps organizations ensure the right people have access to the right information in SharePoint.

Data Security and Compliance – TITUS solutions address regulations, standards, government legislated directives, and internal security awareness policies such as ITAR, ISO 27001, NERC and many others.

Enterprise Certificate Management & Auto-Provisioning

venafi.com

Venafi Director
Securing trust. Protecting keys and certificates.

Venafi Director prevents, detects and remediates attacks and policy violations involving cryptographic keys and digital certificates - the foundation of trust for every enterprise. Forrester reports 44% of enterprises have fallen prey to attacks on keys and certificates and existing security systems “are not a substitute for securing keys and certificates that can provide an attacker trusted status that evades detection”.

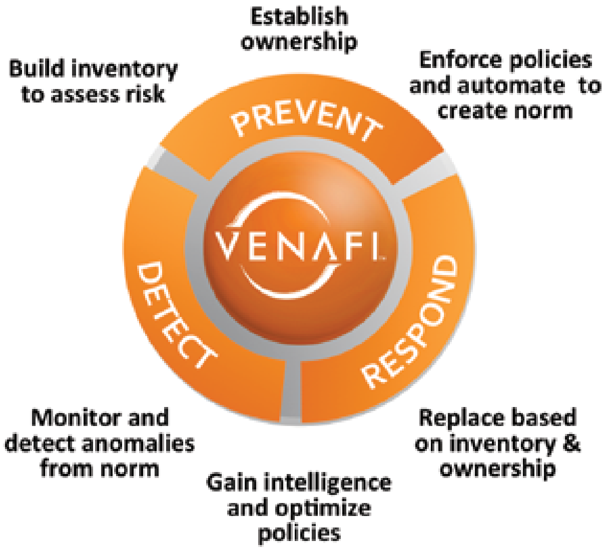
Venafi helps secure and protect keys and certificates by:

Preventing attacks with automated discovery and intelligent policy enforcement.

Detecting and reporting on anomalous activity that deviates from policies.

Remediating anomalies by replacing keys and certificates and returning to a known good state.

Venafi customers include the world’s most prestigious Global 2000 organizations in financial services, insurance, high tech, telecommunications, aerospace, healthcare and retail.


Establish ownership
Build inventory to assess risk
Enforce policies and automate to create norm
PREVENT
VENAFI
DETECT
RESPOND
Monitor and detect anomalies from norm
Replace based on inventory & ownership
Gain intelligence and optimize policies

Integrated Security Solution

IBM integrated security intelligence protects businesses around the world.

IBM offers a deep enterprise security portfolio customized to your company’s needs. Unmatched in ability to help you disrupt new threats, deploy security innovations and reduce the cost and complexity of IT security, IBM can safeguard your most critical data from compromise.

From infrastructure, data and application protection to cloud and managed security services, IBM has the expertise to help safeguard your company’s critical assets. We protect some of the most sophisticated networks in the world, and employ some of the best minds in the business.

Identify - Build a secure enterprise with increased visibility

Risk Management and Compliance Services help you evaluate your existing security practices—including payment card industry (PCI) security, identity and IT regulatory compliance needs and gaps— against your business requirements and objectives. Our skilled security specialists provide recommendations to help you make more informed decisions about allocating your resources to better manage security risks and compliance. We can deliver a wide range of capabilities—from security program development, to regulatory and standards compliance, to security education and training.

Protect - Arm yourself to prevent attacks before they start

IBM identity and access management services target virtually every aspect of identity and access management across your enterprise, including user provisioning, web access management, enterprise single sign-on, multi-factor authentication, and user activity compliance. We offer a range of service options — from migration to consulting to fully managed services — that leverage IBM’s leading security tools, technologies, and expertise. Our security specialists work with you to address your individual needs and provide the solutions that best match your business and security objectives.

Respond - Stop attacks in their tracks and mitigate exposure

IBM’s Cybersecurity Assessment and Response services are designed to help you prepare for and more rapidly respond to an ever-growing variety of security threats. Our seasoned consultants deliver cybersecurity assessments, planning and response services, with proven expertise from mainframe to mobile.

Network Security and Control

ForeScout

forescout.com

For Global 2000 enterprises and government organizations, ForeScout offers the unique ability to see devices the instant they connect to the network, control them and orchestrate information sharing among disparate security tools. Today, more than 2,000 customers rely on ForeScout.

Don't just connect the dots. Control them.

New devices join your network every hour. Unmanaged notebooks, smartphones and tablets. Internet of Things (IoT) devices of all shapes and sizes. Rogue endpoints. Servers. These devices significantly expand your attack surface yet are invisible to many security products.

ForeScout can see them, control them and orchestrate system-wide response.

Transforming Security Through Visibility

The unique capabilities of ForeScout can be summarized in three words:

See - The ForeScout CounterACT™ platform provides real-time visibility into IP-connected devices—managed and unmanaged, corporate and personal, wired and wireless. Because CounterACT™ doesn't require endpoint agents, it also discovers non-traditional IoT devices and personally owned BYOD devices. CounterACT™ identifies endpoints and applications; user, owner and operating system; configuration, software, patch state and the presence of security agents.

Control - CounterACT™ continuously scans the network and monitors the activity of every device. Unlike systems that simply flag violations and send an alert, CounterACT™ automates and enforces a comprehensive range of policy-based controls for network access, endpoint compliance and mobile device security.

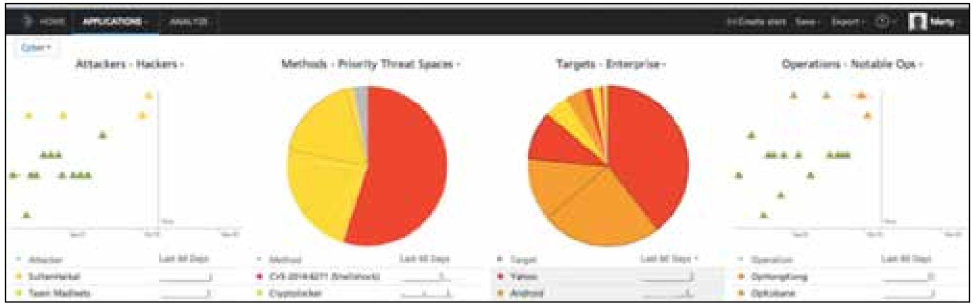
Orchestrate - CounterACT™ integrates with more than 70 network and security. This ability to orchestrate information sharing and operation among security tools you already own allows you to:

- Share context and control intelligence across systems to enforce unified network security policy
- Reduce vulnerability windows by automating system-wide threat response
- Gain higher return on investment (ROI) from your existing security tools while saving time through workflow automation

Real-time Threat Intelligence

Recorded Future recordedfuture.com

Recorded Future arms you with real-time threat intelligence so you can proactively defend your organization against cyber-attacks. With billions of indexed facts, and more added every day, our patented Web Intelligence Engine continuously analyzes the open Web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world.



Overview of your threat environment tailored to your organization and industry.

Why Recorded Future

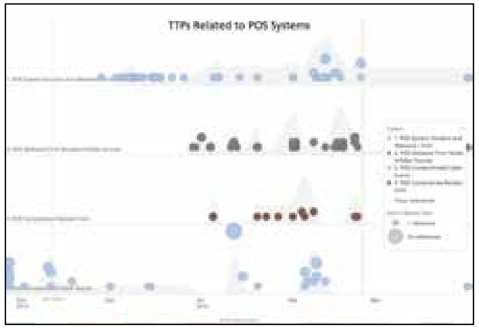
Faster Analysis:
Spend less time collecting data and supercharge your analytic capacity.

Cut the Middleman:
Direct access to billions of data points from the open, deep and dark Web for superior context.

Real-Time Monitoring:
Alerts to direct threats. Share live reports. Enrich your SIEM.

Relevant Intel:
Tailored to your environment, technology infrastructure, and corporate profile.

"Recorded Future gives us incredible context and insight into potential threats."
Dave Ockwell-Jenner, Sr. Manager, Security Threat & Operational Risk Mgmt., SITA



A timeline view enables analysts to visualize emerging trends for proactive security.

Dynamic & Static Application Vulnerability Testing

VERACODE veracode.com

Veracode helps the world's largest enterprises reduce global application-layer risk across web, mobile and third-party applications. Web applications are the #1 attack vector for data breaches, yet only 10% of enterprises test all their critical applications for resilience against cyber-attacks. Why? Because traditional application security slows down innovation.

Veracode offers a simpler and more scalable approach for reducing application-layer risk across your entire global software infrastructure — including web, mobile and third-party applications.

- It's End-to-End: Veracode's single central platform covers web, mobile and legacy applications, from the SDLC to IT operations to the software supply chain and open source.
- It's Built for Scale: Veracode's cloud-based service was purpose-built for the speed and scale required to secure applications enterprise-wide.
- It's Systematic: Veracode program managers help you reduce enterprise security risk by implementing structured governance programs, backed by world-class experts in application security.

Veracode's holistic approach combines our powerful cloud-based platform with multiple analysis technologies to identify application-layer threats, including:

- Binary Static Analysis (SAST): Veracode's patented binary Static Application Security Testing (SAST) technology analyzes all code — including third- party without requiring access to source code.
- Software Composition Analysis: Software composition analysis enables developers to continuously audit their third-party code to identify known vulnerabilities such as Heartbleed and Struts2 vulnerabilities.
- Integration with Agile and DevOps Toolchains: Veracode provides a rich set of APIs and plugins to integrate with development environments by embedding security into build and test processes, including Agile and continuous deployment toolchains.
- Dynamic Analysis (DAST): Dynamic Application Security Testing (DAST) or "black-box" testing, identifies architectural weaknesses and vulnerabilities in your web applications using techniques such as deliberately supplying malicious input to web forms.
- Web Perimeter Monitoring: Veracode's cloud infrastructure discovers obscure or out-of-date websites — to gain access to critical corporate and customer data including unknown sites outside the normal corporate IP range using a combination of advanced search and machine learning.
- WAF Integration: Veracode integrates with leading WAFs to enable rapid "virtual patching" of critical vulnerabilities in production applications.
- Third-Party Security: Veracode's vendor application security testing program reduces the risk associated with third-party software by managing the entire vendor compliance program on your behalf.
- Mobile Application Security: Veracode's Mobile App Reputation Service provides behavioral intelligence by integrating with leading mobile device management (MDM) solutions to help implement secure BYOD program.
- Cloud-Based Platform: Veracode's cloud-based platform provides centralized policies and information sharing across global teams.

Vulnerability Management & Security Benchmarking

tripwire.com

Tripwire is the leading provider of Information Risk & Security Performance Management solutions to more than 6,500 businesses and government agencies worldwide. Tripwire solutions enable enterprises of all sizes to 1) automate compliance and reduce risk, and 2) measure and compare the performance of their IT security program with their own goals and industry peers.

Tripwire delivers an integrated and open solution connecting Tripwire and third-party security products to leverage all available information to protect IT assets and high value data. Tripwire offers the industry's first security performance management application for CISOs - that gives CISOs a metrics language to communicate their company's security performance just like the CFO describes financial performance. From Vulnerability Management to agentless compliance policy auditing and file integrity monitoring,

Tripwire provides best-in-class products for reducing information risk and aligning security strategies with business initiatives. Tripwire delivers solutions for your business' security and compliance needs – regardless of size or industry.

How Tripwire secures your organization:

- Configuration Policy Auditing shows compliance against internal or international policies/ baselines and alerts on deviations
- Vulnerability Management prioritizes remediation of vulnerabilities across the entire technology stack
- File Integrity Monitoring warns on unauthorized changes
- Web Application Scanning finds flaws across your websites
- Security Performance Management consolidates and compares security metrics from your security solutions

Tripwire is headquartered in San Francisco, CA, with regional offices throughout the United States, London and Toronto.

Vulnerability Aggregation, Penetration Testing & Validation

coresecurity.com

Core Security is the leading provider of predictive security intelligence solutions for enterprises and government organizations. Built on the success of CORE Impact, the world's leading penetration testing tool, we help more than 1,400 customers worldwide proactively identify critical risks and match them to unique business objectives, operational processes and regulatory mandates. Core Security partners with a variety of complementary technology vendors to provide prebuilt integration and interoperability. Our patented, proven, award-winning enterprise solutions are backed by more than 15 years of applied expertise from CoreLabs, the company's innovative security research center.

Core Security : The Power of Thinking Ahead

As the leading provider of predictive security intelligence solutions, Core Security answers the call of organizations demanding a proactive approach to eliminating business risk. Our solutions empower customers to think ahead, take control of their security infrastructure and predict and prevent IT security threats.

Organizations have to predict security threats – not just react to them

Today, the majority of security spending is focused on solutions that take defensive or reactive approaches to threats. As a result, security teams are saddled with overwhelming amounts of disparate security data, tools that don't communicate and alerts that sound only after the damage has been done. Organizations that seek to survive and thrive must go on the offensive and predict and preempt threats before it's too late.

Core Insight Enterprise

- Enterprise-class predictive security intelligence platform
- Business risk identification, validation and prioritization
- Continuous threat simulation
- Continuous, proactive threat simulation
- Dashboard view of an organization's security risk profile
- Attack path discovery and remediation modeling

Core Impact Professional

- Automated, on-demand penetration testing
- Vulnerability validation from all leading scanners
- Multi-threat surface investigation
- Regulatory compliance verification

NEXT-GENERATION PORTFOLIO OF 30 VENDORS, AND EVOLVING...

MOMENTUM

THE POWER BEHIND STARLINK

Cloud & Virtualization Security

TREND MICRO

trendmicro.ae

As a global leader in IT security, Trend Micro develops innovative security solutions that make the world safe for businesses and consumers to exchange digital information. With over 25 years of security expertise, we're recognized as the market leader in server security, cloud security, and small business content security.

Trend Micro security fits the needs of our customers and partners. Our solutions protect end users on any device, optimize security for the modern data center, and secure networks against breaches from targeted attacks. We deliver top-ranked client-server, network, and cloud-based protection that stops new threats faster, detects breaches better, and protects data in physical, virtual, and cloud environments.

Our security is powered by Trend Micro™ Smart Protection Network™ global threat intelligence and is supported by over 1,200 security experts around the world.

For more than 25 years, Trend Micro has innovated constantly to keep our customers ahead of an ever-evolving IT threat landscape. It's how we got to be the world's largest pure-play security software provider and the global cloud security leader.

It's how we continue to set the pace for the IT security industry: by delivering simple, integrated solutions that elegantly solve your most pressing challenges.

Today, those challenges stem primarily from three trends that are sweeping the business landscape and reshaping IT infrastructures everywhere:

Consumerization: The explosion of endpoints is boosting productivity—but with users controlling multiple devices and using unsecured consumer applications such as DropBox™ at work, it's also forcing IT managers to re-think traditional perimeter defenses.

Cloud and Virtualization: The growing use of cloud-based and virtualized computing drives dramatic efficiency and operational gains—but if security strategies are not evolved to fit these environments, those benefits are not realized and security gaps are created.

Advanced Cyber Threats: Yesterday's viruses and malware are still lurking out there, requiring vigilant updating of traditional defenses—but the current explosion of advanced targeted attacks demands new, customized detection and response capabilities.

Trend Micro delivers smart, simple security that fits your infrastructure and defends your key assets as well as your bottom line, by letting you fully realize the business benefits of today's technology trends—while avoiding the costs of relying on security that can't keep up. For more information, please visit www.trendmicro.ae.

Deception-Based Threat Detection

Attivo NETWORKS®

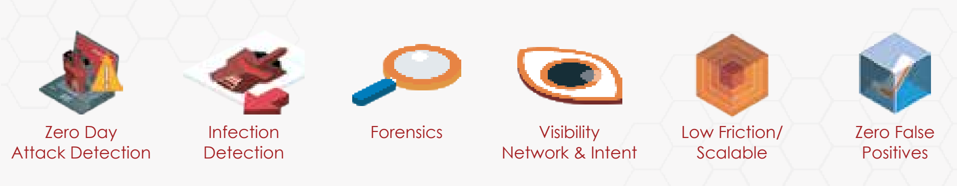
attivonetworks.com

Attivo Active Deception Solutions

The Attivo BOTsink Solution is ideal for detecting BOTs and APTs brought into your network via HTTPS, BYOD devices, spear phishing and the use of stolen credentials. With an Attivo BOTsink interleaved throughout your network, you will be able to:

- Reduces Attack Detection Time - providing accurate, actionable alerts that quickly and accurately identify infected clients, including sleeper and time-triggered agents, to enable remediation of the full extent of the attack before it can do any damage
- Non-disruptive Scalability - supports network, data center, and cloud environments including breach detection for east–west data center traffic
- Sends No False Positives - with a high-efficiency design, Attivo does not send false positives, reducing alert noise and the amount of time and energy required for management
- Capture Actionable Information - identifies the infected client, it prevents any ongoing communications outside the appliance to stop the attack's propagation
- Secure - No data or information ever leaves the user organization's premises for external (cloud) computation

Attivo Products: BOTsink® Engagement Servers, IRES End Point Deception, Attivo Central Manager



Next Generation Malware, APT & Threat Protection

FireEye
SECURITY REIMAGINED

fireeye.com

Like water, cybercrime moves effortlessly around obstacles. Since governments and enterprises have implemented stronger policy and signature-based protections for regulated data and endpoints, sophisticated criminal organizations have changed their tactics, using different tools and targeting intellectual property and other networked assets.

Replacing mass-market malware, this next generation of threats is personalized and persistent. Threats are targeted, ever morphing, dynamic and zero-day. These carefully staged attacks look innocent as they walk by traditional firewall, IPS, anti-virus and Web gateways that rely on signatures and known patterns of misbehaviour. Once inside, malware phones home for instructions, which could be to steal data, infect other endpoints, allow reconnaissance, or lie dormant until the attacker is ready to strike.

FireEye is the leading provider of next-generation threat protection focused on combating advanced malware, zero-day and targeted APT attacks. FireEye's solutions supplement security defenses such as next generation and traditional Firewalls, IPS, AV and Web gateways, which can't stop advanced malware. These technologies leave significant security holes in the majority of corporate networks.

FireEye's Malware Protection Systems feature both in-bound and out-bound protection and a signature-less analysis engine that utilizes the most sophisticated virtual execution engine in the world to stop advanced threats that attack over Web and email. Our customers include enterprises and mid-sized companies across every industry as well as Federal agencies. Based in Milpitas, California, FireEye is backed by premier financial partners.

Today, security-conscious enterprises and Federal governments choose FireEye™ for industry leading protection against these next-generation threats. FireEye combats advanced malware, zero day and targeted APT attacks. FireEye's appliances supplement traditional and next-generation firewalls, IPS, AV and web gateways, adding integrated inbound and outbound protection against today's stealthy Web and email threats.

"Some IPS/IDS/NGFW vendors are no better at handling evasions today than they were when they released their original products."

Advanced Evasion Techniques: Weapon of Mass Destruction or Absolute Dud?, Bob Walder, Gartner, 2011

"With FireEye, we can now see and stop the attacks targeting our in-house and remote users. It has been an eye-opener for us to be able to determine with accuracy the threats that are passing through the firewall, URL gateway, IPS and antivirus." Director of Information and Data Security, Global 500 Financial Services firm.

The Next-generation Cybersecurity Analytics

LINKSHADOW

linkshadow.com

LinkShadow is designed to manage threats in real-time with attacker behavioral analysis which is meant for organizations that are looking to enhance their defenses against advanced cyber-attacks, zero-day malware and ransomware, while simultaneously gaining rapid insight into the effectiveness of their existing security investments.

AttackScape Viewer

TrafficSense Visualizer

ThreatScore Quadrant

Identity Inteligence

Asset AutoDiscovery

BlockCount Ratio

Advanced Threat Prevention based on Artificial Intelligence

CYLANCE

cylance.com

Cylance® Consulting has one goal in mind – securing our clients as quickly as possible and maintaining a higher level of security via prevention using AI technology. Our team is comprised of industry-leading experts in the most advanced technologies. No one in the industry can bring more depth of services and expertise than Cylance PERIOD.

SMARTER SECURITY FASTER SERVICES

Industrial Control Systems

Internet of Things / Embedded Systems

Red Team Services

ThreatZERO™

Incident Response & Compromise Assessments

Training

MOMENTUM

THE POWER BEHIND STARLINK

Secure Managed File Transfer & Large-File Email Bypass

ipswitch

ipswitch.com

MOVEit Managed File Transfer: Today's businesses share more information electronically than ever before between their business partners, customers, and employees. Ipswitch's MOVEit Managed File Transfer (MFT) System is the best way to reliably move that information in a timely, controlled, and secure manner to improve business productivity, meet SLAs and compliance requirements, and gain visibility and control of file movement.

MOVEit File Transfer: MOVEit File Transfer server is the reliable and secure hub that IT needs to transfer the organization's business files. With its broad protocol support, MOVEit File Transfer server connects with any system, server or client. Using the latest security technologies, it protects files both in transit and at rest. And as part of the MOVEit Managed File Transfer System, MOVEit File Transfer gives IT the visibility and control they need to confidently meet SLAs and compliance requirements.

MOVEit Central: MOVEit Central enables you to easily automate your file-based workflows. MOVEit Central provides a simple but powerful user interface for defining business workflows that's easy enough for anyone on your IT team to use because no scripting is required. The heart of MOVEit Central is a reliable workflow engine that ensures the predictable, secure delivery of your business files. Plus, a powerful centralized console ensures you'll have visibility and control over all file movements. That is why hundreds of companies, including many in healthcare and finance have turned to MOVEit Central to automate their file-based workflows and confidently meet their SLAs and compliance requirements.

MOVEit Mobile: IT departments want to give users the ability to transfer work files using their mobile devices while keeping the enterprise security they rely on with MOVEit. They want to allow users to upload and download files from either iOS or Android phones and tablets. Most importantly, they want to extend the secure, compliant, file-based processes to people when they are mobile. MOVEit Mobile enables mobile workers to reliably and productively participate in file-based business process workflows, while providing IT the security, visibility and control required to confidently run their business and meet compliance requirements.

MOVEit Ad Hoc: To get their work done employees are circumventing IT by turning to new, web-based consumer services to send and receive files, creating control, visibility, and security challenges for the business. MOVEit Ad Hoc Transfer offers employees and businesses a better alternative.

For employees, MOVEit Ad Hoc Transfer enables easy transfer of files of any size using a familiar interface: either Microsoft Outlook or a web browser. For IT, MOVEit Ad Hoc Transfer provides the comfort of knowing sensitive business files are being sent and received through a secure, enterprise-class Managed File Transfer system. Plus, the system relieves your email and storage systems from the burden of transferring and storing large files.

High Precision Location-Based Mobile Security

AIRPATROL™ by SYSOREX

airpatrolcorp.com

AirPatrol develops platforms and tools to deliver software and services to mobile devices based on their location and user context. Leading enterprises and agencies depend upon AirPatrol to help them solve their most pressing wireless security and situational awareness issues.

The mobile computing and Bring Your Own Device (BYOD) revolution has made location and context more important than ever. A smartphone is not simply a phone; a tablet is not simply a web-browser - they are also business computers, cameras, navigation devices, game consoles, social tools and more. And what they are largely depends on where they are and who is using them.

AirPatrol Corporation is dedicated to developing innovative technologies that help enhance and secure these devices by delivering features and functionality that can change based on where they are and who is operating them. The current product line-up includes a suite of location-based mobile and wireless enterprise security solutions that offer detection, precision locationing (within zones as small as 10 feet) and management for devices on WiFi, 2G, 3G and 4G LTE cellular networks.

AirPatrol:

- Combines wireless infrastructure tools with endpoint software to enable enterprise-class end-to-end network risk management capabilities.
- Supports IT best practices and compliance with industry regulations.
- Enforces wireless policies and react to threats in real-time.
- Supports the lowest total cost of ownership in the industry, with solutions that are simple to configure and easy to maintain.
- Designs non-proprietary and scalable systems for the future, combining the network planning and management tools necessary to ensure optimal performance.

Encrypted & Secured USB Drives

kingston.com

Kingston Technology acquired IronKey in March 2016. As a leader in the USB Flash drive market since 2004, Kingston utilises the IronKey product line to deliver FIPS 140-2 Level 3 certification solutions for customers who need the highest level of encryption and security.

Kingston's DataTraveler product line includes their flagship drive DataTraveler Vault Privacy (DTVP) which is also available in managed and anti-virus versions as well as the DataTraveler 2000 (DT2000), an OS independent keypad encrypted USB drive. Both drives are FIPS 197 certified.

With their DataTraveler and IronKey product lines Kingston delivers secure USB storage solutions for the mission-critical mobile workforce and the invaluable data they carry.

- SECURE DATA: High-performance encrypted USB flash drives with stronger security and comprehensive device management (see below) to help secure organizations' sensitive and mission-critical data.
- MANAGED SOLUTIONS: With its EMS software, Kingston's partner, DataLocker offers a software management solution for Ironkey Enterprise drives that allows to establish and secure a centralized workspace or storage command center where you can deploy and manage devices easily. The DTVP is also available in a managed version and the management software SafeConsole is provided by DataLocker.
- SOLUTIONS FOR THE MOBILE WORKFORCE: IronKey's Workspace Encrypted USB drive; W700 with 'Windows To Go' is a PCs on a stick that equips employees and contractors with a portable Windows 10 or Windows 8/8.1 corporate image.

These solutions enable you to be confident that your organization has the right solutions in place to safeguard data for your road warriors, teleworkers and contractors.

Secure Information Sharing: Encryption & Rights Management

accellion.com

Accellion, Inc. is the industry leader in providing private cloud solutions for secure access and sharing of enterprise information across devices, enabling employees to work securely wherever. kiteworks™ by Accellion is a secure file sharing platform that facilitates access to enterprise content sources by allowing internal and external users to share, send, sync and edit files on any type of device from any content store.

Secure File Sharing

kiteworks™ enables internal and external sharing of enterprise content, and a platform for designing and deploying custom applications and workflows to increase productivity around content collaboration.

Key Capabilities:

- Private Cloud Architecture
- Content Collaboration and Productivity
- Secure Connectors to Enterprise Content
- Security and Governance
- Microsoft Office 365 Integration
- Mobile Enablement
- REST APIs and SDKs

Private Cloud Architecture

The kiteworks™ platform was designed from the ground up for enterprise scalability, security, and agility.

Private Cloud – The kiteworks™ architecture offers dedicated and isolated cloud infrastructure enabling enterprises to keep servers, storage, application services, meta-data, and authentication all within the organization's complete control. Deployment options include on-premises, hosted private cloud, and hybrid cloud.

Multi-Tier Architecture - kiteworks™ enables extreme deployment flexibility by allowing the web, application, and storage tiers to be separated and placed anywhere in the network. Each tier can be scaled independently or all can be combined into a single virtual appliance.

Data Sovereignty and Global Deployments – kiteworks™ enables enterprise organizations to enforce data residency policies by restraining data storage to physical geographical boundaries to meet security and compliance requirements.

Content Collaboration and Team Productivity

The kiteworks™ solution helps enhance employee productivity by enabling users to easily collaborate with internal and external stakeholders and share content securely.

Secure Mobile Device Management

MobileIron

mobileiron.com

MobileIron solutions provide end-to-end security and management for apps, docs, and devices. Thousands of customers worldwide trust MobileIron solutions as the foundation of their mobile strategy. Utilizing MobileIron, IT can now establish a virtual perimeter to secure mobile delivery of business data and applications while preserving an excellent user experience, even on employee-owned smartphones and tablets.

MobileIron offers a number of product bundles to enable you to effectively meet your Mobile IT requirements. Whether you currently want to start your mobile journey by securing devices in a BYOD initiative or whether you require a comprehensive mobile IT infrastructure capable of transforming your business into a Mobile First enterprise, MobileIron has the product to meet your requirements.

MobileIron is available as both an on-premise system and as a cloud service through the MobileIron Connected Cloud.

MobileIron Advanced Mobile Managment

MobileIron Advanced Mobile Management is the foundation for your Mobile IT infrastructure. Comprised of MobileIron Atlas and Sentry, it contains all required functionality to 1) Manage mobile devices in a secure and scalable environment and 2) Deploy an enterprise mobile app storefront. All MobileIron solutions for Mobile Apps, Content, and Web Access build upon the Advanced Mobile Management Product.

MobileIron Docs Bundle

The Docs Bundle includes both MobileIron Advanced Mobile Management and Docs@Work. It builds upon the proven MobileIron MDM foundation to enable secure mobile access to corporate web content including Enterprise email attachments and documents stored in SharePoint environments. The Docs Bundle is an ideal solution for those organizations that want to empower their employees with secure mobile access to enterprise content.

MobileIron Apps Bundle

The Apps Bundle includes Apps@Work and Advanced Mobile Management. It provides a complete solution for enterprise mobile apps, securing both the app data on the device through AppConnect functionality, and data in motion, by leveraging AppTunnel. For those organizations that are fully embracing native mobile apps, the Apps Bundle is the choice.

LogRhythm

logrhythm.com

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's patented award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint monitoring, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides unparalleled compliance automation and assurance, and enhanced IT intelligence.

LogRhythm is consistently recognized as a market leader. The company has been positioned as a Leader in Gartner's SIEM Magic Quadrant report for five consecutive years, named a 'Champion' in Info-Tech Research Group's 2014-15 SIEM Vendor Landscape report, received SC Labs 'Recommended' 5-Star rating for SIEM and UTM for 2016 and earned Frost & Sullivan's 2015 Global Security Information and Event Management (SIEM) Enabling Technology Leadership Award.

LogRhythm's security intelligence and analytics platform enables organizations to detect, prioritize and neutralize cyber threats that penetrate the perimeter or originate from within.

Detect, prioritize and neutralize cyber threats that penetrate the perimeter or originate from within with;

- Next-Gen SIEM - Unified platform for advanced detection & response
- Security Analytics - Holistic threat analytics & compliance automation
- Log Management - Centralized visibility into all log and machine data, at any scale
- Network Forensics - Real-time deep packet analytics and full capture
- Endpoint Monitoring - Real-time user, file application and system behavior monitoring

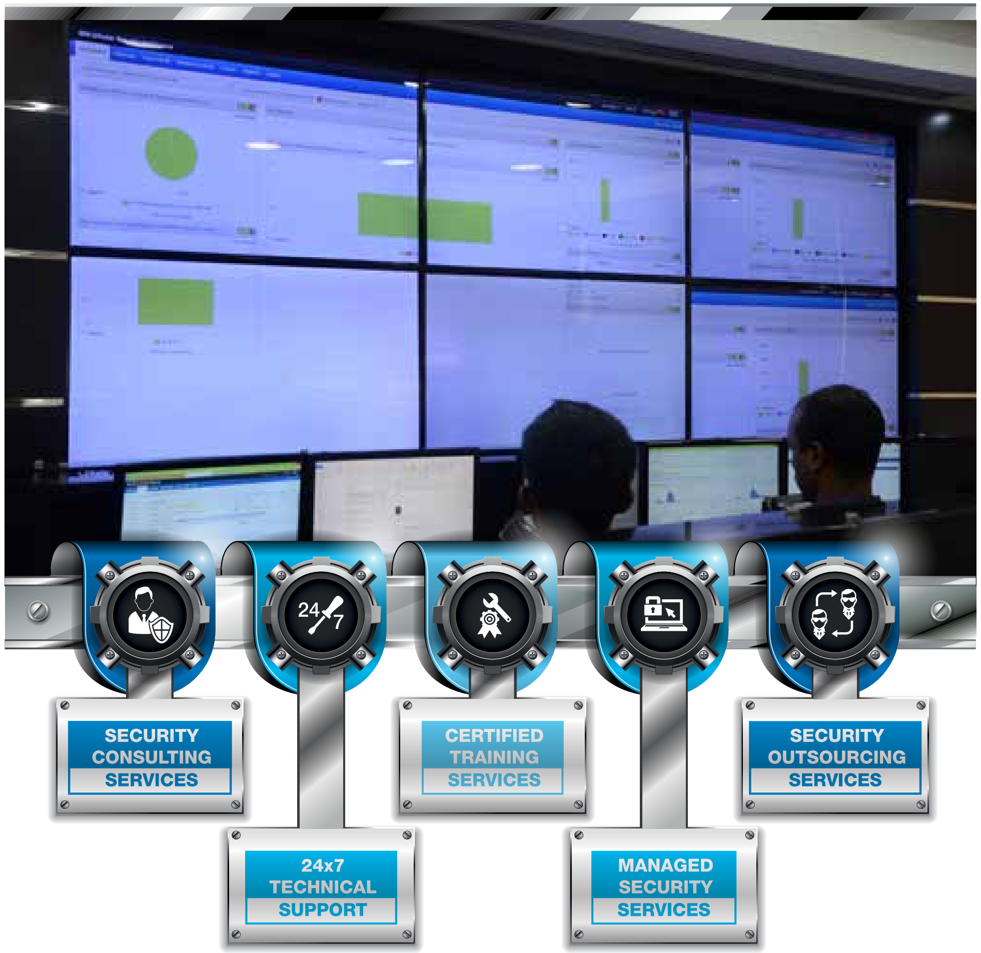
Customer Success Services

Customers implementing IT Security technologies depend on expert technical services and support professionals that understand the challenges being addressed and the business impact, and then provide action in a timely manner to achieve successful deployments.

StarLink Customer Success Services comprises of a highly skilled team of IT Security Consultants offering remote and onsite advanced technical services to customers via Channel Partners.

In order to ensure continued customer success, SCS also offers a centralized approach to provide simplified and preventive IT sustenance post project closure.

The SCS portfolio includes Security Consulting Services, 24x7 Technical Support, Certified Training Services, Managed Security Services, Security Outsourcing Engineering.


SECURITY CONSULTING SERVICES
24x7 TECHNICAL SUPPORT
CERTIFIED TRAINING SERVICES
MANAGED SECURITY SERVICES
SECURITY OUTSOURCING SERVICES

Toll Free 800 STARLINK *
78 27 54 65

* Reach StarLink Consulting Services via:
800-7827 5465 in the UAE | 800-247-0247 in KSA | +971 4279 4000 for all other countries

TRUSTED SECURITY ADVISOR TO 1000 CUSTOMERS, AND ADDING...

MOMENTUM

THE POWER BEHIND STARLINK

1000+ Customers in the META

StarLink's strong base of customers includes leading financial institutions, the largest telecommunications and energy companies, as well as, high-profile government organizations. StarLink helps these organizations achieve and sustain compliance and optimally manage risks through full policy, procedure and controls lifecycle management. StarLink's solution offerings are now installed in more than 1000 data centers in the region, including 50 of the top regional banks, 15 of the region's top Telcos, 100 of region's top energy companies and 200 government entities. Our customers trust StarLink to secure their critical enterprise data and safeguard access to sensitive data in the most demanding datacenter environments by monitoring, securing and auditing privileged user access to provide 100% visibility on all activities.

Customer Testimonials:

Saudi Hollandi Bank Implements e-DMZ Security to Manage Privileged Users' Password and Monitor Remote Access Activities

"We chose the Password Auto Repository (PAR) and eGuardPost (eGP) from e-DMZ Security because it was uniquely designed to solve enterprise security and compliance issues associated with the management and control of shared privileged passwords such as root and administrator. The issue of Privileged Password Management and the unique features of PAR contribute directly to many specific PCI requirements," said Ali Alotaibi, IT Security Manager, Saudi Hollandi Bank.

National Bank of Kuwait Implements Guardium to Prevent Unauthorized Database Changes by "Super Users"

"We chose Guardium because they have become the 'gold standard' for database security and monitoring," said Tamer Gamali, Chief Information Security Officer (CISO), National Bank of Kuwait. "We needed tighter internal controls over our critical Oracle and Microsoft SQL Server-based Financial Systems. We considered solutions based on native database auditing, but Guardium gives us automated, real-time security alerts along with full visibility into all transactions without impacting database performance. It also provides a scalable, cross-DBMS audit architecture for handling the massive amounts of transactions in our large-scale heterogeneous data centers."

Abu Dhabi Commercial Bank Implements Guardium to Strengthen Database Controls

"We were seeking a unified, cross-DBMS solution that delivers granular, real-time controls without the complexity, overhead and risk of native DBMS-resident auditing, and Guardium fulfilled all our requirements. Our goal is to ensure that critical information is stored securely through the adoption of best-of-breed technologies." said Steve Dulvin, Head of IT Security at Abu Dhabi Commercial Bank.

Our Prestigious Customers

بنك مسقط BankMuscat

NBB

etisalat

تداول Tadawul

البنك السعودي الهولندي Saudi Hollandi Bank

BBK بنك البحرين والكويت

بنك دبي التجاري Commercial Bank of Dubai

الإسلامي AL ISLAMI بنك دبي الإسلامي Dubai Islamic Bank

أرامكو السعودية Saudi Aramco

بنك الرياض riyad bank

du

بنك أبوظبي الوطني NBAD

DUBAI BANK

QNB

كيوتل Qtel

NCB الأهلي

NOOR BANK

البنك السعودي الفرنسي Banque Saudi Fransi

BARCLAYS

الوطني NBK

mashreq المشرق WE MAKE POSSIBLE

Emirates

بنك الإمارات دبي الوطني Emirates NBD

الاتحاد ETIHAD AIRWAYS

موبايلي mobily

بيت التمويل الكويتي Kuwait Finance House

بنك الاتحاد الوطني UNION NATIONAL BANK the bank that cares

المؤسسة العربية المصرفية ARAB BANKING CORPORATION

ADIB مصرف أبوظبي الإسلامي

RAKBANK Simply Better

SABB ساب

zain

CBI

بنك الخليج الأول FGB

samba سامبا

بنك أبوظبي التجاري ADCB

umniah belong

عمانتل Omantel معاً Together

Bank Sohar S.A.O.G. Excel

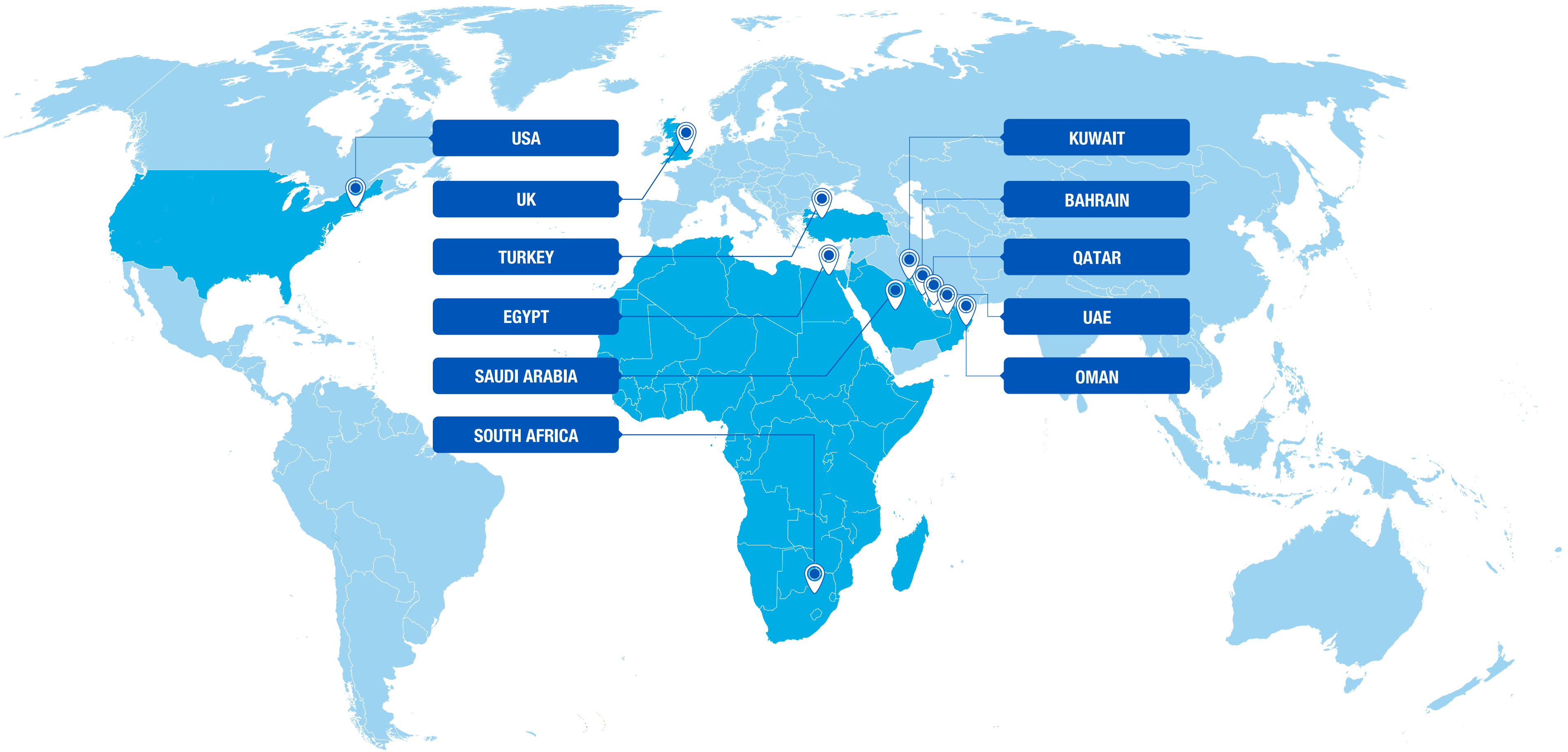
QIB المصرف الالتزام بالريادة Committed to leadership

البنك التجاري Commercial bank

مصرف الهلال al hilal bank

بنك الإسكان للتجارة والتمويل The Housing Bank for Trade & Finance

Global Footprint



Contact Us

Headquarters

Dubai, UAE

Office 4301 Mazaya Business Avenue – BB2,
JLT, P.O. Box 99580, Dubai, UAE
T: +971 4 279 4000 | F: +971 4 279 4001 | info@starlinkme.net

Regional Offices

Massachusetts, USA

14th Floor, One Broadway,
Cambridge, MA 02142, USA
T: +1 877 823 1566
usa@starlinkme.net

London, UK

17 Hanover Square, Mayfair,
London W1S 1BN, UK
T: +44 (0) 203 870 1265
F: +44 (0) 203 102 6301
uk@starlinkme.net

Kuwait City, Kuwait

Office No. 12, 7th Floor, Building No. 14,
Block 1, Abdullah Al Mubarak Street,
P.O.Box 1894, Safat 13019, Kuwait
T: +965 22465571 / 2
F: +965 22465573
kuwait@starlinkme.net

Istanbul, Turkey

Fatih Sultan Mehmet Mah. Poligon Cad. No: 8C,
Buyaka2 Sitesi Kule-3 Daire No: 11834771
Ümraniye, İstanbul, Turkey
T: +90 216 510 6909
F: +90 216 510 6908
turkey@starlinkme.net

Riyadh, KSA

Tulip Tower, 3rd Floor, Office 1,
King Fahad Road,
P.O. Box 295833, Riyadh, KSA
T: +966 1 2177522, 2191952-3
F: +966 1 2191926
ksa@starlinkme.net

Bryanston, South Africa

20 Georgian Crescent, Hampton Office Park,
Charlton House, Ground Floor
Bryanston, South Africa, Code 2191
T: +27 10 020 3610
sa@starlinkme.net

Cairo, Egypt

Villa 55, District No. 3, Area No. 5, Fifth Settlement,
New Cairo, Egypt
T: +20 25627172
egypt@starlinkme.net

Doha, Qatar

1st Floor, Al-Jaidah Square Building
Airport Road, P.O. Box 55743, Doha, Qatar
T: +971 4 2794000
F: +971 4 2794001
M: +974 5595 6678
qatar@starlinkme.net

Manama, Bahrain

T: +966 1 2177522, 2191952-3
bahrain@starlinkme.net

Muscat, Oman

F: +971 4 2794001
M: +974 5595 6678
oman@starlinkme.net

USA | UK | UAE | KSA | KUWAIT | BAHRAIN | QATAR | OMAN | EGYPT | TURKEY | SOUTH AFRICA

info@starlinkme.net | www.starlinkme.net