STARLINK

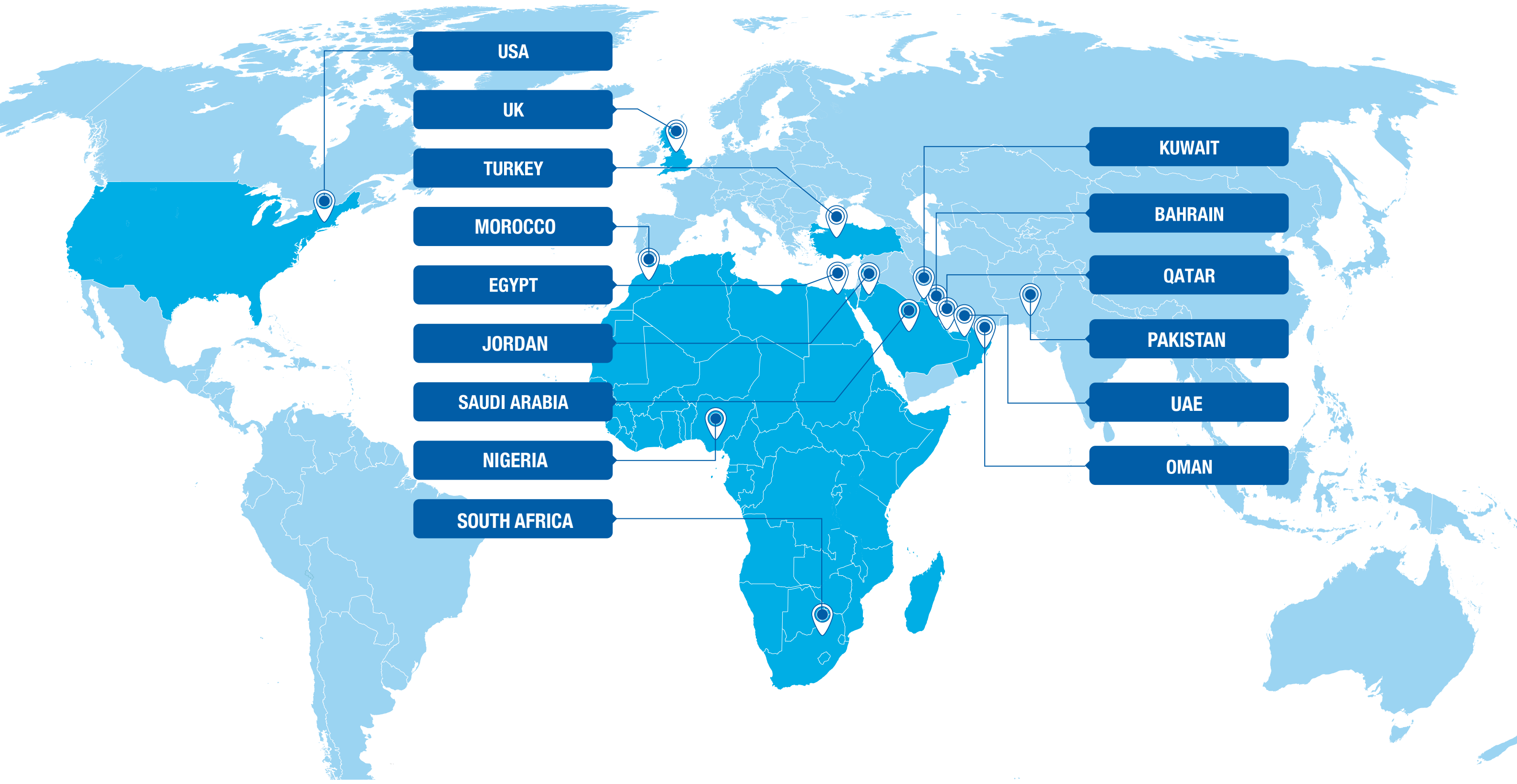
TRUSTED SECURITY ADVISOR

TRUE VALUE-ADDED IT DISTRIBUTOR

ACCELERATE

AT THE SPEED OF STARLINK

About Us

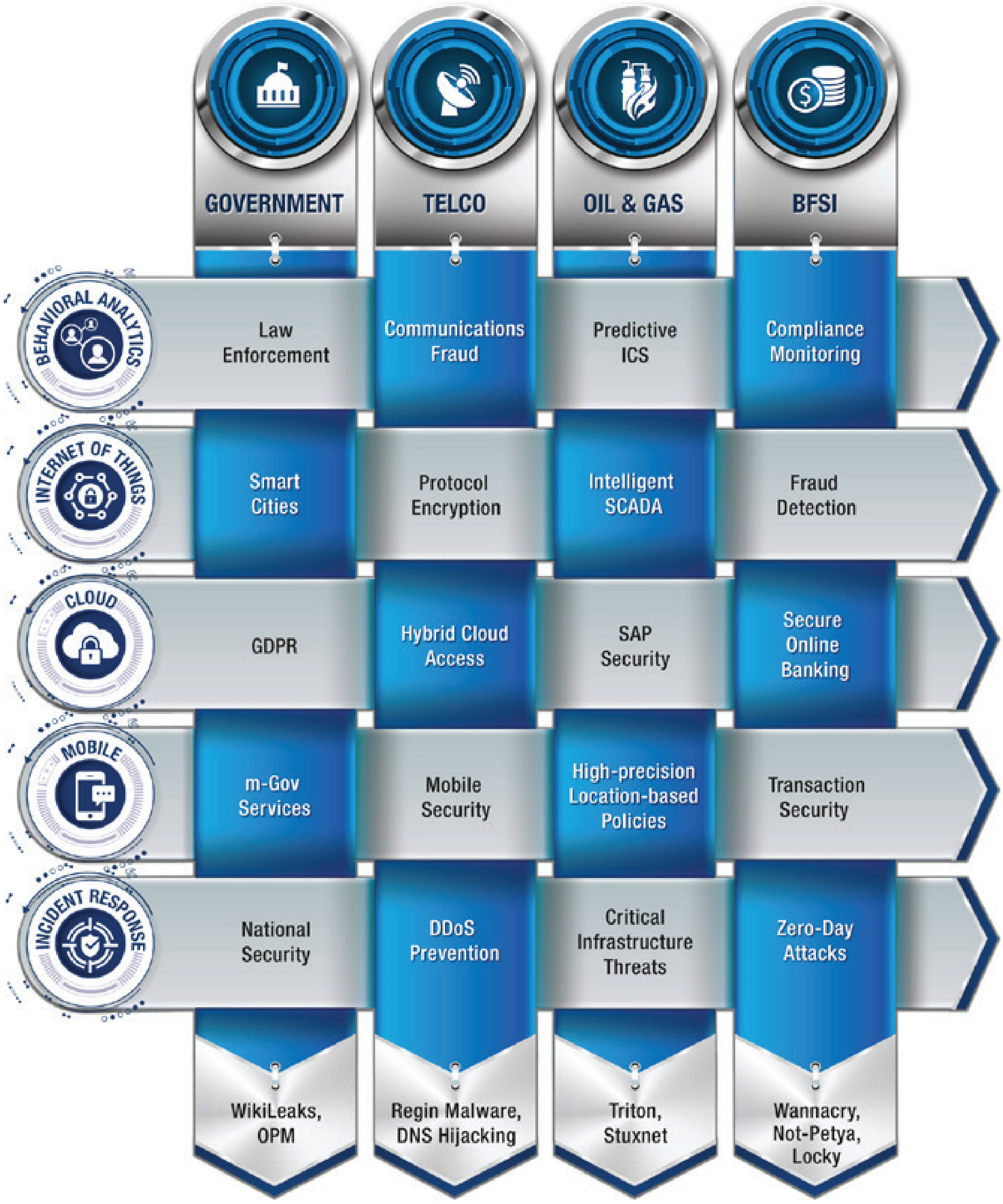


Who We Are

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 15 countries.

With its innovative Security Framework and Vertical Security Trend Matrix StarLink is also recognized as a "Trusted Security Advisor" to over 2200 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 1000 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.



	GOVERNMENT	TELCO	OIL & GAS	BFSI
BEHAVIORAL ANALYTICS	Law Enforcement	Communications Fraud	Predictive ICS	Compliance Monitoring
INTERNET OF THINGS	Smart Cities	Protocol Encryption	Intelligent SCADA	Fraud Detection
CLOUD	GDPR	Hybrid Cloud Access	SAP Security	Secure Online Banking
MOBILE	m-Gov Services	Mobile Security	High-precision Location-based Policies	Transaction Security
INCIDENT RESPONSE	National Security	DDoS Prevention	Critical Infrastructure Threats	Zero-Day Attacks
	WikiLeaks, OPM	Regin Malware, DNS Hijacking	Triton, Stuxnet	Wannacry, Not-Petya, Locky

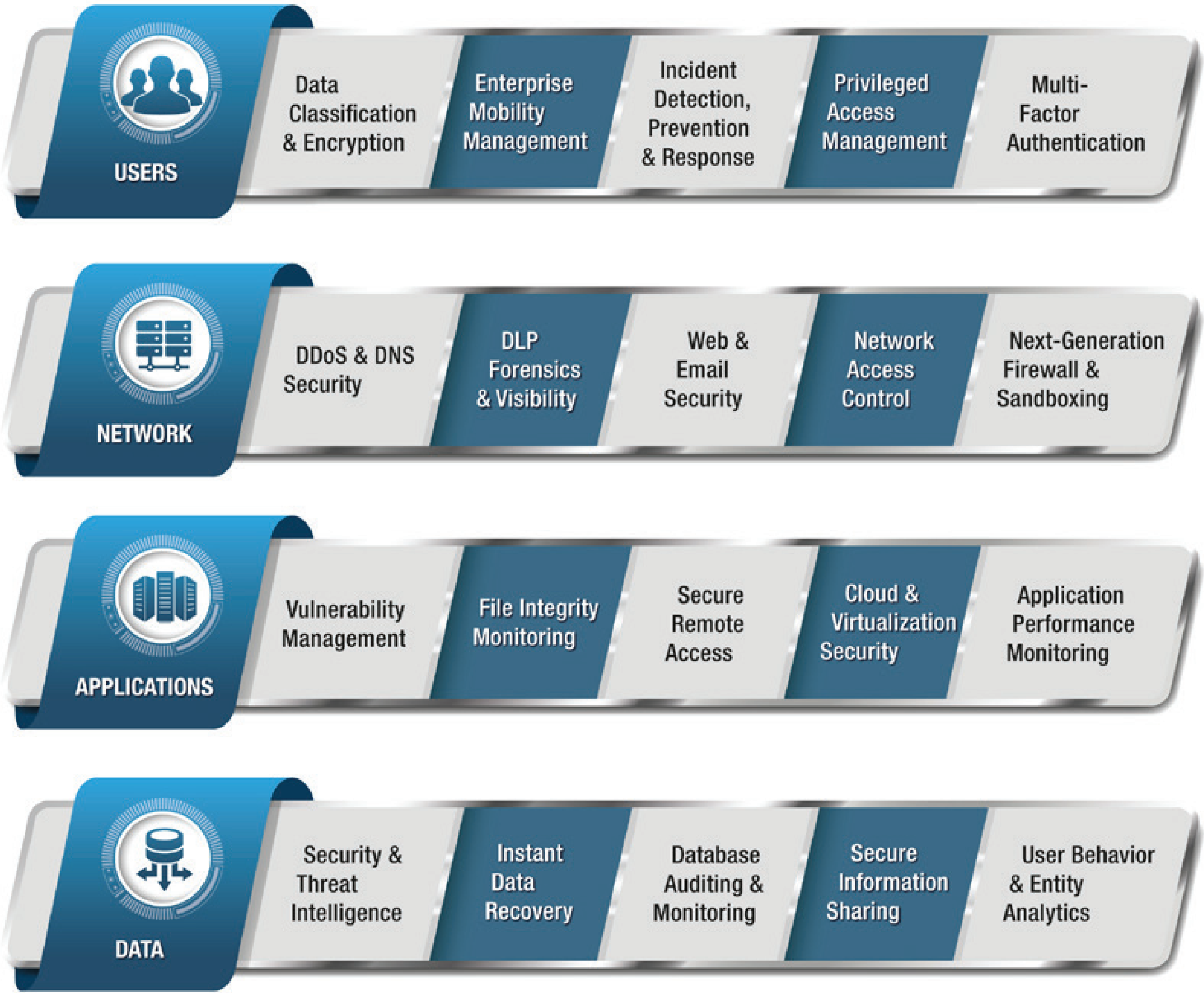
StarLink Vertical Security Trend Matrix

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 & Encryption	Enterprise Mobility Management	Incident Detection, Prevention & Response	Privileged Access Management	Multi-Factor Authentication
NETWORK	DDoS & DNS Security	DLP Forensics & Visibility	Web & Email Security	Network Access Control	Next-Generation Firewall & Sandboxing
APPLICATIONS	Vulnerability Management	File Integrity Monitoring	Secure Remote Access	Cloud & Virtualization Security	Application Performance Monitoring
DATA	Security & Threat Intelligence	Instant Data Recovery	Database Auditing & Monitoring	Secure Information Sharing	User Behavior & Entity Analytics

StarLink Security Framework

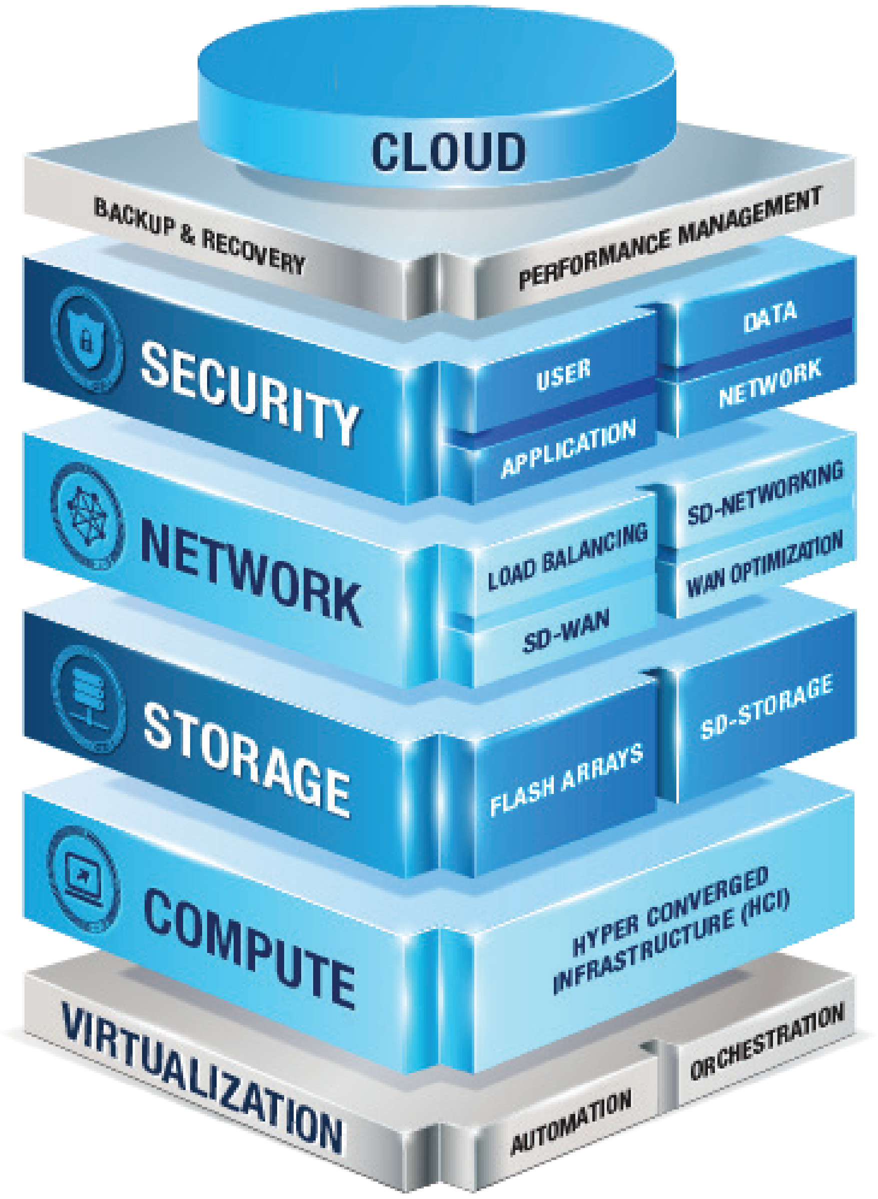
IT Security is a fragmented market, proliferated with many point products that are designed to address specific risks, and which may meet targeted compliance goals, but these solutions typically fail to provide a comprehensive, integrated picture of the threat landscape.

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.

Overview

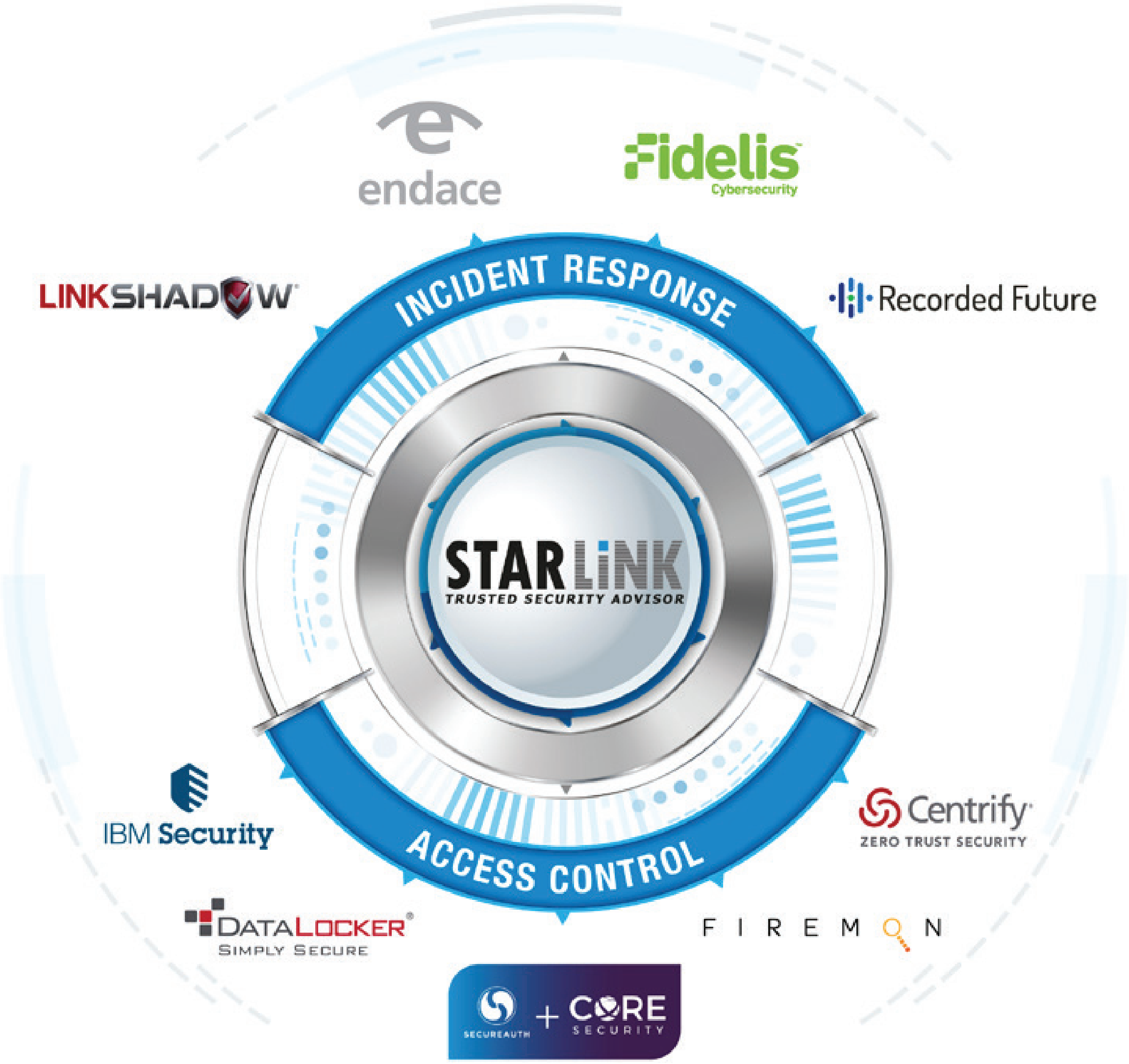


SDDC Technology Architecture

The software-defined data center (SDDC) is now a key focus area for most organizations. The shift in the datacenter paradigm is about reducing costs and providing service agility. To maximize data center ROI, key Security factors needs to be fundamentally considered including lateral movement of malware, network security virtualization, orchestration, people and process.

Simultaneously, with the surge in cyber threats including DDoS, against the cloud and IoT, as well as, ransomware leading to disruptions in IT and OT networks, plus mobile attacks and vulnerabilities on the rise, customers will be increasingly looking at automation and machine learning.

Solution

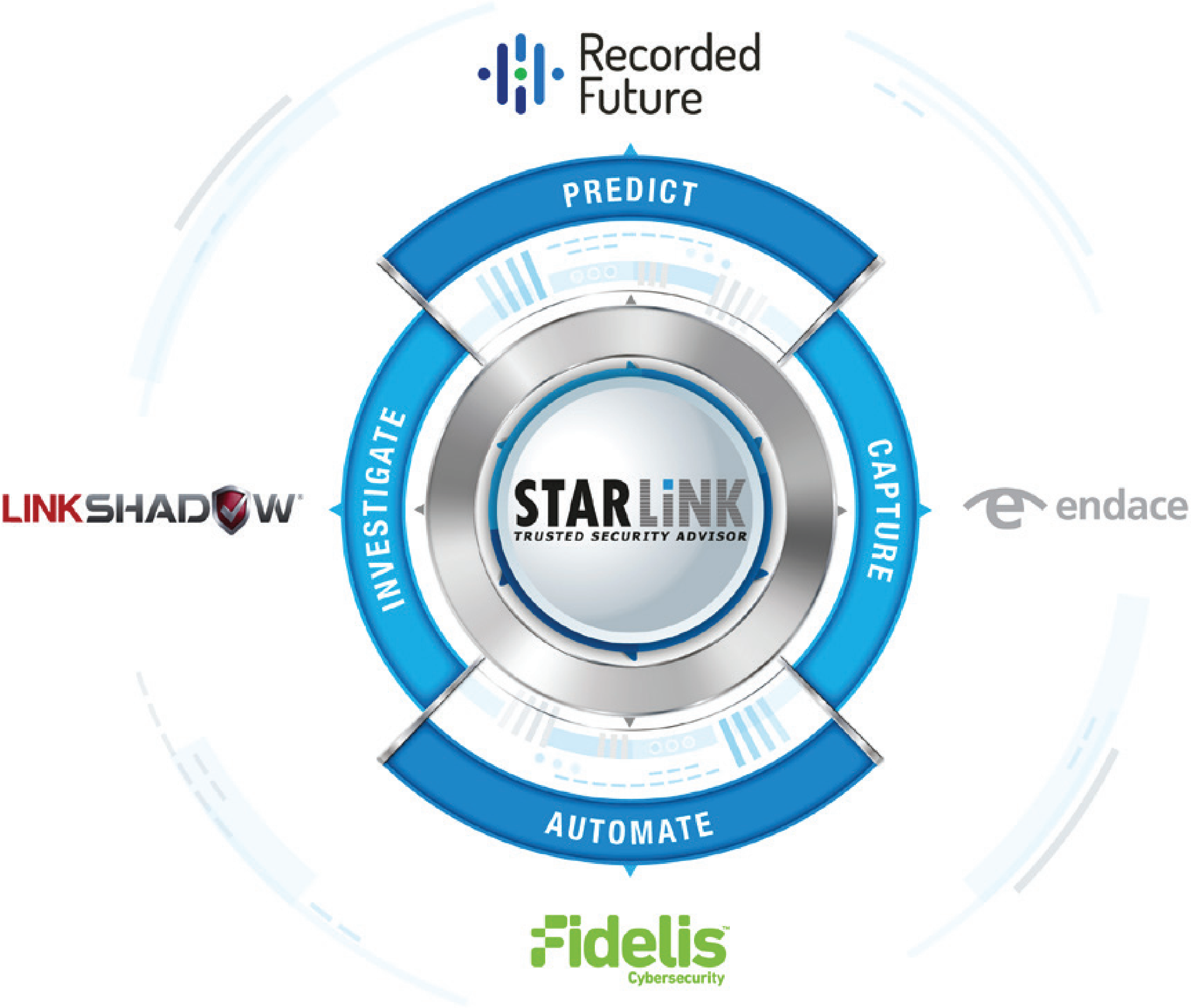


StarLink Solutions Lifecycle

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.

Solution



Incident Response

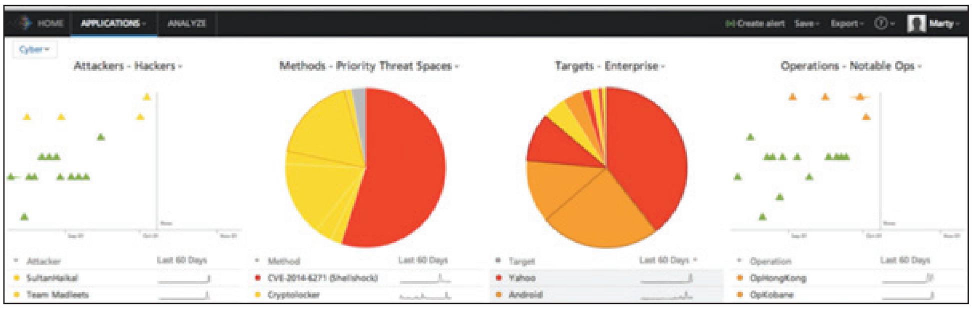
Has my sensitive data been breached?

Incident Response involves the monitoring and detection of security events, and the execution of proper remediation. Breaches can be mitigated with real-time, dynamic threat protection across the different stages of the kill chain. To be prepared to respond to modern malware in real-time and disrupt adversary behavior, sandboxing, endpoint detection, and threat intelligence are critical to identify and block cyber threats. Simultaneously self-learning intelligence of network nodes and users, as well as, behavioral analytics on endpoints, enable the validation of emerging zero-day threats that bypass other security controls, by correlating this information in order to identify outliers that indicate in-progress attacks. Finally, effective investigation and analysis of intrusions gives organizations the ability to pinpoint the root cause, the scope of the breach, the data loss, and the steps required to contain the breach, and enhance the adaptive threat response process to achieve automation.

Real-time Threat Intelligence

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

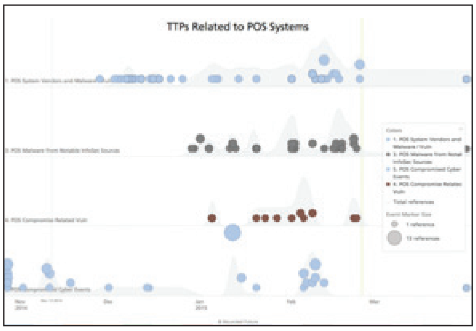
Faster Analysis:
Spend less time collecting data and supercharge your analytic capacity.

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.

Network Visibility

endace.com

The Endace approach to network visibility is the product of more than 15 years of extensive research and development. Our hardware-based, network visibility solutions are based on our proprietary DAG technology and deliver 100% accurate visibility into network traffic regardless of network types, speeds or loads. They are capable of capturing, indexing and recording every packet right up to 100Gbps, and are trusted by some of the world’s largest organisations across many industries to help with a wide range of challenges from reducing resolution times for security and network performance issues to complying with data retention or lawful intercept obligations.

To cope with the demands of modern networks, organisations require a fundamentally different approach to network visibility. To become truly responsive, they need to proactively capture and record network traffic so that history of activity can be used to identify and respond to issues quickly and efficiently. With Endace, when SecOps and NetOps teams need to analyse traffic and drill down to packet level to investigate an event, a full copy of the traffic is available to provide proof of what has happened.

There are three main reasons why StarLink customers buy Endace products:

Performance: We have built our reputation on creating products that work reliably and provide industry-leading performance. Our packet capture products deliver 100% packet capture regardless of network speeds, types or loads and they provide nanosecond-level time stamping accuracy on every packet recorded.

Scalability: Our products can capture up to 40Gpbs at line rate natively and, using EndaceAccess™ Network Visibility Head-Ends, offer a true 100Gbps monitoring and recording solution. With industry-leading storage capacity of up to 192TB per appliance, and true capture-to-storage rates up to a sustained 40Gbps, Endace network monitoring and recording solutions can scale to meet the needs of the fastest networks on the planet.

Open architecture: We believe you should be able to leverage your investment in monitoring and recording infrastructure to enhance the performance of your chosen security and network performance monitoring applications. We’ve designed our products to integrate easily with a wide range of commercial, open-source and custom-developed applications, so customers can choose the applications that best suits their needs.

Next Generation Malware, APT & Threat Protection

fidelissecurity.com

Fidelis Endpoint agent is software installed on customer endpoints to protect systems from a range of threats both proactively and reactively. Fidelis Endpoint agents continually record key system activity and can provide users with requested information from on demand or scheduled tasks. Event data and task results are securely transmitted back to the Fidelis Endpoint Cloud for storage and human analysis. Data includes:

- Endpoint Alert Data: Alerts generated by the Fidelis Endpoint system are stored in the cloud-hosted alert database for automated responses, enrichment, customer notification, and investigation workflows.
- Task Results: Tasks sent to endpoints will securely bring back the requested data and store it for real-time viewing in the Endpoint UI.
- Endpoint Event Metadata: The Fidelis Endpoint agent gathers metadata from the endpoint and sends it to the cloud hosted Endpoint Collector database. The agent continuously monitors and records key endpoint activity including file, registry, network, process information and more..
- User Selected Files and Forensic Artifacts: Users can collect specific files, forensic artifacts and forensic images from systems. Collected artifacts are stored securely in the file store for viewing and retrieval.
- Endpoint Status Information: Receive details about each host such as operating system, last contact time, IP address, agent version, and last logged on user.

The Next-generation Cybersecurity Analytics

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

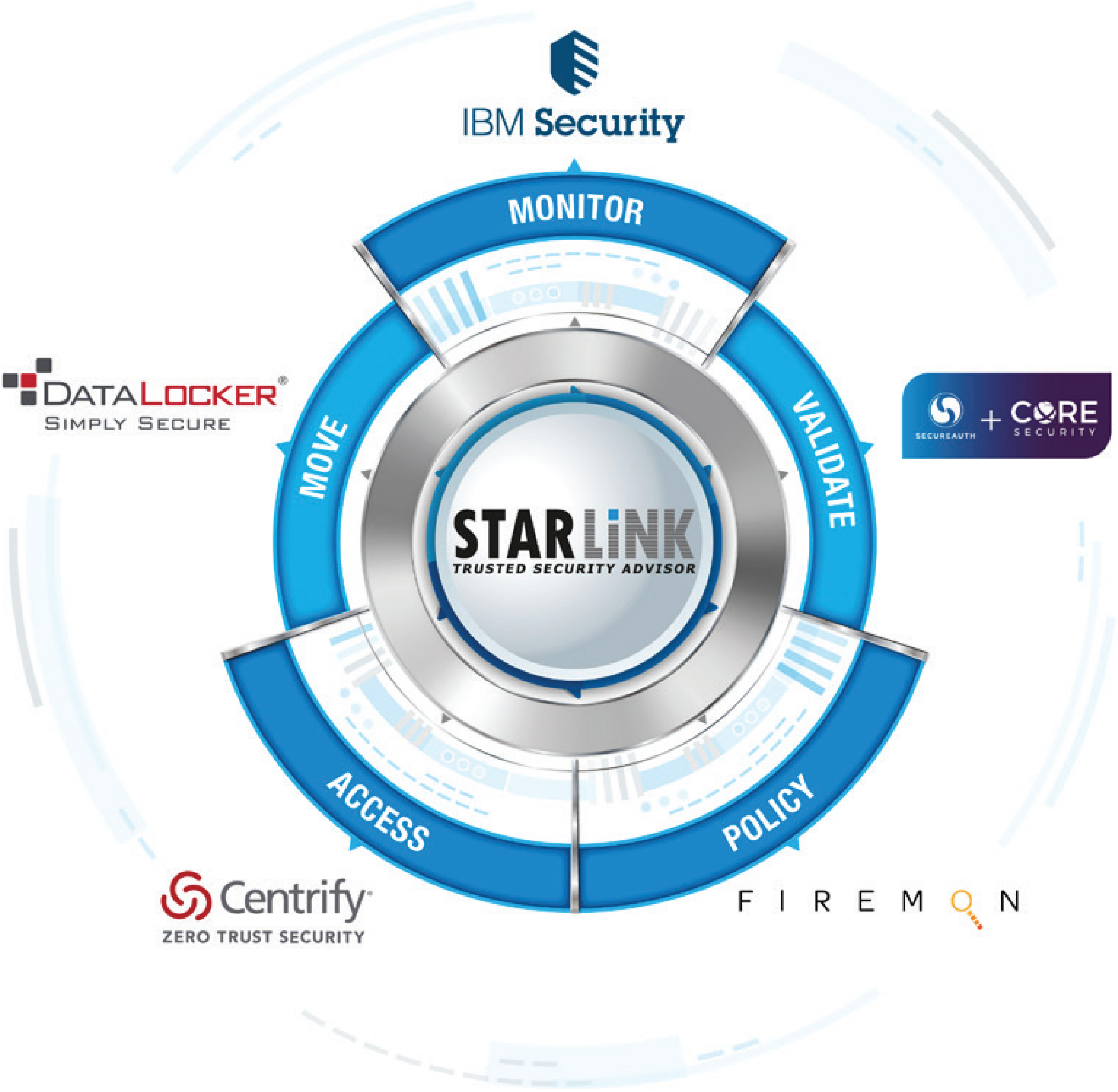
ThreatScore Quadrant

Identity Intelligence

Asset AutoDiscovery

BlockCount Ratio

Solution



Access Control

Where is my Sensitive Data?

Access Control 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.

Integrated Security Solution

IBM Security

ibm.com/security

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.

Vulnerability Aggregation, Penetration Testing & Validation

SECUREAUTH + CORE SECURITY

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

Enterprise Firewall Management

firemon.com

When you choose FireMon for network security policy management, you're getting 15 years of real-world cybersecurity problem-solving and the unique capabilities and services that come with that experience.

We take a holistic approach to security management that spans network security and operations to deliver on all four of Gartner's components in a Network Security Policy Management solution: security policy management, change management, risk and vulnerability analysis and application connectivity management.

Our solutions, whether the flagship Security Manager or the recently acquired Immediate Insight, work together to deliver unmatched visibility, integrations, automation and risk reduction.

With this approach, you gain a single source of truth for network security policy management that reduce complexity, inefficiencies and errors within your security infrastructure.

Identity and Acccess Management

ZERO TRUST SECURITY

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

Data Encryption Solutions

DATALOCKER®
SIMPLY SECURE

datalocker.com

DataLocker is an innovative provider of encryption solutions. The company was founded in 2007 and has offices in the U.S. (headquarters), U.K., and Korea.

Secure By Design

DataLocker products secure sensitive data using military-grade 256-bit encryption. With a wide range of products, DataLocker offers both hardware based external storage and software based cloud storage encryption options. Hardware based products do not require software or drivers to manage, encrypt or decrypt data.

Compliance Driven

DataLocker technology makes it simple to ensure compliance with some of the strictest governmental regulations. Most DataLocker products are FIPS 140-2 validated, issued by the National Institute of Standards and Technology (NIST). FIPS validated DataLocker products are a cost-effective way to comply with HIPAA, SOX, DHS Initiatives, NRC, GLB and any other directive that requires data encryption.

Proven Protection

DataLocker is trusted by governments, military and enterprises around the world. Other industries, including legal, financial and healthcare, use DataLocker products to secure, store, and transfer confidential data. To request a sample contact sales@datalocker.com.

DataLocker products combine superior convenience and usability with state of the art security. DataLocker is “Simply Secure.”

Customer Success Services

PROFESSIONAL SERVICES
STAFFING SERVICES
MANAGED SECURITY SERVICES
24/7
SUPPORT SERVICES
TRAINING SERVICES
Contact StarLink
+1 344 707 288
YOUR TRUSTED SECURITY ADVISOR
Reach StarLink Consulting Services via: uksales@starlinkme.net

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.