forsyte
I.T. SOLUTIONS

semperis

Enhancing Cybersecurity

across the SUNY System

Presented by
Forsyte & Semperis

Microsoft

Partnered for Success

24x7 Cybersecurity Protection at a Predictable Price

- Forsyte is Microsoft's leading provider of cybersecurity solutions for the Education Industry.
- Specialize in Threat Protection, Identity Protection, and Data Protection.
- Forsyte provides 24x7 managed detection and response solution that includes the initial and ongoing configuration and optimization of the underlying security platform.

- Semperis offers the industry's most comprehensive Active Directory and Entra ID threat prevention, detection, response, and recovery platform.
- No vendor or solutions provider can outmatch Semperis' collective Microsoft expertise in Active Directory security and recovery.

Microsoft Defender XDR

Integrated Security Across the Entire Attack Kill Chain

Defender for Office 365

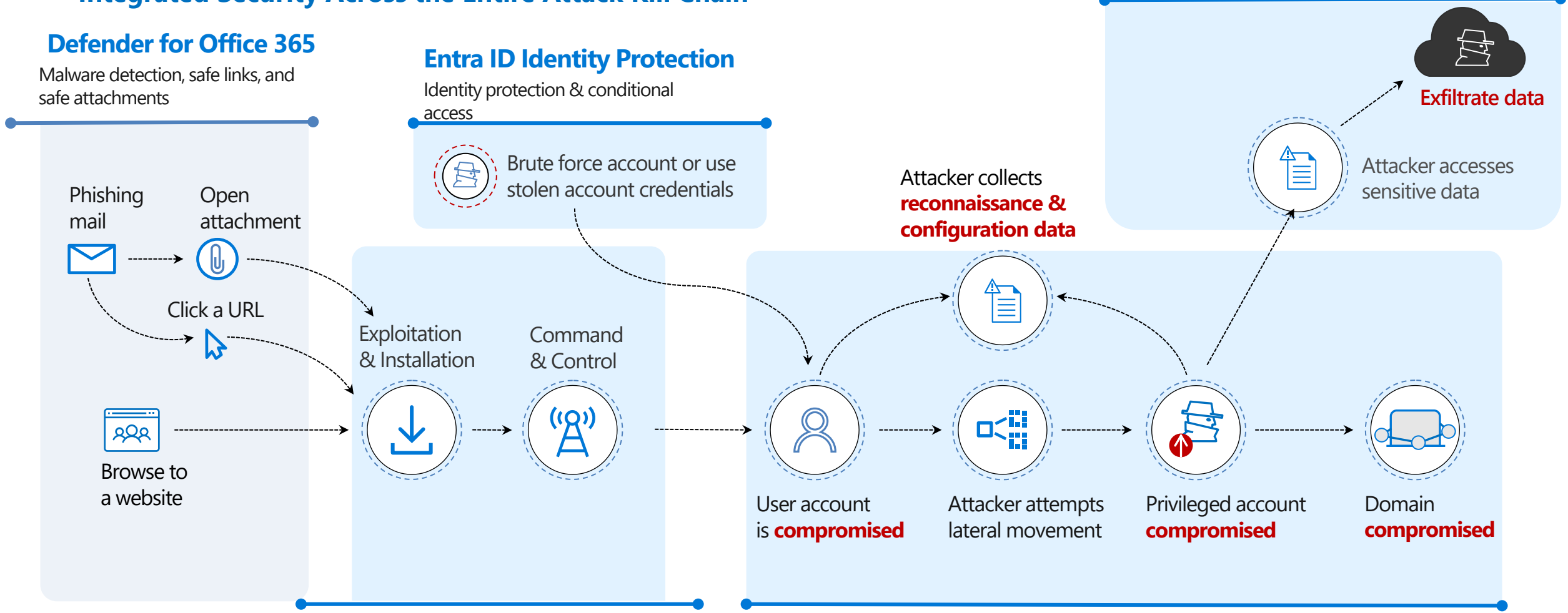
Malware detection, safe links, and safe attachments

Entra ID Identity Protection

Identity protection & conditional access

Defender for Cloud Apps

Extends protection & conditional access to other cloud apps



Defender for Endpoint and Server

Endpoint Detection and Response (EDR)
End-point Protection (EPP)
Web Content Filtering

Defender for Identity

Identity protection

Summary of Guardian Select Benefits

Unified Cybersecurity Monitoring

Guardian Select is designed to enhance security operations by collecting, enriching, and analyzing data from Microsoft M365 and on-premise Active Directory environments, including:

- **Unified Security Monitoring**: Features a data collection & aggregation engine that simplifies threat detection and remediation across Microsoft Defender XDR as well as non-MS security solutions.
- **Centralized Support**: Ideal for decentralized environments with multiple M365 tenants, providing centralized, unified support.
- **Streamlined Operations**: Utilizes a hub-and-spoke data collection system and a robust SOC command center to streamline security operations.
- **Unlimited 24x7 support**, including:
    - Microsoft 365 A5 security deployment and configuration assistance.
    - Best practice configuration and threat detection rules/policies.
    - Tailored onboarding assistance for each campus.
    - 24x7 support with threat hunting and remediation.
    - On-going M365 optimization to ensure resiliency against the latest attack vectors.

Summary of Semperis DSP Benefits

Industry's most comprehensive hybrid AD threat detection and response platform

DSP puts hybrid AD security on autopilot with continuous monitoring and unparalleled visibility across on-premises AD and Entra ID environments, tamperproof tracking, and automatic rollback of malicious changes.

- **Catch AD and Entra ID vulnerabilities before attackers do:** DSP continuously monitors for indicators of exposure and compromise – uncovered by the Semperis threat research team – that threaten AD and Entra ID
- **Eliminate Blind Spots in Hybrid AD Security:** DSP uses multiple data sources - including the AD replication stream– to capture changes that evade agent-based or log-based detection
- **Enable Rapid Recovery:** Semperis DSP automatically rolls back malicious changes in on-prem AD and Entra ID, offers manual rollback of Entra ID changes, and provides a unified dashboard so you can correlate changes across the hybrid AD environment
- **Premier, 24x7 Support**, including:
    - Dedicated Customer Success Manager
    - Deployment and configuration assistance

Summary of Semperis ADFR Benefits

Reducing the time to recover AD up to 90%

ADFR helps organizations prepare for the worst by ensuring a fast, malware-free AD forest recovery in the event of a cyber disaster, including:

- **Cyber-First Disaster Recovery**: Recover Active Directory even if domain controllers are infected or wiped out.
- **Anywhere Recovery**: Restore Active Directory to alternate hardware (virtual or physical).
- **Clean Recovery**: Eliminate reinfection of malware from system state backups by decoupling AD from the Operating System.
- **Advanced Automation**: Automate the entire recovery process and reduce downtime.
- **Post-breach Forensics** – ADFR provides a post-breach scanning tool specifically designed to spot backdoors so you can eliminate them before they become an issue.
- **Premier, 24x7 Support**, including:
    - Dedicated Customer Success Manager
    - Deployment and configuration assistance
    - 1 hour or less SLA for Catastrophic AD outage

24x7x365 Managed Security Operations

Guardian 365 3-Phased Onboarding Process

Phase I Assessment	Phase II Deployment	Phase III Managed Services

Evaluation & Assessment

- Security Assessment
- Gap Analysis
- Cyberinsurance Review

Implementation & Configuration

- Implementation of M365 Security Suite
- Deployment of Microsoft Sentinel
- Deployment of ADFR and DSP
- Deploy Standard Security Policies
- Pilot Testing Followed By Full-Scale Production Rollout
- Establish SOPs for Delivery

Ongoing Managed Services

- 24x7 Security Monitoring & Alerting
- Recurring Health Calls
- On-going System Optimization
- Annual Pen Testing
- Attack Simulation & Phishing Training
- Realtime Incident & KPI Portal

Other Critical Areas

- Microsoft Purview Data Security and Compliance.
  - Leverages the intelligence generated by the Purview suite of products to quickly identify, remediate, and contain assets that present threats to your data estate.
  - Includes support to configure a best-practice set of policies across the Purview suite.
    - Sensitivity Labels.
    - Data Loss Prevention & Endpoint Data Loss Prevention.
    - Insider Risk Management.
- Patching for Workstations and Servers.
  - Includes infrastructure evaluation and tiering.
  - SOPs for patch deployment & server and workstation testing and rollback, device hardening.
  - Recurring patch and system update reporting to ensure consistent and reliable support.